Hillstone Networks

StoneOS CLI User Guide

Complete Book

Version 5.5R11



TechDocs | docs.hillstonenet.com

Copyright 2024 Hillstone Networks. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks.

Hillstone Networks

Contact Information:

US Headquarters:

Hillstone Networks

5201 Great America Pkwy, #420

Santa Clara, CA 95054

Phone: 1-408-508-6750

http://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you comprehensive configuration instructions of Hillstone Networks StoneOS .

For more information, refer to the documentation site: https://docs.hillstonenet.com.

To provide feedback on the documentation, please write to us at:

TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-CUG-UNI-5.5R11-EN-V1.0-2024-09-12

Contents

Contents 1

About This Guide 1

Content 1

CLI 1

WebUI 2

Command Line Interface 2

Overview 2

CLI Modes and Prompts 2

Execution Mode 2

Global Configuration Mode 2

Sub-module Configuration Mode 3

Switching between CLI Modes 3

CLI Error Message 3

Command Input 4

Command Short Form 4

Listing Available Commands 4

Completing Partial Commands 5

Using CLI 5

Previous Commands 5

Shortcut Keys 5

Filtering Output of Show Commands 6
CLI Page Display 7
Specifying Screen Size 8
Specifying Connection Timeout 8
Redirecting the Output of Show Commands 9
Periodically Refreshing the Output of Show Commands 10
Diagnostic Commands 10
Viewing device Processes 10
Chapter 1 Firewall 1
Configuration Environment 4
Overview 4
Accessing a Device via Console Port 4
Accessing a Device via Telnet 5
Accessing a Device over SSH 6
Accessing a Device via WebUI 7
Logging in by Using Certificate Authentication 8
Configuring the Device Side 9
Configuring the Client Side 10
Unfreezing the WebUI 11
Application Mode 12
Overview 12
Transparent Mode 12

Mix Mode 12
Routing Mode 13
VSwitch 14
Basic Concepts 14
L2 Zones 14
L2 Interfaces 15
Forwarding Rules in VSwitch 15
Configuring a VSwitch 17
Viewing MAC Table Information 17
Virtual Wire 18
Configuring a Virtual Wire 19
Enabling Virtual Wire 19
Configuring a Virtual Wire Interface Pair 19
Viewing Virtual Wire Configuration Information 20
NSH Proxy 20
Enabling NSH layer 2 Proxy 21
NSH Proxy Debugging 21
Viewing the NSH Packets on Interfaces 21
Viewing the NSH Sessions 21
Viewing Virtual Wire and NSH Proxy Configurations 22
VLAN Transparent in the Transparent Mode 22
Configuration Example 23

Configuration Steps 24
Configuring Transparent ARP 26
Configuring a VRouter 26
Enabling and Disabling Mult-VR 26
Creating a VRouter 27
Viewing VRouter Information 27
Deployment Mode 28
Overview 28
Inline Mode 28
Bypass Mode 28
Mix Mode 29
Working Principle of Bypass Mode 30
Configuring Bypass Mode 30
Creating a Tap Zone 31
Binding an Interface to a Tap Zone 31
Configuring a Bypass Control Interface 31
Specifying a Statistical Range 32
Configuring a Linkage Firewall 33
Example of Configuring Bypass Mode 34
Topology 34
Configuration Steps 35
StoneOS Architecture 36

Overview 36
Interfaces 36
Zones 36
VSwitches 37
VRouter 37
Policy 38
VPN 38
Packet Handling Process 39
Deny Session 42
Configuring the Deny Session Function 43
Specifying the Deny Session Type 43
Specifying the Maximum Number of Deny Sessions 44
Specifying the Timeout Value 45
Viewing the Deny Session Configuration Information 45
Viewing the Deny Session Information 45
TCP RST Packet Check 45
Global Network Parameters 46
Configuring MSS 46
TCP Sequence Number Check 46
TCP Three-way Handshaking Timeout Check 47
Configuring the Global TCP Three-Way Handshaking Timeout Check Function 47

Configuring the TCP Three-Way Handshaking Timeout Check Function Based on Policy Rules 48
TCP Connection State Age-time 48
TCP SYN Packet Check 49
IP Fragment 50
SYN packets dropping 51
Enabling/Disabling SYN Packets Dropping 51
Show the state of the function of SYN packets dropping 51
Jumbo Frame 52
Configuring TCP Packet Timestamp 53
Validity Check for Layer 4 Protocol 54
Enabling/Disabling Validity Check for Layer 4 Protocol 54
Checking Whether Validity Check for Layer 4 Protocol is Enabled 54
Session Information 54
Showing Session Information 55
Clearing Session Information 57
Delay Deleting Session 58
Enable delaying deleting session 58
Show the state of the function of delaying deleting session 59
RTO Query Optimization 59
Enabling/Disabling RTO Query Optimization 59
Displaying the State of RTO Query Optimization 60

Low Latency Mode 60
Packet Length Sanity Check 61
Enabling/Disabling Packet Length Sanity Check 61
Displaying the State of Packet Length Sanity Check 61
Configuring TSO/LRO Function 61
Application Layer Fast Forward 62
Enabling/Disabling Application Layer Fast Forward 62
Displaying the State of Application Layer Fast Forward 62
Response Traceroute Function 63
Enabling/Disabling the Response Traceroute Function 63
Displaying the Status of the Response Traceroute Function 63
Zone 64
Overview 64
Predefined Security Zone 64
Configuring a Security Zone 64
Viewing the Zone Information 65
Creating a Zone 65
Specifying the Description 65
Binding a Layer 3 Zone to a VRouter 66
Binding a Layer 2 Zone to a VSwitch 66
Specifying the Service Type 67
Configuration Example 67

Interface 68
Overview 68
Interface Types 68
Interface Dependency 70
Viewing Interface Information 71
Viewing All Interfaces 71
Viewing a Specific Interface 73
Configuring an Interface 73
Binding an Interface to a Zone 75
Specifying the Description 76
Configuring an Interface IP Address 76
Configuring Interface Secondary IP 77
Configuring an Interface MTU Value 78
Configuring Interface Force Shutdown 78
Specifying the Track Object 79
Configuring Interface ARP Timeout 79
Configuring an Interface Protocol 80
Configuring FTP on the Interface 80
Configuring Port Mirroring 81
Limits and Precautions 82
Configuring Mirror Filter 95
Configuring Traffic Mirroring 97

Configuring a Mirror Profile 98
Mirroring Traffic to an Interface 98
Mirroring Traffic to an IP Address 99
Binding a Mirror Profile to a Policy 100
Viewing Mirror Profile Information 100
Interface Reverse Route 100
Configuring Interface Backup 101
Configuring Hold Time 102
Configuring the Keepalive Function of Interface 103
Configuring the Interface Group 103
Disabling Recording Interface IP Address Conflict Log Triggered by DAD Mode ARP Packets 104
Configuring Local ARP Proxy for Interfaces 105
Configuring 10 G Interface Auto Tuning 105
Enabling/Disabling the First Data Proxy Function of Interface 106
Configuring Interface Proxy ARP 107
PnP IP Configuration Example 108
Configuring Local Property 110
Configuring a Loopback Interface 110
Creating a Loopback Interface 110
Configuring an Ethernet Interface 111
Configuring an Ethernet Sub-interface 111

Entering the Ethernet Configuration Mode 111
Configuring an Interface Duplex Mode and Speed 112
Cloning a MAC Address 113
Configuring a Combo Type 113
Configuring a VSwitch Interface 114
Creating a VSwitch Interface 114
Configuring an Aggregate Interface 114
Creating an Aggregate Interface and Sub-interface 115
Adding a Physical Interface 115
Example of Configuring an Aggregate Interface 116
Configuring a Redundant Interface 116
Creating a Redundant Interfaces and Sub-interface 116
Adding a Physical Interface 117
Specifying the Primary Interface 118
Enabling/Disabling alarm logs of ARP loops 118
Example of Configuring a Redundant Interface 118
Configuring a Tunnel Interface 119
Creating a Tunnel Interface 119
Binding a Tunnel 120
Cloning a MAC Address 121
Multi-tunnel OSPF 121
Borrowing an IP Address (IP Unnumbered) 122

Viewing Tunnel Information 122
Configuring a PPPoE Sub-interface 122
Configuring a Vif Interface 123
Creating a Vif Interface 123
Link Aggregation 123
LACP 124
Member Status in an Aggregate Group 124
Configuring LACP 125
Enabling/Disabling LACP 125
Specifying LACP System Priority 126
Specifying Interface LACP Priority 126
Specifying LACP Timeout 127
Specifying the Maximum Active Links 127
Specifying the Minimum Active Links 128
Specifying the Load Balance Mode 128
Viewing Aggregate Group Information 129
Bypassing the Device 129
Network Layout with Bypass Module 130
Enable / Disable Forced Bypass 131
Monitor the Status of Ports 132
Address 133
Overview 133

Address Entry 133
Configuring an Address Book 133
Global Configuration of Address Book 134
Entering the Global Configuration Mode of Address Book 134
Enabling/Disabling Ordered Address Book Function 134
Adding or Deleting an Address Entry 135
Specifying the IP Range of an Address Entry 136
Excluding Address Entries 141
Exlcuding an IPv4 Address Entry 142
Excluding IPv6 Address Entries 143
Specifying the IP Address of an Ordered Address Entry 144
Moving a Member of the Ordered Address Entry 144
Renaming an Address Entry 145
Viewing the Reference Address of an Address Entry 145
Viewing the Address Book Details 146
Address Book Configuration Example 148
Configuration Example 1 148
Configuration Example 2 148
Custom IP Geolocation 149
Configuring Custom IP Geolocation 149
Viewing Custom IP Geolocation 150
Service and Application 151

Service Overview 151
Viewing Service or Service Group Information via CLI 151
Viewing Service Information That Contains Specified Keywords 153
Viewing Service References 153
Predefined Services 155
RSH 155
Sun RPC 155
MS RPC 155
Predefined Service Group 156
User-defined Service 156
Creating/Deleting a User-defined Service 156
Adding/Deleting a User-defined Service Entry 157
Renaming a User-defined Service Entry 159
Configuration Example 159
Service Group 160
Creating/Deleting a Service Group 160
Adding/Deleting a Service/Service Group 161
Adding/Deleting Description to a Service/Server Group 161
Renaming a Service Group 162
Application Overview 162
Predefined Application 162
Predefined Application Groups 163

Userdefined Application 163
Creating/Deleting the User-defined Applications 164
Configuring the Category/Subcategory of User-defined Applications 164
Configuring the Technology Used by User-defined Applications 166
Configuring Signatures for User-defined Applications 167
Viewing the Configuration of User-defined Applications 168
Enabling the User-defined Application Signature Configuration Mode 168
Creating/Deleting the User-defined Application Signature Rule 168
Configuring Rules in User-defined Application Signature Configuration Mode 168
Configuring Rules in Application Signature Rule Configuration Mode 169
Configuring the Entry of the User-defined Application Signature Rule 170
Configuring the Application Timeout Value 172
Modifying the Order of the User-defined Application Signature Rule 173
User-defined Application Group 173
Creating/Deleting an Application Group 174
Adding/Deleting an Application or Application Group 174
Adding/Deleting a Description for an Application or Application Group 175
Application Identification 175
Dynamic Identification 175
SIP Deep Identification 176
Enabling/Disabling SIP Deep Identification 176
Viewing the Status of SIP Deep Identification 176

Application Identification Bypass 177
Enabling/Disabling Application Identification Bypass 177
Configuring CPU Usage Range 177
Viewing Information of Application Identification Bypass 178
Application Identification Cache Table 178
Enabling/Disabling Application Identification Cache Table 178
Specifying a Working Mode for the Dynamic Application Identification Cache Table 179
Clearing the Application Identification Cache Table 180
Viewing Application Identification Cache Table Information 180
Updating the Signature Database 180
Configuring an Application Signature Update Mode 181
Configuring an Update Protocol 181
Configure an Update Server 181
Specifying a HTTP Proxy Server 182
Specifying an Update Schedule 182
Updating Now 183
Viewing Application Signature Information 183
Viewing Application Signature Update Information 184
Application Filter Group 185
Creating Application Filter Group 186
Specifying Application Category 186

Specifying Application Subcategory 186
Specifying Application Technology 187
Specifying Risk Value for Application 187
Specifying Application Characteristics 187
Configuration Example 188
DNS 190
Overview 190
Configuring a DNS Server 190
Configuring a Domain Name 190
Configuring a DNS Domain Name Server 191
Configuring a DNS Proxy 191
Configuring a DNS Proxy Rule 192
Creating a DNS Proxy Rule 193
Configuring the Filtering Condition of a DNS Proxy rule 193
Specifying Ingress Interface 193
Specifying Source Address 193
Specifying Destination Address 194
Specifying Domain Name 195
Specifying the Action of a DNS Proxy Rule 195
Configuring DNS Proxy Servers 196
Modifying/Deleting the Descriptions of a Proxy Rule 197
Enabling/Disabling DNS Proxy Log 197

Enabling/Disabling a DNS Proxy Rule 197
Moving a DNS Proxy Rule 198
Configuring Time Interval of Tracking for DNS Proxy 198
Enabling/Disabling Calculating the Checksum of UDP Packet for DNS Proxy 199
Specifying the TTL for DNS-proxy Response Packets 199
DNS Proxy Hit Analysis 199
Viewing DNS Proxy Statistical Information 200
Clearing DNS Proxy Statistical Information 200
Viewing the DNS Proxy Rule 200
Resolution 200
Specifying the Timeout of DNS Requests 200
Specifying the Retry Times of DNS Requests 201
Specifying the Maximum Request Interval for DNS Resolution 201
Specifying the TTL for DNS Resolution Cache 202
Configuring Host TTL 202
Viewing the Configuration Information of Host TTL 203
Enabling the DNS Resolution Log 203
DNS Cache 204
Adding a Static DNS Mapping 204
Viewing a DNS Mapping 205
Deleting a Dynamic DNS Mapping 205
Secure DNS 205

Enabling/Disabling the Secure DNS Function 206
Entering the Secure-DNS Profile Configuration Mode of a Specified Provider 207
Configuring the DoH Server 207
Enabling/Disabling the Function of Sending the Client Address 207
Configuring the Health Check Interval 208
Enabling/Disabling the Function of Generating Logs 208
Viewing Information about Secure DNS Configuration 209
DNS Snooping 210
Specifying the Domain Name Resolution Mode 210
Specifying the Maximum Mapping IP Addresses for a Specific Domain Name 211
Specifying the Forward Delay of DNS Response Packets 211
Specifying the Maximum Wildcard Domain Names 212
Specifying the TTL for DNS Snooping Mapping Cache 212
Configuring the UDP Packet Length That Can Be Parsed by DNS Snooping in the Active Mode 213
Viewing the Configuration Information of DNS Snooping 214
Viewing the Mapping information of DNS Snooping 214
Enabling/Disabling DNS 214
Viewing DNS configuration information 215
DNS Configuration Example 215
Requirement 215
Configuration Steps 215

DDNS 217
Configuring DDNS 217
Configuring a DDNS Name 218
Specifying the DDNS Provider 218
Specifying the DDNS Server Name and Port 219
Specifying the Minimum Update Interval 219
Specifying the Maximum Update Interval 220
Specifying the DDNS Username/Password 220
Binding a DDNS Name to an Interface 220
Viewing DDNS Information 221
Example of Configuring DDNS 221
Requirement 221
Configuration Steps 221
DHCP 224
DHCP on Hillstone Devices 224
Configuring a DHCP Client 224
Obtaining an IP Address via DHCP 225
Releasing and Renewing the IP Address 225
Configuring the Route Priority (Administration distance) and Route Weight 226
Enable/ Disable Classless Static Routing Options 226
Viewing DHCP Client Configuration Information 227
Obtaining the Server MTU 227

Configuring the DNS Management Priority 228
Configuring a DHCP Server 228
Basic Configuration of the DHCP Address Pool 229
Configuring an IP Range 229
Configuring a Reserved Address 230
Configuring a Gateway 230
Configuring a Netmask 230
Configuring a DHCP Lease Time 231
Configuring Auto-config 231
Configuring DNS/WINS Servers and Domain Name for the DHCP Client 231
Configuring SMTP/ POP3/news Servers for the DHCP Client 232
Configure the IP Address of the Relay Agent 233
IP-MAC Binding 233
Binding the Address Pool to an Interface 234
Configuring DHCP Options 234
Configuring Option 43 234
Configuring the VSI Carried by Option 43 for DHCP Server 234
Configuring Option 49 235
Configuring Option 60 235
Verifying VCI Carried by Option 60 236
Configuring the VCI Carried by Option 60 for DHCP Server 236
Configuring Option 66 237

Configuring Option 67 237
Configuring Option 138 238
Configuring Option 150 238
Configuring Option 242 239
Viewing DHCP Configuration Information 239
Configuring a DHCP Relay Proxy 240
Specifying the IP Address of the DHCP Server 240
Enabling DHCP Relay Proxy on an Interface 240
Enabling the Function of Replacing the Source IP of the DHCP Relay Packets 241
PPPoE 242
Configuring PPPoE 242
Configuring a PPPoE Instance 243
Specifying the Access Concentrator 243
Specifying the Authentication Method 243
Configuring a PPPoE Connection Method 244
Specifying the Netmask 245
Specifying the Route Distance/Weight 245
Specifying the Service 245
Specifying the Static IP 246
Specifying the PPPoE User Information 246
Configuring the Schedule 246
Specifying the MAC Address of the PPPoE Server 247

Configuring Connection Status Detection 248
Obtaining an IP Address via PPPoE 248
Binding a PPPoE Instance to an Interface 249
Manually Connecting or Disconnecting PPPoE 249
Viewing PPPoE Configuration Information 249
Example of Configuring PPPoE 250
Requirement 250
Configuration Steps 250
NAT 252
Overview 252
Basic Translation Process 252
NAT of Hillstone Devices 253
Limits on Configuring NAT in HA Scenario 254
Configuring a NAT Rule 254
Creating a BNAT Rule 255
Moving an BNAT Rule 258
Specifying a Schedule for a BNAT Rule 258
Viewing BNAT Configuration Information 258
Creating an SNAT Rule 259
Enabling/Disabling SNAT Rule 265
Moving an SNAT Rule 266
Enabling/Disabling Expanded PAT Port Pool 266

Enabling/Disabling the Function of Expanding Translated IP Address Range 267
Checking Whether the Function of Expanding Translated IP Address Range is Enabled 268
Deleting an SNAT Rule 268
Modifying/Deleting the Descriptions of a SNAT Rule 268
Specifying a Schedule for an SNAT Rule 268
Configuring the SNAT Rule Port Resource Monitor Function 269
Viewing the SNAT Rule Port Usage Monitor Function Configuration 269
Viewing SNAT Configuration Information 269
Viewing SNAT Source Utilization 270
Viewing Tracked Failed Information of SNAT Translated Address 271
Viewing SNAT Rule Hit Counts 271
Viewing Statistics on SNAT Rule Hits 272
Clearing Statistics on SNAT Rule Hits 275
Creating a DNAT Rule 275
Enableing/Disabling DNAT Rule 279
Moving a DNAT Rule 279
Modifying/Deleting the Descriptions of a DNAT Rule 280
Deleting a DNAT Rule 280
Specifying a Schedule for a DNAT Rule 280
Viewing DNAT Configuration Information 281
Viewing DNAT Rule Hit Counts 283

Viewing Statistics on DNAT Rule Hits 283
Clearing Statistics on DNAT Rule Hits 286
Configuring an Excluding Port Rule 287
Creating a SNAT Port Group 287
Specifying the Description of SNAT Port Group 287
Specifying the Excluding Port Number 288
Binding the SNAT Port Group to VRouter 288
Viewing the SNAT Port Group Information 289
Viewing the SNAT Port Group References 289
Redundancy Check 289
DNS Rewrite 290
Configuring DNS Rewrite Rules 291
Modifying/Deleting DNS Rewrite Rule Description 291
Viewing DNS Rewrite Rules 292
Viewing Dynamic Mapping Entries of DNS Rewrite 292
Adjusting the Priority of DNS Rewrite Rule 293
Enabling/Disabling DNS Rewrite Rule Rematch 294
NAT444 294
Configuring NAT444 294
Monitoring the Port Utilization and Port Block Utilization 297
Viewing NAT444 Configuration Information 298
Full-cone NAT 298

Viewing Full-cone NAT Configuration Information 300
Bounce NAT 301
Example of Configuring NAT 302
Requirement 302
Configuration Steps 303
Application Layer Identification and Control 307
Overview 307
Fragment Reassembly 307
Application Layer Gateway (ALG) 307
HTTP, P2P and IM 308
Configuring ALG 309
Enabling/Disabling DNS Rewrite by DNAT 311
Specifying SIP Proxy Server Mode 312
Showing ALG SIP 312
Examples of Configuring Application Layer Identification and Control 312
Configuration Steps for Example 1 313
Configuration Steps for Example 2 314
RSTP 316
Configuring RSTP 316
Creating RSTP 317
Enabling RSTP on the Device 317
Enabling RSTP on an Interface 317

Configuring the Bridge Priority 317
Configuring the Hello Interval 318
Configuring the Forward Delay Time 318
Configuring the Maximum Age of BPDU Message 319
Configuring the RSTP Priority on an Interface 319
Configuring the RSTP Cost on an Interface 320
Viewing RSTP Configuration 320
Configuration Example 320
Requirement 320
Configuration Steps 321
Wireless Access Mode 324
Introduction 324
WLAN 324
Configuring WLAN Settings 324
Enabling WLAN Function 325
Creating WLAN Profile 325
Configuring SSID 325
Enabling/Disabling SSID Broadcast 326
Configuring Security Mode and Authentication Encryption Method 326
Enabling/Disabling User Isolation 328
Configuring Maximum User Numbers 328
Specifying the Authentication Server 328

Binding the WLAN Profile to a WLAN Interface 329
Configuring Global Parameters 329
Configuring the Country/Region Code 330
Configuring the Operation Mode 336
Configuring the Channel 337
Specifying the Maximum Transmit Power 337
Enabling/Disabling Wireless Multimedia Function 338
Viewing WLAN Settings 338
WLAN Configuration Example 338
Requirement 339
Configuration Steps 339
3G/4G 343
Configuring 3G/4G Function 343
Configuring Basic Parameters 343
Configuring the Access Point Name 344
Enabling/Disabling the 3G/4G Function 344
Authenticating 4G module password 345
Specifying the Connection Mode 345
Configuring the Dial-up String 346
Specifying the Verification Method 346
Specifying the Route Distance and Weight 346
Specifying the Static IP Address 347

Specifying the Online Mode 347
Specifying the User Information 348
Configuring the Schedule 348
Manually Connect/Disconnect the 3G/4G Connection 349
Managing the PIN Code 349
Enabling/Disabling the PIN Code Protection 350
Automatically Verifying the PIN Code 350
Manually Verifying the PIN Code 350
Modifying the PIN Code 351
Unlocking the PIN Code 351
Viewing the 3G/4G Configurations 351
3G Configuration Example 352
Requirement 352
Configuration Steps 352
LLDP 353
LLDP Work Mode 354
Configuring LLDP 354
Enabling/Disabling Global LLDP 355
Enabling/Disabling LLDP of Port 355
Configuring LLDP Work Mode 356
Configuring the Initialization Delay of Port 356
Configuring the Transmission Delay of LLDP Messages 357

Configuring the Transmission Interval of LLDP Messages 357
Configuring TTL Multiplier 358
Displaying LLDP Local Information 358
Displaying LLDP Neighbor Information of Port 358
Displaying LLDP Statistical Information 359
Displaying LLDP Status Information 359
Hardware Fast Forwarding 359
Introduction 359
Precautions and Limits 360
Enabling/Disabling Hardware Fast Forwarding 360
Enabling/Disabling the Fast Aging Function of TCP Hardware Fast Forwarding Flow Table Entries 361
Enabling Congestion Packet Loss on Egress Interface for Device 362
Viewing Configuration Information of Hardware Fast Forwarding 362
Chapter 2 Policy 364
Security Policy 365
Overview 365
Basic Elements of Policy Rules 365
Defining a Policy Rule 366
Introduction to Profile 366
QoS Tag 366
Configuring Access Control for a Policy 366

Configuring an ACL Profile 367
Configuring an Access Control Rule 367
Configuring the Default Action 368
Viewing ACL Profile Information 368
Configuring a Policy Rule 368
Entering the Policy Configuration mode 369
Switching to the Multi-Zone Mode 369
Creating a Policy Rule 369
Editing a Policy Rule 373
Enabling/Disabling a Policy Rule 378
Log Management of Policy Rules 378
Configuring the Service Rule 379
Specifying the Default Action 382
Moving a Policy Rule 382
Viewing Resource Usage in Policy Rules 383
show policy resource 383
Rule Redundancy Check 383
Specifying the Issue Types of Redundancy Check 384
Viewing the Issue Types of Redundancy Check 385
Starting Redundancy Check 385
Stopping Redundancy Check 385
Viewing Redundancy Check Results 385

Viewing the Coverage of Policy Rules 386
Configuring Ignored Time of Redundant Policy Rules 386
Configuring Ignored Days 386
Configuring Expiration Time for Ignorance 387
Unignoring Redundant Policy Rules 387
Viewing Ignored Redundant Policy Rules 387
Clearing Redundant Check Results 387
Configuring the Session Timeout Period of Policy Rule 388
Viewing the Status of Persistent-Connection Session 388
Configuring Policy Audit Function 388
Enabling/Disabling the Policy Audit Function 389
Adding the Audit Comment 389
Viewing Policy Audit Enabled Status 389
Policy Group 390
Configuring Policy Group 390
Creating/Deleting a Policy Group 390
Enabling/Disabling a Policy Group 390
Modifying/Deleting the Descriptions of a policy group 391
Adding/Deleting a Policy Rule Member 391
Renaming a Policy Group 392
Configuring a policy group for VSYS Profile 392
Viewing Policy Group Information 392

User Online Notification 392
Configuring the User Online Notification URL 393
Configuring the Idle Time 394
Customizing the Logo Picture 394
Viewing Online Notification Users 395
Configuring Policy Custom Attributes 395
Configuring Custom Attributes Mapping 395
Configuring Custom Attributes for Policies 396
Viewing Policy Custom Attribute Information 397
Specifying That the Policy Matches the Post-DNAT Destination Address 397
Viewing Policy Rules That Contain Specified Service Keywords 398
Viewing Policy Rule Information 398
Viewing the current policy configuration information of the device 402
Policy Hit Count 403
Viewing Statistics on Policy Rule Hits 405
Clearing Statistics on Policy Rule Hits 407
Enabling/Disabling Traffic Statistics of Policies 408
Viewing the Status of Policy Traffic Statistics 408
Enabling/Disabling the Delay Address Update Time Function 408
Configuring the Policy Assistant 409
Enabling/Disabling the Policy Assistant 409
Viewing the Policy of the Policy Assistant Enabled 410

Enabling Traffic Statistics of Policy Assistant 410
Viewing the Status of Policy Assistant Traffic Statistics 410
Aggregate Policy 410
Creating an Aggregate Policy 411
Adding an Aggregate Policy Member 412
Removing an Aggregate Policy Member 412
Deleting an Aggregate Policy 413
Adjusting Position 413
Enabling/Disabling an Aggregate Policy 414
Adding/Deleting an Aggregate Policy Description 415
Share Access 416
Share Access Rule 416
Creating Share Access Rules 416
Configuring Share Access Rules 417
Viewing Share Access Rules 419
Share Access Signature Database 419
Configuring the Update Mode of Share Access Signature Database 420
Updating Share Access Signature Database 421
Importing a Share Access Signature File 421
Viewing Update Information of Share Access Signature Database 422
Viewing Information of Share Access Signature Database 422
Viewing Statistics of Share Access 422

Share Access Log 423
Configuring the Status of Share Access Log 424
Configuring the Output Destination of Share Access Log 424
Viewing Share Access Logs 424
ARP Defense 425
IP-MAC Binding 425
Static Binding 425
Adding a Static IP-MAC Binding 425
Adding a Static IP-Port Binding 426
Only Allowing Hosts with Static IP-MAC Binding Accessing the Internet 426
Dynamic IP-MAC-Port Binding 427
ARP Learning 427
ARP Learning Limit 427
MAC Learning 428
Viewing IP-MAC-Port Binding Information 428
Clearing ARP Binding Information 428
Forcing Dynamic MAC-Port Binding 429
DHCP Snooping 429
Enabling/Disabling DHCP Snooping 430
Configuring DHCP Snooping 430
Configuring DHCP Packet Rate Limit 431
Viewing DHCP Snooping Configuration Information 431

DHCP Snooping List 432
ARP Inspection 432
Enabling/Disabling ARP Inspection 433
Configuring a Trusted Interface 434
Configuring an ARP Rate 434
ARP Defense 435
Host Defense 435
Chapter 3 Routing 437
Enabling/Disabling Static Routing Query 438
Enabling/Disabling the Route Rematch by Session 438
VRouter 440
Specifying the Maximum Number of Routing Entries 441
Importing VRouter Routing Entries 441
Disable the Highest Priority of Direct Route 441
Destination Route 442
Configuring a Destination Route 442
Adding a Destination Route 442
Viewing destination routing information 444
Destination Interface Route 444
Adding a Destination Interface Route 444
Viewing Destination Interface Route Information 446
Viewing FIB Information about Destination Interface Route 446

ISP Route 446
Configuring the ISP Information Database 447
Configuring the Update Mode of the ISP Information Database 448
Configuring the Transmission Protocol for Update 448
Configuring the Update Server 448
Specifying the HTTP Proxy Server 449
Specifying the Update Time 450
Updating Immediately 450
Importing Predefined ISP Profiles 450
Deleting Predefined ISP Profiles 451
Deleting Predefined IPv4 ISP Profiles 451
Deleting Predefined IPv6 ISP Profiles 452
Displaying Information about the ISP Information Database 452
Displaying the Update Configuration of the ISP Information Database 453
Configuring IPv4 ISP Information 454
Adding a Subnet Entry 454
Adding an IPv4 ISP Information Entry 455
Configuring an IPv4 ISP Route 455
Viewing IPv4 ISP Route Configuration Information 456
Uploading/Downloading a User-defined IPv4 ISP Profile 457
Uploading a User-defined IPv4 ISP Profile 458
Downloading a User-defined IPv4 ISP Profile 458

Configuring IPv6 ISP Information 458
Adding an IPv6 Subnet Entry 459
Adding an IPv6 ISP Information Entry 459
Configuring an IPv6 ISP Route 460
Viewing IPv6 ISP Information 461
Uploading/Downloading a User-defined IPv6 ISP Profile 461
Uploading a User-defined IPv6 ISP Profile 462
Downloading a User-defined IPv6 ISP Profile 463
Source Route 463
Adding a Source Route 463
Viewing Source Route Information 464
Src-If Route 464
Adding a Src-If Route 465
Viewing Src-If Route Information 466
Policy-based Route 466
Creating a PBR Policy 466
Creating a PBR Rule 466
Editing a PBR Rule 468
Enabling/Disabling a PBR Rule 470
Moving a PBR Rule 470
Configuring Prioritized Destination Routing Lookup 471
Applying a PBR Rule 471

Configuring the Global Match Order of PBR 471
Viewing the the Global Match Order of PBR 472
Configuring TTL Range for a PBR Rule 472
Viewing PBR Rule Information 473
DNS Redirect 473
Configuration Example of Web Video Traffic Redirection 474
Domain Name Route 476
Configuring a Domain Name Route 477
Dynamic Routing 478
Configuring RIP 479
Basic Options 479
Specifying a Version 479
Specifying a Metric 480
Specifying a Distance 480
Configuring the Default Information Originate 480
Specifying a Timer 481
Configuring Redistribute 482
Configuring a Passive IF 482
Configuring a Neighbor 483
Configuring a Network 483
Configuring a Distance 483
RIP Database 484

Configuring RIP for Interfaces 484
Configuring an Authentication Mode 484
Specifying RIP Version 485
Configuring Split Horizon 486
Viewing System RIP Information 486
Configuring OSPF 486
Configuring OSPF Protocol 487
Configuring a Router ID 489
Configuring Area Authentication 489
Specifying the Network Type for an Interface 489
Configuring Route Aggregation for an Area 490
Configuring the Default Cost for an Area 491
Configuring the Virtual Link for an Area 491
Configuring a Stub Area 493
Configuring a NSSA Area 493
Configuring the Reference Bandwidth for OSPF 494
Configuring the Default Metric 494
Configuring the Default Information Originate 494
Configuring the Default Distance 495
Configuring a Timer for OSPF 495
Specifying an OSPF Network Interface 496
Configuring Redistribute 496

Configuring a Distance 497
Configuring a Passive IF 498
Configuring Route Filters Based on the Route Access-list 498
Configuring OSPF GR 498
Enabling Opaque LSA Capability 500
Enabling the GR function of the GR Restarter 500
Configuring GR Interval of the GR Restarter 501
Enabling the GR Helper Feature 501
Enabling GR Helper Strict LSA Check 501
Viewing OSPF GR Information 502
Configuring OSPF for an Interface 502
Configuring OSPF Authentication for an Interface 502
Specifying the Link Cost for an Interface 503
Configuring the Timer for an Interface 503
Specifying the Router Priority for an Interface 505
Specifying the Network Type for an Interface 505
Viewing OSPF Route Information 506
Configuring IS-IS 507
Basic Settings 509
Configuring the Router Type 509
Enabling IS-IS at Interfaces 510
Configure the Interface Type 510

Configuring the Network as Point-to-Point Type 510
Routing Information Settings 510
Configuring the NET Address 510
Configuring the Administrative Distance 511
Configuring the Metric Style 511
Configuring the Interface Metric 512
Configuring Redistribute 512
Configuring the Default Route Advertisement 513
Network Optimization 513
Configuring the Interval for Sending Hello Packets 513
Configuring the Multiplier for Hello Packets 514
Configuring Padding for Hello Packets 514
Configuring Priority for DIS Election 515
Configuring the Passive Interface 515
Configuring LSP Generation Interval 515
Configuring Maximum Age of LSPs 516
Configuring LSP Refresh Interval 516
Configuring SPF Calculation Interval 517
Configuring the Overload Bit 517
Configuring Hostname Mappings 517
Authentication 518
Configuring the Authentication Methods 518

Configuring the Interface Authentication 519
Viewing IS-IS Information 520
Configuring BGP 520
Configuring BGP Protocol 522
Entering the BGP Configuration Mode 523
Specifying a Router ID 523
Creating a Route Aggregation 524
Adding a Static BGP Route 524
Configuring a Timer 525
Specifying the Administration distance of BGP Route 526
Specifying the Default Metric 526
Creating a BGP Peer Group 527
Adding a BGP Peer-to-peer Group 527
Configuring a BGP Peer 527
Configuring BGP MD5 Authentication 528
Activating a BGP Connection 528
Configuring the Default Information Originate 529
Configuring Description 529
Configuring a BGP Peer Timer 530
Configuring the Next Hop as Itself 531
Configuring EBGP Multihop 531
Disabling a Peer/Peer Group 531

Resetting a BGP Connection 532
Redistributing Routes into BGP 532
Displaying Communities Attribute in the AA:NN Format 533
Configuring Route Filters Based on the AS-path Access List 533
Sending Communities Path Attributes to Peers or Peer Groups 534
Configuring Route Filters Based on the Route Map 534
Configuring Equal Cost Multipath Routing 535
Viewing BGP Information 535
Enabling/Disabling multipath-relax of EBGP 536
Configuring BGP GR 537
Route Object 541
Route Map 541
Configuring a Route Map 544
Configuring a Route Map and Adding a Matching Rule 544
Adding a Matching Condition 545
Continuing to Match Another Matching Rule 547
Modifying Attributes of Introduced Routing Information 548
Access List Route 549
Configuring a Route Access List 550
Configuring an IPv4 Route Access List 550
Configuring an IPv6 Route Access List 552
AS Path Access List 553

Configuring an AS-path Access List 554
Community List 554
Configuring BGP Communities 555
ECMP 555
Configuring ECMP 556
Configuring ECMP Route Selection 556
Static Multicast Routing 556
Enabling/Disabling a Multicast Route 557
Configuring a Static Multicast Route 557
Specifying an Ingress/Egress Interface 558
Viewing Multicast Route Information 558
Viewing Multicast FIB Information 559
IGMP 559
IGMP Proxy 559
Enabling an IGMP Proxy 560
Configuring an IGMP Proxy Mode for an Interface 561
Viewing IGMP Proxy Information 561
IGMP Snooping 562
Enabling IGMP Snooping 562
Configuring IGMP Snooping 563
Dropping Unknown Multicast 563
Viewing IGMP Snooping Information 563

BFD 564
BFD Work Mode 564
BFD Echo 565
Configuring BFD 565
Configuring the BFD Detection Methods 566
Configuring the BFD Session Parameters 566
Enabling/Disabling the Echo Function 567
Specifying the Interval of Receiving Echo Packets 568
Configuring the Source IP Address of the Echo Packets 568
Configuring BFD Multi-hop Detection 569
Creating a BFD Multi-hop Detection Template 569
Specifying the Encrypted Authentication Mode of BFD Control Packets 570
Configuring BFD Multi-hop Session Parameters. 570
Integrating BFD with Routing Protocols 571
Integrating BFD with the Static Route 571
Integrating BFD with the OSPF Route 572
Integrating BFD with the BGP Route 572
Integrating BFD with the IS-IS Route 572
Viewing BFD Session Information 573
MPLS 573
Protocol Independent Multicast (PIM) 574
Basic Principles of PIM-SM 575

Configuring PIM-SM 576
Basic Configurations 577
Enabling/Disabling the PIM-SM 578
Configuring a Candidate RP 578
Configuring a Candidate BSR 579
Configuring a Static RP 579
Configuring the Switchover to SPT 580
Configuring PIM-SM for Interfaces 581
Enabling/Disabling the PIM-SM for Interfaces 581
Configuring the Priority of DR 582
Specifying the Interval for Sending the Hello Packets 582
Specifying the Interval for Sending IGMP General Query Messages 583
Specifying the IGMP General Query Timeout 583
Specifying the Maximum Response Time for IGMP General Query 583
Specifying the Non-direct Multicast Source Address 584
Configuring the MSR Function 585
Viewing PIM-SM Information 586
PIM-SSM 587
Configuring PIM-SSM 588
Configuring Address Range of PIM-SSM Multicast Group 588
Configuring IGMP Packets Filtering 589
Adding Multicast Router Interface to Multicast Group 590

MLD 591
MLDv1 591
MLDv2 592
Configuring IPv6 PIM-SM 592
Basic Configurations of IPv6 PIM-SM 593
Enabling/Disabling the IPv6 PIM-SM 593
Configuring a Candidate RP 594
Configuring a Candidate BSR 594
Configuring a Static RP 595
Configuring the Switchover to SPT 596
Configuring IPv6 PIM-SM for Interfaces 597
Configuring the Priority of DR 597
Specifying the Interval for Sending the Hello Packets 598
Specifying the Interval for Sending MLD General Query Messages 598
Specifying the MLD General Query Timeout 599
Specifying the Maximum Response Time for MLD General Query 599
Viewing IPv6 PIM-SM Information 600
Examples of Configuring Routes 601
Example of Configuring Static Route Query 601
Configuration Steps 602
Example of Configuring Multi-VR 603
Independent Multi-VR Forwarding 604

Configuration Steps 604
Inter-VR Forwarding 606
Configuration Steps 606
Example of Configuring Static Multicast Route 607
Requirement 608
Configuration Steps 608
Example of Configuring IGMP Proxy 610
Requirement 610
Configuration Steps 610
Example of Configuring IGMP Snooping 612
Requirement 613
Configuration Steps 613
Example of Configuring BFD 615
Requirement 615
Configuration Steps 616
Integrating BFD with the Static Route 616
Integrating BFD with the OSPF Route 617
Integrating BFD with the BGP Route 618
Example of Configuring LLB 619
Requirement 619
Configuration Steps 620
Example of Configuring PIM-SM 622

Requirement 622
Configuration Steps 623
Chapter 4 System Management 625
Naming Rules 626
Configuring a Host Name 627
Configuring the Displayable Length of the Host Name 627
Viewing the Displayable Length of the Host Name 628
Configuring Tab Title at WebUI Login 628
Configuring System Admin Users 629
Creating Administrator Roles 631
Specifying Administrator Role's Privileges 632
Specifying Administrator Role's Description 632
Creating an Admin User 632
Assigning a Role 633
Configuring Password 633
Configuring Password Policy for Admin Users 634
Viewing Password Policy for Admin Users 636
Configuring the Function of Resetting the Administrator Password by Security Question 637
Configuring Accesses for Admin Users 638
Configuring Single Sign-on (SSO) 639
Enabling/Disabling SSO 639

Specifying the SSO scheme as CAS_QIMING 640
Specifying the SSO Scheme as CTYUN 640
Viewing/Deleting the Token Information of CTYUN 641
Specifying the SSO Scheme as 360_YUNZHEN 641
Viewing the Token Information of 360_YUNZHEN 641
Viewing the SSO Information 641
Configuring Two-factor Authentication for Admin Users Logging in to the WebUI 642
Enabling SMS/Email Two-factor Authentication 642
Configuring the Mobile Number for an Administrator 643
Configuring the Email Address for an Administrator 643
Configuring an API Token for an Administrator 643
Creating an API Token 643
Changing the Validity Period of the API Token 644
Updating the API Token 644
Renewing the API Token 644
Enabling the API Token 644
Disabling the API Token 644
Deleting the API Token 645
Viewing API Token 645
Configuring Log Types for Auditors 646
Specifying Login Limit 647
Configuring the Maximum Number of Admin Users 648

Configuring Login Options for the Default Administrator 649
Enabling Telnet/HTTP Login Type for the Default Administrator 649
Viewing Admin roles 649
Viewing Admin Users 649
VSYS Admin Users 650
Logging in to the Device by Using the API Token 653
Creating an API Token 654
Changing the Validity Period of the API Token 654
Updating the API Token 654
Renewing the API Token 654
Enabling the API Token 654
Disabling the API Token 655
Deleting the API Token 655
Viewing API Token 655
Creating a Trusted Host 656
Creating an IPv6 Trusted Host 657
Viewing Trusted Host IP 658
Configuring NetBIOS Name Resolution 659
Enabling NetBIOS Name Resolution 660
Resolving an IP to NetBIOS Name 660
Clearing NetBIOS Cache 661
Viewing NetBIOS Cache 661

Management of System User 661
Configuring Users 663
Binding an IP/MAC Address to a User 663
Configuring Users in the Local AAA Servers 664
Configuring Password 664
Specifying a User Expiration Date 665
Describing a User 666
Specifying an IKE ID 666
Specifying a User Group 666
Viewing User/User Group Information 667
Configuring a User Group 667
User Going Offline Alarm 668
Creating a User Going Offline Alarm Profile 669
Configuring User Going Offline Alarm Threshold 669
Configuring a User Going Offline Alarm Mode 670
Enabling/Disabling the SNMP Trap Alarm Function 671
Enabling/Disabling the SMS Alarm Function 671
Specifying the SMS Alarm Type 671
Specifying the SMS Gateway 672
Specifying the Mobile Number Used for Receiving Text Messages 673
Enabling/Disabling the Email Alarm Function 673
Specifying the Email Server 673

Specifying the Email Address Used for Receiving Alarm Emails 674
Viewing a User Going Offline Alarm Profile 674
Configuring a Role 675
Creating a Role 675
Creating a Role Mapping Rule 675
Configuring a User Attribute Instance 677
Configuring a Role Combination 679
Configuring a Role Blacklist 679
Viewing Role Information 680
Configuring a MGT Interface 680
Configuring a Console MGT Port 680
Configuring the Baud Rate 680
Configuring Timeout 681
Configuring a Telnet MGT Interface 681
Configuring a SSH MGT Interface 683
Configuring a WebUI MGT Interface 684
Viewing MGT Interface Configuration Information 687
Configuring a Storage Device 688
Formatting a Storage Device 688
Removing a Storage Device 688
Upgrading Database Data 689
Viewing Upgrade Status of Database Data 689

Configuring Storage Management 690
Configuring Threshold Alarm 691
Specifying the Action to Handle Logs Exceeding the Storage Threshold 691
Configuring the Calculated Mode of the Storage Threshold 691
Enabling/Disabling Threshold Alarm 692
Configuring Total Log Storage Threshold 692
Configuring the Log Storage Threshold for Each Type 692
Configuring Storage Threshold of Report 693
Configuring Long-term Monitor Storage Size 693
Configuring a Packet Loss Storage Size 694
Viewing the Configuration of Storage Threshold 694
Managing Configuration Files 694
Managing Configuration Information 694
Viewing Configuration Information 695
Comparing the Differences Between Current Configuration and Current/Backup Start-up Configuration 695
Rolling Back to Previous Configurations 699
Exiting the Configuration Rollback Mode 700
Configuring the Action 701
Deleting a Configuration File 701
Saving Configuration Information 701
Backing up Configuration File Automatically 702

Viewing backing up configuration file automatically Information 703
Exporting Configuration Information 703
Importing Configuration Information 705
Enabling /Disabling Importing Configuration in USB Automatically 706
Restoring Factory Defaults 707
Switching the Working Mode of Fiber-optic Interfaces 708
Switching Mode 709
Configuring the Negotiation Mode of Fiber-optic Interface 710
Enabling/Disabling the Transceiver Module 711
Manually Configuring the Fiber-optic Interface to Negotiate with Peer Port 712
Deleting Configuration Information of Expansion Slots 713
Viewing the Configuration of Current Object 714
Viewing the Information of Optical Module 715
Deleting Configuration Information of a virtual NIC 717
Configuring Banner 718
Configuring the system language 719
System Maintenance and Debugging 719
Ping 720
Traceroute 721
System Debugging 723
Collecting and Saving Tech-support Information to File 724
Viewing the Tech-support Information 724

Viewing the Information of Nvramlog or Watchdoglog File 725
Rebooting the System 725
Rebooting the Device 725
Rebooting the Expansion Module 726
Upgrading StoneOS 727
Upgrading StoneOS via CLI 727
Upgrading StoneOS via FTP Server 727
Upgrading StoneOS via TFTP Server 730
Upgrading StoneOS via FTPS Server 731
Upgrading StoneOS via SFTP Server 732
Upgrading StoneOS via USB Drive 733
Upgrading StoneOS via Sysloader 734
Introduction to the Boot System 734
Physical Connection Requirements for the Device 734
PC Directly Connected to the Firewall via the Console Port 735
PC Connected to the Firewall via a Serial Server 735
Upgrade Procedure 735
Upgrading StoneOS via TFTP Server in Sysloader 736
Upgrading StoneOS via FTP Server in Sysloader 743
Upgrading StoneOS via USB Port in Sysloader 744
Introduction to the Sysloader Menu 745
Upgrading StoneOS by Using Hotfix 747

Importing a Patch File 748
Loading/Activating/Running/Deleting a Patch 750
Viewing the Patch Status 751
Synchronizing the Firmware 751
SCM HA 751
Device HA Switchover When Switch Module failed 752
License Management 753
CloudEdge License 765
CloudEdge Platform Licenses 766
CloudEdge Sub Licenses 767
CloudEdge Function Licenses 769
Applying for a License 771
Installing a License 771
Connecting to License server 772
Managing a License Using CLI 773
Generating a Request for License 773
Installing/Uninstalling a License 773
Verifying the Licenses 774
Viewing License Summary Information 775
Configuring HA Backup Device to Communicate with LMS through Master Device 777
Replacing the Digital Certificate used for Connecting CloudEdge and LMS 777
View LMS Information 778

Batch Installing Licenses 779
Batch Installing Procedure 779
Installing a License 780
Simple Network Management Protocol (SNMP) 781
Hillstone SNMP 781
Supported RFCs 782
Supported MIBs 783
Supported Traps 783
Configuring SNMP 783
Enabling/Disabling the SNMP Agent Function 784
Configuring the SNMP Port Number 785
Configuring SNMP Engine ID 785
Creating an SNMPv3 User Group 785
Creating an SNMPv3 User 786
Configuring the IP Address of the Management Host 787
Configuring Recipient of SNMP Trap 788
Configuring sysContact 789
Configuring sysLocation 789
Specifying the VRouter on Which the SNMP is Enabled 789
Configuring SNMP Server 790
Clearing the ARP Table Information of SNMP Server 790
Viewing the SNMP Server Information 791

Viewing SNMP Information 791
Entering the SNMP Agent Configuration Mode 791
Enabling/Disabling the SNMP OID Statistics Function 791
Viewing SNMP OID Statistics 792
Clearing SNMP OID Statistics 795
Exporting the SNMP MIB File 795
SNMP Configuration Examples 796
Requirements 796
Example 1 797
Example 2 797
Network Configuration Protocol (NETCONF) 799
Enabling/Disabling the NETCONF Agent 800
Enabling/Disabling the NETCONF candidate 801
Configuring the NETCONF Timeout 801
Viewing NETCONF Agent Configuration Information 801
HSM Agent 802
Configuring HSM Agent 802
Changing Digital Certificate 805
Enabling/Disabling HSM Agent 806
Viewing HSM Agent Configuration Information 806
Network Time Protocol (NTP) 806
Configuring NTP 807

Configuring System Clock Manually 807
Configuring Time Zone Manually 807
Configuring Summer Time 808
Viewing System Clock Configuration Information 810
Configuring NTP Service 810
Enabling/Disabling NTP Service 810
Configuring an NTP Server 811
Configuring the Max Adjustment Value 811
Configuring the Query Interval 812
Enabling/Disabling NTP Authentication 812
Configuring NTP Authentication 812
Viewing NTP Status 813
NTP Configuration Example 813
Password-free Login to CLI via WebUI 814
Configuring Maximum Number of Connections for CLI Window 814
Viewing Configuration of CLI Window 815
Configuring Schedule 815
Creating a Schedule 815
Configuring an Absolute Schedule 816
Configuring a Periodic Schedule 816
Configuring a Track Object 818
Viewing the Track Objects Configuration Information 819

Track by ICMP Packets 820
Dynamic Ping Message ID 821
Track by IPv6 ICMP Packets 821
Track by HTTP Packets 822
Track by ARP Packets 823
Track by DNS Packets 824
Track by TCP Packets 824
Track by BFD Packets 825
Interface Status Track 827
Interface Bandwidth Track 827
Interface Quality Track 828
Configuring a Threshold 829
Monitor Object FailureThreshold 829
Fail Close 830
Enabling/Disabling Fail Close 830
Viewing Fail Close Status 830
Enabling/Disabling Application Layer Security Bypass 831
Viewing Application Layer Security Bypass Status 831
Monitor Alarm 831
CPU Cache Error Monitor 834
The Maximum Concurrent Sessions 835
Adjusting the Maximum Concurrent Sessions 847

Connecting to Hillstone Cloud Service Platform 848
Configuring the Cloud Service Platform Server 849
Changing Digital Certificate 850
Enabling CloudView 851
Enabling CloudView 852
Enabling Information Upload 852
Enabling Log Report 852
Enabling Monitoring Data Uploading 854
Enabling Cloud Inspection 855
Enabling the Cloud Configuration 855
Enabling/Disabling Cloud Assets Identification Function 856
Configuring Hillstone CloudVista 856
Entering the CloudVista Configuration Mode 857
Enabling/Disabling IOC Details Cloud Collaborative Query 857
Joining the User Experience Improvement Program 857
Showing Configurations of the Cloud Service Platform 858
Connecting to iSource 859
iSource Typical Deployment 859
Stand-alone Deployment 859
Cluster Deployment 860
Connecting to iSource 861
Enter the iSource Configuration Mode 862

Enabling Connecting to iSource 862
Configuring the IP Address of iSource 862
Configuring the VRouter of iSource 863
Configuring the Data Types Sent to iSource 863
Showing the Configuration of Connecting to iSource 864
Configuring the RESTful API Interface to Upload Files 864
Clearing Alarm Status of Indicators 864
Automatically Clearing Alarm Status of Indicators 865
Specifying the Device as an SSH/Telnet Client 865
Specifying the Device as an SSH Client 865
Specifying the Device as a Telnet Client 866
Switching the Working Mode of SIOM Module 867
Specifying the Maximum Retry Time for Configuration Deployment 868
Enabling/Disabling the Function of IP Fragmented Packets Reassembling in the IOM/SIOM Module 869
Viewing the Temperature, Fan, and Power Supply Information of the Device 870
Viewing the CPU Utilization of the Device 871
Viewing Information about MAC Table 871
Viewing Information about MAC Table 871
Clearing MAC Table Information 872
Managing SSH Algorithms 872
Disabling a Specified SSH Algorithm 872

Re-enabling an SSH Algorithm 872
Viewing Disabled SSH Algorithms 873
Chapter 5 Virtual System (VSYS) 874
VSYS Objects 874
Root VSYS and Non-root VSYS 874
Administrator 875
VRouter, VSwitch, Zone, Interface 878
Shared VRouter 879
Shared VSwitch 880
Shared Zone 880
Shared Interface 880
Interface Configuration 880
Configuring VSYS 880
Creating a Non-root VSYS 881
Configure the Alias of Non-root VSYS 881
Specifying the Description for VSYS 882
Creating a VSYS Profile 882
Configuring Resource Quota 884
Configuring the Quota of Log Buffer 886
Configuring URL Filter 886
Configuring IPS 887
Configuring Anti-Virus 888

Configuring Perimeter Traffic Filtering 889
Configuring QoS 890
Configuring Botnet Prevention 890
Entering the Botnet Prevention Configuration Mode 890
Enabling or Disabling the Botnet Prevention Function 891
Configuring the Quota of Botnet Prevention Profile Resource in VSYS 891
Enabling/Disabling the CPU Resource Quota 891
Binding a VSYS Profile to a VSYS 892
Entering the VSYS 892
Configuring the Shared Property 895
Exporting a Physical Interface 895
Allocating a Logical Interface 896
Binding a Track Object 896
Monitoring a Specified VSYS 897
Rolling Back to Previous Configurations 898
Exiting the Configuration Rollback Mode 899
Configuring the Action 900
Configuring VSYS Log 900
Configuring Cross-VSYS Traffic Forwarding 901
Enabling/Disabling the Cross-VSYS Traffic Forwarding 901
Configuring a Simple-Switch 902
Creating a Simple-Switch 902

Binding the L2 Zone to the Simple-Switch 902
Creating a VWANIF interface 903
Creating a VPort Interface 903
Configuring the VWANIF Interface 904
Allocating a VWANIF Interface 904
Viewing Cross-VSYS Traffic Forwarding Information 904
Viewing the VWANIF interface Configuration Information 904
Viewing the VWANIF Interface IPv6 Configuration Information 904
Viewing VSYS Information 905
Viewing VSYS Profile Information 905
VSYS Configuration Examples 905
Example 1: L3 Traffic Transmitting in a Single VSYS 906
Configuration Steps 906
Example 2: L3 Traffic Transmitting among Multiple VSYSs via Shared VRouters 908
Configuration Steps 909
Example 3: L2 Traffic Transmitting among Multiple VSYSs via Shared VSwitch 913
Configuration Steps 914
Example 4: Traffic transmitting among multiple VSYSs via Simple-Switch 918
Configuration Steps 919
Chapter 6 High Availability (HA) 923
Overview 923
HA Cluster 924

HA Group 924
HA Node 925
HA Group Interface and Virtual MAC 925
HA Selection 925
HA Synchronization 925
Limits on Configuring NAT in HA Scenario 927
Configuring HA 927
Configuring an HA Group 928
Specifying the Priority 929
Specifying the Hello Interval 929
Specifying the Hello Threshold 930
Specifying the Hello Packet Transport Protocol 930
Configuring the Preempt Mode 931
Specifying the Gratuitous ARP Packet Number 931
Sending Gratuitous ARP Packets 932
Specifying the Description 932
Specifying the Track Object 933
Configuring an HA group interface 933
Configuring the Next-hop IP Address of the Interface 935
Configuring SNAT Port Distribution 935
Configuring a HA Link 936
Specifying an HA Link Interface 937

Specifying the Work Mode of HA Link Interface 938
Specifying the IP Address of HA link 939
Specifying an HA Assist Link Interface 939
Specifying the MAC Address of HA Link Interface on ClouldEdge 940
Enable the Real MAC Address of Interface On CloudEdge 941
Configuring a Custom HA MAC Address 942
Configuring HA Negotiation through Two Layer Unicast Mode 942
Specifying the MTU Value of HA link Interface 943
Configuring a HA Cluster 943
Configuring HA VMAC Prefix 944
Viewing HA VMAC Prefix 945
Configuring HA Base Virtual MAC 945
Viewing HA Base Virtual MAC 946
Configuring a Management IP 946
Configuring Local Property 947
Configuring the Layer 3 Port Down-up Function 947
Manually Synchronizing HA Information 948
HA Full Synchronization 952
Enabling/Disabling Automatic HA Session Synchronization 953
Enabling/Disabling Scheduled Comparison of HA Configurations 953
Manually Switching Main and Backup Device Status of HA 954
Configure the Deployment Mode of HA on Cloudplatform 954

Specifying the Cloud platform of HA deploying 955
Viewing the HA Cloud Deployment Information 955
Specifying the AccessKey of Cloud Platform 955
Checking the Connectivity to Cloud Platform API 956
Verifying the Access ID and Password of the Cloud platform 956
Viewing the AccessKey of Cloud Platform 956
Enabling/Disabling Platform Checking of HA devices 956
Viewing the Status of HA Platform checking 957
Configuring HA Traffic 957
Enabling HA Traffic 958
Configuring HA Traffic Delay 958
Configuring First Packet Forwarding 959
Configuring First Packet Forwarding Bounce Back 959
Configuring HA Route Rematch by Session 960
Viewing HA Configuration 962
Enabling HAVIP function that Alibaba Cloud provides to deploy HA 963
Configuring the Accesskey of Alibaba Cloud 963
HSVRP 964
Typical Scenario 964
Basic Concepts 965
HSVRP Group 965
Referencing an HSVRP Group by an Interface 965

HSVRP Group Status 966
Configuring HSVRP 967
Creating an HSVRP Group 967
Configuring the Virtual IP Address of an HSVRP Group 968
Viewing an HSVRP Group 969
Referencing an HSVRP Group by an Interface 970
VRRP 971
Basic Principle and Concept 972
Scenario 974
Master-Backup Redundancy 974
Load Balancing 975
Configuring VRRP 976
Configuring the VRRP Backup Group 977
Configuring the Virtual IP Address of the VRRP Backup Group 977
Configuring the Preempt Mode 978
Specifying the Priority 978
Configuring the Interval of Sending VRRP Advertisement Messages 978
Bind the VRRP Backup Group to Interface 979
Configuring the Checksum Calculation Method for VRRP Messages 980
Viewing Information about VRRP Backup Group 981
Twin-mode HA 983
Introduction 983

Twin-mode HA Deployment Scenarios 984
Twin-mode HA Synchronization 986
Configuring Twin-mode HA 987
Specifying the deployment mode and synchronization mode 988
Specifying the Node 989
Specifying the Priority 989
Configuring the Preempt Mode 990
Specifying the Hello Interval 990
Specifying the Hello Threshold 991
Configuring Twin-mode HA Link 991
Specifying a Twin-mode HA Link Interface 991
Specifying the IP Address of Twin-mode HA link Interface 992
Specifying the Peer IP Address 993
Enabling/Disabling Twin-mode HA 993
Specifying the Forwarding Mode of Asymmetric Traffic 994
Configuring Twin-mode HA First Packet Forwarding Bounce Back 994
Configuring Twin-mode HA Gateway 995
Configuring the Switching Mode of Twin-mode HA Session State 996
Manually Synchronizing Twin-mode HA Configuration Information 997
Viewing/Clearing the Transfer Packet Count of Twin-mode HA 997
Viewing Twin-mode HA Configuration 997
Examples of HA 999

Example 1: Example of HA in A/P Mode 999
Requirement 999
Configuration Steps 999
Example 2: Example of HA Peer Mode and HA Traffic 1003
Requirement 1003
Configuration Steps 1004
Chapter 7 IPv6 1008
Configuring an IPv6 Address 1009
Specifying a Global IPv6 Address 1010
Configuring an IPv6 General Prefix 1010
Specifying Address Auto-config 1011
Specifying an EUI-64 Address 1011
Specifying a Link-local Address 1012
Specifying an IPv6 MTU 1012
Viewing IPv6 Configuration 1013
Configuring IPv6 Neighbor Discovery Protocol 1013
Configuring DAD 1014
Specifying Reachable Time 1015
Specifying RA Parameters 1015
Specifying a Hop Limit 1015
Advertising MTU 1015
Specifying DNS Configuration Options 1016

Specifying an Auto-config Type Flag 1017
Specifying an IPv6 Prefix and Parameters 1018
Specifying a RA Interval 1019
Specifying RA Lifetime 1019
Specifying DRP 1020
Configuring RA Suppress on LAN Interfaces 1020
Adding/Deleting a IPv6 Neighbor Cache Entry 1021
IPv6 System Management 1022
Configuring IPv6 SNMP 1024
Configuring an IPv6 Management Host 1024
Configuring an IPv6 Trap Destination Host 1025
Creating an SNMPv3 User 1026
Configuring IPv6 Debugging 1027
Configuring IPv6 Routing 1027
Configuring an IPv6 DBR Entry 1027
Configuring an IPv6 SBR Entry 1028
Configuring an IPv6 SIBR Entry 1029
Configuring an IPv6 DIBR Entry 1031
Viewing IPv6 Routing Information 1032
Configuring RIPng 1032
Basic Options 1033
Specifying a Default Metric 1033

Specifying a Default Distance 1034
Specifying a Timer 1034
Configuring the Default Information Originate 1035
Configuring Redistribute 1035
Configuring a Network 1036
Configuring a Passive IF 1036
Configuring Split Horizon 1037
Configuring Poison Reverse 1037
Viewing RIPng Information 1037
Configuring OSPFv3 1038
Configuring a Router ID 1040
Enabling Encryption and Authentication for an Area and on an Interface 1040
Enabling AH Authentication for an Area 1042
Enabling AH Authentication on an Interface 1042
Enabling ESP Authentication for an Area 1043
Enabling ESP Authentication on an Interface 1044
Configuring the Virtual Link for an Area 1044
Configuring the Default Metric 1045
Configuring the Default Administrative Distance 1045
Configuring the Default Information Originate 1046
Configuring the Interface Area and Instance 1046
Configuring Redistribute 1047

Configuring a Passive Interface 1048
Configuring the Timer for an Interface 1048
Configuring the Router Priority for an Interface 1049
Configuring the Link Cost for an Interface 1050
Configuring the MTU Check for an Interface 1051
Configuring the Network Type for an Interface 1051
Disabling or Enabling OSPFv3 1051
Viewing OSPFv3 Information 1052
Configuring IPv6 BGP 1054
Entering the IPv6 Unicast Routing Configuration Mode 1055
Configuring IPv6 Unicast Route Redistribute 1055
Activating a BGP Connection 1055
Sending Community Path Attributes to a Peer/Peer Group 1056
Specifying Upper Limit of Prefixes 1056
Viewing BGP Routing Information 1057
Configuring IPv6 Policy-based Route 1058
Creating a PBR Policy 1058
Creating a IPv6 PBR Rule 1058
Configuring IPv6 IS-IS 1060
Enabling IPv6 IS-IS at interfaces 1061
Configuring the Interface Metric 1062
Entering into the IPv6 Unicast Routing Configuration Mode 1062

Configuring the Default Route Advertisement 1062
Configuring the Administrative Distance 1063
Configuring Redistribute 1063
Configuring the Overload Bit 1064
Configuring the SPF Calculation Interval 1064
Configuring Multiple-Topology Routing 1065
Viewing IPv6 IS-IS Information 1065
Configuring IPv6 Static Multicast Routing 1066
Configuring an IPv6 Static Multicast Route Entry 1066
Specifying an Ingress/Egress Interface 1066
Viewing IPv6 Multicast Route Information 1067
Viewing IPv6 Multicast FIB Information 1068
Configuring IPv6 BFD 1068
Configuring the Source IP Address of the Echo Packets 1069
Integrating BFD with the IPv6 Static Route 1069
Integrating BFD with the OSPFv3 Route 1070
Viewing IPv6 BFD Session Information 1070
Configuring IPv6 DHCP 1071
Configuring a DHCP Client 1071
Obtaining an IPv6 address via DHCP 1071
Releasing and Renewing the IPv6 Address 1072
Configuring a DHCP Server 1072

Basic Configuration of the DHCP Address Pool 1073
Configuring an IP Range 1073
Configuring Domain Name for the DHCP Client 1073
Configuring DNS Servers for the DHCP Client 1074
Binding the Address Pool to an Interface 1074
Configuring a DHCP Relay Proxy 1075
Enabling DHCP Relay Proxy on an Interface 1075
Specifying the IP Address of the DHCP Server 1075
Viewing DHCP Configuration Information 1076
Configuring IPv6 DNS 1076
Configuring a IPv6 DNS Proxy Rule 1076
Specifying IPv6 Source Address 1077
Specifying IPv6 Destination Address 1078
Configuring IPv6 DNS Proxy Servers 1078
Configuring IPv6 DNS Servers 1079
Configuring an IPv6 DNS Proxy Server List 1079
Enabling/Disabling IPv6 DNS Proxy 1080
Adding a Static IPv6 DNS Mapping Entry 1080
Clearing a Dynamic IPv6 DNS Mapping Entry 1081
Viewing IPv6 DNS Mapping Entries 1081
Viewing IPv6 DNS Configuration 1082
Configuring PMTU 1082

Configuring User-defined Application 1083
Creating/Deleting the User-defined Applications 1084
Enabling the User-defined Application Signature Configuration Mode 1084
Enabling the Application Signature Rule Configuration Mode 1084
Configuring IPv6 Source Address 1085
Configuring IPv6 Destination Address 1085
Configuring a User-defined ICMPv6 Application Rule 1085
Configuring an IPv6 Policy Rule 1086
Configuring an IPv6 Address Entry 1086
Configuring an IPv6 Service 1087
Configuring an Action for IPv6 Policy Rule 1088
Configuring an IPv6 Policy Rule 1088
Editing an IPv6 Policy Rule 1090
Configuring Access Control for an IPv6 Policy 1091
Configuring an ACL Profile 1091
Configuring an Access Control Rule 1091
Configuring the Default Action 1093
Binding the ACL Profile to a Policy Rule 1093
Viewing ACL Profile Information 1093
Configuring IPv6 ALG 1094
NDP Protection 1094
IP-MAC Binding 1095

Adding a Static IP-MAC Binding Entry 1096
One-click Binding 1096
Permitting Static IP-MAC Binding Hosts Only 1096
Viewing IP-MAC Binding Information 1097
Clearing Dynamic IP-MAC Binding Information 1097
NDP Learning 1098
NDP Learning Limit 1098
NDP Inspection 1099
Enabling/Disabling NDP Inspection 1099
Configuring a Trusted Interface 1099
Denying RA Packets 1100
Configuring an NDP Packet Rate Limit 1100
Viewing NDP Inspection Configuration 1101
Configuring NDP Spoofing Defense 1101
Viewing NDP Spoofing Statistics 1102
NDP Spoofing Prevention 1102
Configuring the Aging Time of ND Table Entries 1102
Enabling/Disabling Validity Detection for Aged ND Table Entries 1103
Attack Defense 1103
IPv6 over IPv4 Tunnel 1105
Configuring an Automatic 6to4 Tunnel 1105
Creating a Tunnel 1106

Specifying IPv6 6to4 Subtunnel Limit 1106
Specifying an Egress Interface 1107
Binding an IPv6 Automatic 6to4 tunnel to the Tunnel Interface 1107
Showing Configuration Information About IPv6 Automatic 6to4 Tunnel 1107
Configuring a Manual 6to4 Tunnel 1108
Creating a tunnel 1108
Specifying an Egress Interface 1108
Specifying a Destination Address for the Manual Tunnel 1109
Binding an IPv6 Manual 6to4 tunnel to the Tunnel Interface 1109
Showing Configuration Information About IPv6 Manual 6to4 Tunnel 1110
IPv4 over IPv6 Tunnel 1110
Configuring a Manual 4to6 Tunnel 1110
Creating a tunnel 1111
Specifying the Source Address/Egress Interface 1111
Specifying a Destination Address for the Tunnel 1111
Binding an IPv6 manual 4to6 Tunnel to the Tunnel Interface 1112
Showing the Configuration Information About the IPv6 Manual 4to6 Tunnel 1112
Configuring a 6RD Tunnel 1112
Creating a 6RD Tunnel 1114
Specifying an Egress Interface of the 6RD Tunnel 1114
Specifying a 6RD Prefix 1114
Specifying the IPv4 Prefix Length 1115

Configuring the BR's IPv4 Address 1115
Specifying 6RD Subtunnel Limit 1116
Binding the 6RD Tunnel to a Tunnel Interface 1116
Showing the Configuration Information About the 6RD Tunnel 1116
Configuring an ISATAP Tunnel 1118
Creating an ISATAP Tunnel 1119
Specifying ISATAP Subtunnel Limit 1119
Specifying an Egress Interface of ISATAP Tunnel 1119
Binding an ISATAP tunnel to the Tunnel Interface 1120
Showing Configuration Information About the ISATAP Tunnel 1120
Configuring a DS-lite Tunnel 1120
Creating a DS-lite Tunnel 1121
Specifying an Interface and IP Address for the DS-lite Tunnel 1121
Specifying DS-lite Subtunnel Limit 1122
Binding a DS-lite Tunnel to the Tunnel Interface 1122
Showing Configuration Information About the DS-lite Tunnel 1122
Configuring NAT-PT 1122
Configuring a NAT-PT Rule 1123
Creating an SNAT Rule 1124
Moving an SNAT Rule 1126
Deleting an SNAT Rule 1127
Viewing SNAT Configuration Information 1127

Creating a DNAT Rule 1127
Moving a DNAT Rule 1129
Deleting a DNAT Rule 1130
Viewing DNAT Configuration Information 1130
Configuring DNS64 and NAT64 1131
Enabling/Disabling DNS64 1131
Configuring DNS64 Server 1132
Configuring DNS64 Prefix 1132
Creating a DNS64 Rule 1132
Creating a DNAT Rule 1133
Configuring a IPv6 Track Object 1134
Track by IPv6 ICMP Packets 1135
Track by IPv6 HTTP Packets 1136
Track by IPv6 DNS Packets 1137
Track by NDP Packets 1138
Track by IPv6 TCP Packets 1138
IPv6 Configuration Examples 1139
Example 1: IPv6 Transparent Mode Configuration 1140
Example 2: IPv6 Routing Mode Configuration 1142
Example 3: IPv6 Manual 6to4 Tunnel Configuration 1144
Example 4: IPv6 Automatic 6to4 Tunnel Configuration 1148
Example 5: IPv6 SNMP Configuration 1153

Viewing IPv6 MIB Information via an IPv4 Network 1154
Viewing IPv6 MIB Information via an Ipv6 Network 1154
Example 6: IPv6 NAT-PT Configuration 1155
Requirement 1 1156
Requirement 2 1157
Example 7: IPv6 DNS64 and NAT64 Configuration 1159
Appendix 1: ICMPv6 Type and Code 1161
Chapter 8 User Authentication 1166
Authentication, Authorization and Accounting 1167
Overview 1167
External Authentication Procedure 1168
Configuring an AAA Server 1168
Creating an AAA Server 1169
Configuring a Local Authentication Server 1170
Configuring the Account Control 1170
Configuring the Password Control 1171
Allowing Password Change by Local Users 1172
Configuring Change Password after First Login 1172
Configuring the Password Validity and Password Expiry Warning 1173
Configuring the History Password Check 1173
Configuring the Password Complexity 1174
Specifying User Name Format 1175

Configuring a Role Mapping Rule 1176
Configuring a User Blacklist 1176
Configuring a Backup Authentication Server 1176
Configuring the Brute-force Cracking Defense 1177
Enabling/Disabling the Brute-force Cracking Defense 1177
Configuring the Number of Attempts 1178
Configuring the Lockout Time 1178
Viewing the Lockout Information 1178
Unlocking the User / IP 1179
Configuring a RADIUS Authentication Server 1179
Configuring LOCAL NAS IP for RADIUS Authentication 1180
Configuring the IP Address, Domain Name, or VRouter of the Primary Server 1181
Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1 1181
Configuring the IP Address, Domain Name, or VRouter of the Backup Server 2 1182
Configuring the Port Number 1182
Configuring the Secret 1182
Configuring the Retry Times 1183
Configuring the Timeout 1183
Specifying User Name Format 1184
Specifying a Role Mapping Rule 1184
Configuring the Brute-force Cracking Defense 1185
Enabling/Disabling the Brute-force Cracking Defense 1185

Configuring the Number of Attempts 1185
Configuring the Lockout Time 1186
Viewing the Lockout Information 1186
Unlocking the User / IP 1186
Configuring a User Blacklist 1187
Configuring a Backup Authentication Server 1187
Enabling / Disabling the Authentication Policy 1188
Adding Authentication Policy to Aggregate Policy 1189
Importing Dictionary 1189
Configuring an Active-Directory Authentication Server 1191
Configuring the IP Address, Domain Name, and VRouter of the Primary Server 1193
Configuring the IP Address, Domain Name, VRouter of the Backup Server 1 1193
Configuring the IP Address or Domain Name of the Backup Server 2 1194
Configuring the Port Number 1194
Configuring the Authentication or Synchronization Method 1195
Specifying the Base-DN 1195
Specifying the Synchronization Base-DN 1196
Specifying the Synchronization Object 1196
Specifying the Authentication Base-DN 1197
Specifying the Login DN 1197
Specifying sAMAccountName 1198
Specifying the Login Password 1198

Specifying the Mobile Number Attribute Name 1198
Specifying the Email Attribute Name 1199
Enabling/Disabling the SSL Encrypted Connection 1199
Specifying User Name Format 1199
Specifying a Role Mapping Rule 1200
Configuring a User Blacklist 1200
Configuring an LDAP User 1201
Configuring User Expiration 1201
Configuring the Brute-force Cracking Defense 1201
Enabling/Disabling the Brute-force Cracking Defense 1202
Configuring the Number of Attempts 1202
Configuring the Lockout Time 1203
Viewing the Lockout Information 1203
Unlocking the User / IP 1203
Configuring an AD User 1204
Configuring User Expiration 1204
User Synchronization 1204
Enable or Disable User Synchronization 1204
Configuring User Synchronization 1205
Specifying Naming Attribute 1206
Specifying Group Class 1206
Specifying User Class 1207

Configuring User Filter 1207
Configuring Synchronization Mode of User Information 1208
Configuring a Backup Authentication Server 1209
Configuring the User-Groups under Base-DN Synchronization 1210
Enabling/Disabling Authentication Simplification 1211
Configuring an LDAP Authentication Server 1211
Configuring the IP Address, Domain Name, or VRouter of the Primary Server 1213
Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1 1213
Configuring the IP Address, Domain Name, VRouter of the Backup Server 2 1214
Configuring the Port Number 1214
Configuring the Authentication or Synchronization Method 1215
Specifying the Base-DN 1215
Specifying the Synchronization Base-DN 1216
Specifying the Synchronization Object 1216
Specifying the Authentication Base-DN 1216
Specifying the Login DN 1217
Specifying Authid 1217
Configuring the Login Password 1218
Enabling/Disabling the SSL Encrypted Connection 1218
Specifying the Name Attribute 1218
Specifying the Group Name Attribute 1219
Specifying the Group-class 1219

Specifying User Class 1219
Specifying the Member Attribute 1220
Specifying the Mobile Number Attribute Name 1220
Specifying the Email Attribute Name 1221
Specifying User Name Format 1221
Specifying the Mobile Attribute field 1222
Specifying a Role Mapping Rule 1222
Configuring a User Blacklist 1222
Configuring the Brute-force Cracking Defense 1223
Enabling/Disabling the Brute-force Cracking Defense 1223
Configuring the Number of Attempts 1223
Configuring the Lockout Time 1224
Viewing the Lockout Information 1224
Unlocking the User / IP 1224
User Synchronization 1225
Enable or Disable User Synchronization 1225
Configuring User Synchronization 1225
Configuring User Filter 1226
Configuring Synchronization Mode of User Information 1227
Configuring a Backup AAA Server 1228
Enabling/Disabling Authentication Simplification 1229
Configuring TACACS+ Authentication Server 1230

Configuring IP or Domain Name of Primary Authentication Server 1230
Configuring IP Address or Domain Name of Backup Server 1 1231
Configuring IP Address or Domain Name of Backup Server 2 1231
Configuring Port Number of TACACS+ Server 1232
Configuring Secret of TACACS+ Server 1232
Specifying User Name Format 1232
Specifying Role Mapping Rule 1233
Configuring TACACS+ Server 1233
Configuring the Brute-force Cracking Defense 1235
Enabling/Disabling the Brute-force Cracking Defense 1236
Configuring the Number of Attempts 1236
Configuring the Lockout Time 1236
Viewing the Lockout Information 1237
Unlocking the User / IP 1237
Configuring an OAuth2 Authorization Server 1237
Basic Configuration 1238
Specifying the Organization Source Server 1238
Specifying the Virtual Router to which the OAuth2 Server Belongs 1238
Specifying the Name of the OAuth2 Authentication Icon 1239
Get Authorization Code Configuration 1239
Entering the Authorization Code Request Configuration Mode 1239
Configuring the OAuth2 Server URL of the Authorization Code Request 1240

Configuring client_id 1240
Configuring redirect_uri 1240
Configuring the Response Type of the Authorization Code Request 1241
Configuring Custom Attribute of the Authorization Code Request 1241
Configuring the Response Parameter of the Authorization Code 1242
Get Access Token Configuration 1242
Entering the Access Token Request Configuration Mode 1242
Configuring the URL of the OAuth2 Server from which the System Requests an Access Token 1243
Configuring grant_type 1243
Configuring code 1244
Configuring redirect_uri 1244
Configuring Custom Attribute of the Access Token Request 1245
Configuring the Response Parameter of the Access Token 1245
Get User Information Configuration 1246
Entering the User Information Request Configuration Mode 1246
Configuring the OAuth2 Server URL of the User Information Request 1246
Configuring Custom Attribute of the User Information Request 1246
Configuring the Response Parameter of User Information 1247
Viewing Configuration Information about the Oauth2 Server 1247
Configuring a RADIUS Accounting Server 1249
Enabling/Disabling the Accounting Function 1250

Configuring the IP Address or Domain Name of the Primary/Backup Server 1250
Configuring the Port Number 1251
Configuring the Secret 1251
Enabling/Disabling the Offline Management of Accounting User 1251
Configuring the Extended Password Encryption Algorithm of SM4 1252
Configuring Authentication and Authorization for the Server 1252
Configuring Authentication and Authorization for the Server 1253
Viewing the Authorization Information of the Authentication Server 1254
Viewing Local Server Authentication Enabled Status 1254
Configuring the Authentication Server for the administrator 1254
Viewing and Debugging AAA 1255
Radius Dynamic Authorization 1256
Enabling / Disabling Radius dynamic authorization 1256
Configuring a Radius Dynamic Authorization Server 1256
Configuring the Port Number 1257
Viewing Radius Dynamic Authorization Server Configurations 1257
Radius Snooping 1258
Entering the Radius Snooping Configuration Mode 1258
Enabling the Radius Snooping Function 1258
Specifying the AAA Server 1258
Configuring the Idle Time 1259
Specifying the Force Timeout Time 1259

Configuring the Heartbeat Timeout Value 1260
Configuring the Username Filter 1260
Viewing the Radius Snooping Configuration Information 1261
Configuration Example 1261
Requirement 1261
Configuration Steps 1261
User Identification 1264
Overview 1264
Web Authentication 1264
Entering the WebAuth Configuration Mode 1264
Enabling/Disabling WebAuth 1264
Configuring the WebAuth Mode 1265
Configuring the Single Authentication Mode 1265
Configuring the Combined Authentication Mode 1266
Configuring the Protocol Type of Authentication 1267
Specifying the WebAuth Global Default Configuration of Interface 1267
Configuring the Port Number 1267
Specifying HTTP Proxy Server Port 1268
Configuring the HTTPS Trust Domain 1269
Specifying the HTTPS Certificate Chain 1269
Specifying the Address Type 1270
Configuring Multi-logon Function 1271

Configuring Auto-kickout Function 1271
Enabling/Disabling Proactive WebAuth 1272
Enabling/Disabling the WebAuth of Interface 1273
Configuring the WebAuth Domain Name 1274
Disconnecting a User 1274
Allowing Password Change by Local Users 1275
Configuring a Policy Rule for WebAuth 1277
Customizing WebAuth Login Pages 1278
Customizing the Login Page 1278
Exporting the Login Page 1280
Password Authentication 1280
Configuring the Re-auth Interval 1280
Configuring the Redirect URL Function 1281
Configuring the Forced Timeout Value 1282
Configuring the Idle Timeout Value 1282
Configuring the Heartbeat Timeout Value 1283
SMS Authentication 1284
Configuring the Forced Timeout Value 1284
Configuring the Idle Timeout Value 1284
Configuring the Verification Code Interval 1285
Specifying the Sender Name or Sign Name 1285
Configuring the Verification Code Length 1286

Specifying the Template Code 1286
Specifying SMS Modem to Send SMS 1287
Specifying SMS Gateway to Send SMS 1287
NTLM Authentication 1287
Configuring Forced Timeout Value 1287
Using the Compatibility Mode 1288
Configuring the Idle Timeout Value 1288
OAuth2 Authentication 1289
Enabling/Disabling the OAuth2 Authentication Mode 1289
Binding the OAuth2 Server 1289
Configuring the Forced Timeout Period of OAuth2 Authentication 1290
Configuring the Heartbeat Timeout Period of OAuth2 Authentication 1290
Configuring the Idle Timeout Period of OAuth2 Authentication 1291
Viewing the WebAuth Configuration Information 1291
Viewing the Online User Information 1291
Single Sign-On 1292
Configuring AD Scripting for SSO 1292
Entering the AD Scripting Configuration Mode 1292
Enabling the AD Scripting Function 1292
Specifying the AAA Server 1293
Configuring the Idle Time 1293
Configuring Simultaneously Online Settings 1294

Viewing Configuration Information 1294
Viewing the User Mapping Information 1294
Viewing the Authenticated User Table 1294
Deleting the User Mapping Information 1295
Configuring SSO Radius for SSO 1295
Receiving Radius Accounting Packets 1295
Specifying the AAA Server 1295
Specifying the Port Number for Receiving Radius Packets 1296
Configuring the Radius Client 1296
Configuring the Shared Secret 1297
Configuring the Heartbeat Timeout 1297
Configuring Idle Timeout 1297
Configuring Forced Timeout 1298
Viewing the SSO Radius Configuration Information 1298
Viewing the User Mapping Information 1299
Viewing the Authentication User Table 1299
Deleting the User Mapping Information 1299
SSO via Agile Controller 1299
Entering the Agile Controller Configuration Mode 1299
Enabling/Disabling Agile Controller 1299
Specifying the Port for StoneOS to Receive Agile Controller Packets 1300
Specifying the AAA Server 1300

Specifying Query Address Range 1300
Specifying the Query Rate 1301
Specifying the Query Interval 1301
Specifying the Maximum IPs Queried Each Time 1301
Specifying Forced Timeout 1302
Configuring an Agile Controller Client 1302
Specifying the IP Address of the Agile Controller Server 1302
Configuring the Shared Key 1303
Configuring the Encryption Algorithm 1303
Enabling/Disabling Active Query 1304
Displaying Configuration Information of the Agile Controller 1304
Configuring AD Polling for SSO 1304
Creating an AD Polling Profile 1304
Enabling / Disabling the AD Polling Function 1305
Specifying the Authentication Server 1305
Specifying the AAA Server 1305
Specifying the Account 1306
Specifying the Password 1306
Specifying the AD Polling Interval 1307
Specifying the Client Probing Interval 1307
Specifying the Force Timeout Time 1307
Viewing the AD Polling Configuration 1308

Viewing the User Mapping Information 1308
Viewing the Authenticated User Table 1308
Deleting the User Mapping Information 1308
Configuring SSO Monitor for SSO 1309
Creating SSO Monitor Profile 1309
Enabling/Disabling the SSO Monitor Function 1310
Configuring User Address 1310
Specifying the External Server 1310
Specifying the AAA Server 1311
Specifying the Port 1312
Specifying the Organization Source 1312
Specifying the Disconnection Timeout 1313
Specifying Forced Timeout of SSO Monitor 1313
Viewing the SSO Monitor Configuration 1314
Viewing the User Mapping Information 1314
Viewing the Authentication User Table 1314
Deleting the User Mapping Information 1315
Configuring TS Agent for SSO 1315
Creating TS Agent Profile 1315
Enabling / Disabling the TS Agent Function 1316
Specifying the TS Agent Server 1316
Specifying the TS Agent Port 1316

Specifying the AAA Server 1317
Specifying the Disconnection Timeout 1317
Specifying the Traffic IP 1318
Viewing the TS Agent Configuration 1318
Viewing the TS Agent Status 1318
Viewing the User Mapping Information 1319
Viewing the Authentication User Table 1319
Deleting the User Mapping Information 1319
SSO Web for SSO 1319
Typical Scenarios of SSO Web for SSO 1319
Configuring SSO Web for SSO 1321
Configuring SSO Web 1321
Entering the SSO Web Configuration Mode 1321
Enabling the SSO Web Function 1321
Specifying the AAA Server 1322
Configuring Forced Timeout 1322
Specifying IP Range of Trusted Client 1322
Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System 1323
Viewing Configuration Information 1325
Viewing the Authenticated SSO Web 1325
Viewing the SSO Web User Mapping Information 1325

Kicking out SSO Web User 1326
Portal Authentication 1326
Configuring a Policy Rule that Triggers the Portal Authentication 1327
Example of Configuring WebAuth 1327
Example of Configuring HTTP WebAuth 1327
Example of Configuring NTLM Authentication 1330
Example of Configuring SSO 1331
Example of Configuring AD Scripting for SSO 1331
Example of configuring AD Polling for SSO 1336
Configuration Examples of Using SSO Monitor for SSO 1337
Configuration Examples of SSO Radius Login 1342
Example of Configuring TS Agent for SSO 1343
Example of Configuring Agile Controller for SSO 1345
Example of Configuring SSO Web for SSO 1346
Procedure of SSO Web for SSO 1347
Configuration Steps 1347
Example of Configuring Portal Authentication 1351
802.1X Authentication 1355
Overview 1355
802.1X Architecture 1355
802.1X Authentication Process 1356
Authenticating by EAP-MD5 Method 1356

Authenticating by EAP-TLS Method 1357
Configuring 802.1X Authentication 1357
Configuring an 802.1X Profile 1358
Configuring the Maximum Retry Times 1358
Configuring the Re-auth Period 1358
Configuring the Quiet Period 1359
Configuring the Client Timeout 1359
Configuring the Server Timeout 1360
Specifying the 802.1X Authentication Server 1360
Configuring 802.1X Attributes on Port 1361
Enabling/Disabling 802.1X Authentication 1361
Binding 802.1X Profile to a Port 1361
Configuring the Port Access Control Mode 1361
Configuring the Port Access Control Method 1362
Configuring 802.1X Global Parameters 1362
Configuring the Maximum User Number 1362
Configuring the Timeout of Authenticated Clients 1363
Configuring Multi-logon Function 1363
Configuring Auto-kickout Function 1363
Configuring Manual Kick-out Client 1364
Viewing 802.1X Configurations 1364
PKI 1365

Overview 1365
PKI Function of Hillstone Devices 1366
Configuring PKI 1366
Generating/Deleting a PKI Key Pair 1367
Configuring a PKI Trust Domain 1368
Specifying an Enrollment Type 1368
Specifying a Key Pair 1369
Configuring Subject Content 1369
Adding the Subject Alternative Name 1370
Configuring a CRL 1371
Configuring Online Certificate Status Protocol 1372
Specifying the OCSP Responder 1373
Configuring the Random Number for OCSP Requests 1373
Specifying the Invalidity Time for OCSP Response Information 1374
Importing a CA Certificate 1374
Importing a Key 1375
Importing a Key Pair 1375
Generate a Certificate Request 1376
Importing a Local Certificate 1376
Obtaining a CRL 1377
Importing/Exporting a PKI Trust Domain 1377
Exporting the PKI Trust Domain Information 1377

Importing the PKI Trust Domain Information 1378
Importing a Trust Certificate 1379
Exporting/Importing a Local Certificate 1380
Exporting a Local Certificate 1380
Importing a Local Certificate 1381
Importing Customized Certificate for HTTPS WebAuth 1382
Importing Customized Certificate 1382
Viewing Importing Customized Certificate Information 1383
Certificate Expiry Configurations 1383
Viewing the PKI Configuration Information 1384
Configuring a Certificate Chain 1384
Creating a Certificate Chain 1384
Importing a Certificate Chain 1385
Exporting a Certificate Chain 1386
Viewing Certificate Chain Information 1386
Configuring Certificate Validity Check 1387
Enabling/Disabling Certificate Validity Check 1387
Configuring Certificate Validity Check 1387
Viewing Check Configuration and Check Result of Certificate Validity 1387
Example for Configuring IKE 1388
Requirement 1388
Configuration Steps 1389

Chapter 9 VPN 1397
IPsec Protocol 1398
Overview 1398
Security Association 1398
Establishing a SA 1399
Phase 1 SA 1399
Phase 2 SA 1400
Hash Algorithm 1401
Encryption Algorithm 1402
Compression Algorithm 1402
References 1402
Applying an IPsec VPN 1403
Configuring an IPsec VPN 1403
Improving the Decrypting Performance of IPSec VPN 1404
Improving the New Session Processing Performance of IPSec VPN 1404
Configuring the Number of CPU Cores Used By the System Data Plane 1404
Enabling/Disabling the VPN Multi-Process Function 1405
The asynchronous mode of IPSec 1405
Enabling/Disabling the asynchronous mode of IPSec 1406
Viewing the Information of the Hardware Accelerator 1406
View Statistics on Encryption and Decryption Queues 1406
Manual Key VPN 1407

Creating a Manual Key VPN 1407
Specifying the Encapsulation Mode of IPsec Protocol 1407
Specifying a SPI 1407
Specifying a Protocol Type 1408
Specifying an Encryption Algorithm 1408
Specifying a Hash Algorithm 1409
Specifying a Compression Algorithm 1409
Specifying a Peer IP Address 1410
Configuring a Hash Key for the Protocol 1410
Configuring an Encryption Key for the Protocol 1410
Specifying an Egress Interface 1411
IKEv1 VPN 1411
Configuring a P1 Proposal 1411
Creating a P1 Proposal 1412
Specifying an Authentication Method 1412
Specifying an Encryption Algorithm 1413
Specifying a Hash Algorithm 1413
Selecting a DH Group 1414
Specify the Lifetime of SA 1415
Configuring an ISAKMP Gateway 1416
Creating an ISAKMP Gateway 1416
Binding an Interface to the ISAKMP Gateway 1416

Configuring an IKE Negotiation Mode 1417
Configuring the Custom IKE Negotiation Port 1417
Configuring the Custom IKE Negotiation Port Pool 1417
Binding the Custom IKE Negotiation Port Pool 1419
Specifying the IP Address and Peer Type 1419
Accepting the Peer ID 1420
Specifying a P1 Proposal 1420
Configuring a Pre-shared Key 1420
Configuring a PKI Trust Domain 1421
Configuring the Trust Domain of Peer Certificate 1421
Configuring the Trust Domain of Encryption Certificate 1421
Configuring the Negotiation Protocol Standard 1422
Configuring a Local ID 1422
Configuring a Peer ID 1423
Specifying a Connection Type 1423
Enabling NAT Traversal 1424
Configuring Auto Routing 1424
Configuring DPD 1425
Specifying Description 1426
Enabling/Disabling ISAKMP SA and IPSec SA Negotiation Separation Mode 1426
Configuring a P2 Proposal 1426
Creating a P2 Proposal 1427

Specifying a Protocol Type 1427
Specifying an Encryption Algorithm 1427
Specifying a Hash Algorithm 1428
Specifying a Compression Algorithm 1429
Configuring PFS 1429
Specifying a Lifetime 1430
Configuring the smart link 1431
Configuring the Smart Link Profile 1432
Creating a Link 1432
Configuring the Link Detection Parameters 1433
Configuring the Threshold of Link Quality Parameters 1434
Configuring the Threshold of Cycle Switching Times 1434
Enabling/Disabling Link Detection and Switch 1435
Activating a Link for Negotiation 1435
Adjusting Link Order 1435
Configuring Silence Period 1436
Configuring a Tunnel 1436
Creating an IKE Tunnel 1436
Enabling /Disabling an IKE Tunnel 1436
Specifying the Encapsulation Mode of IPsec Protocol 1437
Specifying an ISAKMP Gateway 1437
Specifying a Smart Link Profile 1437

Specifying a P2 Proposal 1438
Specifying a Phase 2 ID 1438
Configuring IPsec VPN Traffic Distribution and Limitation 1439
Accepting All Proxy ID 1440
Configuring Auto-connection 1440
Configuring DF-bit 1441
Configuring Anti-replay 1441
Configuring VPN Track and Redundant Backup 1442
Enabling/Disabling Notification of VPN Tunnel Status 1445
Setting a Commit Bit 1445
Specifying Description 1445
IKEv2 VPN 1446
Configuring a P1 Proposal 1446
Creating a P1 Proposal 1446
Specifying an Authentication Method 1447
Specifying an Encryption Algorithm 1447
Specifying a Hash Algorithm 1448
Specifying a PRF Algorithm 1448
Selecting a DH Group 1449
Specify the Lifetime of SA 1450
Configuring an ISAKMP Gateway 1450
Creating an ISAKMP Gateway 1451

Binding an Interface to the ISAKMP Gateway 1451
Configuring the Negotiation Protocol Standard 1451
Configuring the Custom IKE Negotiation Port 1452
Specifying the IP Address and Peer Type 1452
Specifying a P1 Proposal 1452
Configuring a Pre-shared Key 1453
Configuring a PKI Trust Domain 1453
Configuring the Trust Domain of Peer Certificate 1453
Configuring a Local ID 1454
Configuring a Peer ID 1454
Specifying a Connection Type 1455
Configuring Auto Routing 1455
Configuring DPD 1456
Specifying Description 1457
Configuring a P2 Proposal 1457
Creating a P2 Proposal 1457
Specifying a Protocol Type 1457
Specifying an Encryption Algorithm 1458
Specifying a Hash Algorithm 1458
Specifying a Compression Algorithm 1459
Configuring PFS 1459
Specifying a Lifetime 1460

Configuring a Tunnel 1461
Creating an IKE Tunnel 1461
Enabling /Disabling an IKE Tunnel 1461
Specifying the Encapsulation Mode of IPsec Protocol 1461
Specifying an ISAKMP Gateway 1462
Specifying a P2 Proposal 1462
Specifying a Phase 2 ID 1462
Configuring IPsec VPN Traffic Distribution and Limitation 1463
Configuring Auto-connection 1464
Configuring DF-bit 1465
Configuring VPN Track and Redundant Backup 1465
Enabling/Disabling Notification of VPN Tunnel Status 1468
Specifying Description 1468
XAUTH 1469
Enabling an XAUTH Server 1470
Configuring an XAUTH Address Pool 1470
Binding an Address Pool to the XAUTH Server 1471
Configuring IP Binding Rules 1472
Changing the Sequence of IP-Role Binding 1473
Configuring a WINS/DNS Server 1474
Kicking out an XAUTH Client 1474
Configuring Tunnel Quota for Non-root VSYS 1475

Viewing IPsec Configuration 1475
Examples of Configuring IPsec VPN 1477
Example of Configuring Manual Key VPN 1478
Requirement 1478
Configuration Steps 1478
Example of Configuring IKE VPN 1483
Requirement 1483
Configuration Steps 1483
Example of Configuring Route-based VPN Track and Redundant Backup 1490
Requirement 1490
Configuration Steps 1491
Example of Configuring Policy-based VPN Track and Redundant Backup 1498
Requirement 1498
Configuration Steps 1499
Example of Configuring XAUTH 1506
Requirement 1506
Configuration Steps 1506
Example of Using IPsec VPN in HA Peer Mode 1510
Configuration Steps 1510
SSL VPN 1515
Overview 1515
Configuring SSL VPN Server 1515

Configuring an IPv4 Access Address Pool 1516
Configuring an IP Range of the Address Pool 1517
Configuring Reserved Addresses 1518
Configuring IP Binding Rules 1518
Binding an IP to a User 1519
Binding an IP to a Role 1519
Changing the Sequence of IP-Role Binding 1520
Configuring a DNS Server 1520
Configuring a WINS Server 1520
Viewing IPv4 Address Pool 1521
Configuring an IPv6 Access Address Pool 1522
Configuring an IP Range of the Address Pool 1523
Configuring Reserved Addresses 1523
Configuring IP Binding Rules 1524
Binding an IP to a User 1524
Binding an IP to a Role 1525
Changing the Sequence of IP-Role Binding 1525
Configuring a DNS Server 1526
Viewing IPv6 Address Pool 1526
Configuring Resources List 1528
Adding Resource Items 1529
Viewing Resource List 1529

Configuring a UDP Port 1530
Configuring an SSL VPN Instance 1530
Specifying the Service Type 1532
Specifying an Access Address Pool 1532
Specifying a Server Interface 1532
Specifying an SSL Protocol Version 1533
Specifying a PKI Trust Domain 1534
Specifying an Encryption Trust Domain 1535
Specifying Tunnel Cipher Suite 1535
Specifying an AAA Server 1536
Specifying an HTTPS Port Number 1536
Configuring the Transport Protocol 1537
Configuring an SSL VPN Tunnel Route 1537
Configuring an IPv4 Tunnel Route to the Specified Network Segment 1538
Configuring an IPv6 Tunnel Route to the Specified Network Segment 1538
Configuring the Domain Route Function 1539
Enabling Dedicated SSL VPN Tunnel 1540
Configuring Anti-replay 1541
Configuring Packet Fragmentation 1542
Configuring Idle Time 1542
Configuring Forced Logoff Schedule 1543
Configuring Multi-logon 1543

Configuring URL Redirection 1544
URL Format 1544
Clearing Cache Data of the Host that Uses the SSL VPN Client 1545
Using SSL VPN in HA Peer Mode 1545
Binding L2TP VPN Instance 1546
Binding Resources 1547
Enabling/Disabling the Browser Download Function 1548
Binding SSL VPN Instance to a Tunnel Interface 1548
Authentication with USB Key Certificate 1548
Enabling USB Key Certificate Authentication 1549
Importing a USB Key Certificate to a Trust Domain 1550
Specifying a Trust Domain for the CA Certificate 1550
Two-Step Verification 1551
Enabling/Disabling Two-Step Verification 1551
Specifying the Type of Two-Step Verification 1551
Token Authentication 1552
Configuring Prompt Message 1552
SMS Authentication 1552
Modem Authentication 1552
Configuring a Mobile Phone Number for SMS Authentication 1553
Configuring Expiration Time of SMS Auth-code 1554
Configuring the SMS Verification Code Length 1554

Configuring the SMS Verification Content 1555
Configuring a Maximum SMS Number 1555
Sending a Test Message 1555
Viewing SMS Modem Settings 1556
SMS Gateway Authentication 1556
Specifying the Default Protocol Type of SMS gateway 1556
Creating an SP Instance 1557
Specifying the VRouter 1559
Specifying the Request Method 1560
Specifying the Content Type of the HTTP(S) Packets 1560
Specifying the Charset 1561
Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol 1561
Specifying the URL 1561
Specifying Source Mobile Number 1562
Configuring Platform ID 1562
Configuring Platform Password 1562
Configuring Platform Subsystem ID 1563
Configuring Template ID 1563
Specifying the Success Code 1563
Specifying the Attributes 1564
Configuring the Protocol Subtype 1567
Specifying the Gateway Address and Port Number 1568

Specifying the Number to Send Auth-message 1569
Specifying the Device ID 1569
Specifying the Username and Password 1570
Specifying the Template Parameter 1570
Specifying a Maximum SMS Number 1571
Enabling/Disabling the Sending Sign Code Function 1571
Sending a Test Message 1571
Specifying the Company Code 1572
Specifying the AccessKeyId 1572
Specifying the AccessKeySecret 1572
Specifying Instance of SMS Gateway 1573
Enabling/Disabling SMS Gateway Authentication 1573
Specifying the Sender Name or Sign Name 1574
Specifying the Template Code 1574
Sending a Test Message 1575
Specifying the Request Type 1575
Specifying the Organization Code 1575
Specifying the SMS Service Type 1576
Specifying the Trading Code 1576
Specifying the Channel 1576
Viewing SMS Gateway Settings 1577
Viewing SMS Statistic Information 1577

Email Authentication 1577
Configuring the Email Address 1578
Specifying the Email Server 1579
Configuring the Verification Code Length 1579
Configuring the Lifetime of Email Verification Code 1579
Configuring the Sender Name 1580
Configuring the Email Verification Content 1580
Host Binding 1581
Enabling Host Binding 1581
Approving a Candidate 1582
Configuring a Super User 1582
Configuring a Shared Host 1582
Increasing/Decreasing Pre-approved Hosts 1583
Clearing a Binding List 1584
Exporting/Importing a Binding List 1584
Host Check 1585
Checked Factors 1585
Role Based Access Control and Host Check Procedure 1586
Configuring a Host Check Profile 1587
Configuring a Host Check Profile via WebUI 1587
Referencing a Host Check Profile to a Rule 1591
Selecting an Optimal Path 1593

Kicking out an SSL VPN Client 1596
Configuring Change Password URL of the Client 1597
Configuring Forgot Password URL of the Client 1597
Exporting and Importing a User-list File 1597
Exporting a User-list File 1598
Importing a User-list File 1599
Control the Access by Using the Radius Server 1600
Configuring Radius Server 1601
Configuring the Allowed Client Types 1601
General Configuration 1602
Configuring SSL Cipher Suite 1602
Allowing Password Change by Local Users 1603
Customizing Client Download Source 1604
Viewing Secure Connect Client Information 1605
Customizing the Background Picture of Client Download Page 1605
Configuring Upgrade URL for Windows/Linux/macOS Type Client 1607
Customizing the Page Title 1608
Viewing SSL VPN Settings 1608
Hillstone Secure Connect Client for Windows 1609
Downloading and Installing the Client 1610
Starting Up and Connecting 1610
Editing and Deleting Login Entry 1618

Viewing Connection and Statistics Information 1618
Viewing Interface and Routing Information 1620
Viewing Log Information 1621
Third-party USB Key 1621
Client Menu 1623
General Configuration 1624
Uninstalling the Client 1624
Hillstone Secure Connect Client for Linux 1624
Downloading and Installing the Client 1625
Starting Up and Connecting 1625
Editing and Deleting Login Entry 1630
Viewing Connection and Statistics Information 1630
Viewing Interface and Routing Information 1631
Viewing Log Information 1632
Client Menu 1633
General Configuration 1634
Hillstone Secure Connect Client for Android 1634
Downloading and Installing the Client 1635
Starting Up and Connecting 1636
Editing and Deleting Login Entry 1640
Viewing Connection Information 1640
Hillstone Secure Connect Client for iOS 1642

Downloading and Installing the Client 1642
Starting Up and Connecting 1642
Editing and Deleting Login Entry 1646
Viewing Connection Information 1646
Hillstone Secure Connect Client for macOS 1647
Downloading and Installing the Client 1648
Starting Up and Connecting 1649
Editing and Deleting Login Entry 1653
Viewing Connection and Statistics Information 1653
Viewing Interface and Routing Information 1654
Viewing Log Information 1655
Client Menu 1656
General Configuration 1657
Uninstalling the Client 1657
Example of Configuring URL Redirect 1657
Configuration Steps 1658
Examples of Configuring SSL VPN 1660
Requirement 1660
Example 1 1661
Example 2 1663
Preparations 1663
Configuration Steps 1663

Example of Configuring Host Check 1665
Requirements 1665
Configuration Steps 1666
Example of Configuring Optimal Path 1673
Requirement 1 1673
Using SSL VPN Server to Choose an Optimal Path 1674
Using SSL VPN Client to Choose an Optimal Path 1677
Requirement 2 1678
Using SSL VPN Server to Choose an Optimal Path 1679
Using SSL VPN Client to Choose an Optimal Path 1681
Dial-up VPN 1683
Overview 1683
Applying Dial-up VPN 1683
Configuring the Center Device 1683
Configuring P1 Proposal 1684
Creating a P1 Proposal 1684
Specifying an Authentication Method 1684
Specifying an Encryption Algorithm 1685
Specifying a Hash Algorithm 1685
Selecting a DH Group 1686
Specifying a SA Lifetime 1687
Configuring an ISAKMP Gateway 1687

Creating an ISAKMP Gateway 1687
Specifying an AAA Server for ISAKMP Gateway 1688
Binding an Interface to the ISAKMP Gateway 1688
Configuring an IKE Negotiation Mode 1688
Specifying a Peer Type 1689
Specifying P1 Proposal 1689
Configuring a Pre-shared Key 1689
Configuring a PKI Trust Domain 1690
Configuring a Local ID 1690
Specifying a Connection Type 1691
Enabling NAT Traversal 1691
Configuring DPD 1691
Specifying Description 1692
Configuring P2 Proposal 1692
Creating P2 Proposal 1692
Specifying a Protocol Type 1693
Specifying an Encryption Algorithm 1693
Specifying a Hash Algorithm 1694
Configuring PFS 1694
Specifying a Lifetime/Lifesize 1695
Configuring a Tunnel 1696
Creating an IKE Tunnel 1696

Specifying an IPsec Mode 1696
Specifying an ISAKMP Gateway 1696
Specifying P2 Proposal 1697
Specify a Phase 2 ID 1697
Creating an IPSec SA When There is Inclusion Relation for ID 1698
Configuring IPSec Balancing and Filtering 1698
Enabling Auto Connection 1698
Configuring Packet Fragmentation 1699
Configuring Anti-replay 1699
Configuring Commit Bit 1700
Configuring Idle Time 1700
Specifying Description 1700
Configuring Auto Routing 1701
Configuring a Dial-up User 1702
Creating a Dial-up User Account 1702
Generating a Pre-shared Key for Dial-up User 1702
Configuring the Dial-up Client 1703
Example of Configuring Dial-up VPN 1703
Requirement 1703
Configuring the Center Device 1703
Configuring Dial-up Client 1 1706
Configuring Dial-up Client 2 1708

PnPVPN 1711
Overview 1711
PnPVPN Workflow 1711
PnPVPN Link Redundancy 1712
Configuring a PnPVPN Server 1712
Configuring a PnPVPN Server Using CLI 1712
Configuring User's Network 1713
Configuring Tunnel Network 1714
Configuring Wildcard of ISAKMP Gateway's Peer 1715
Configuring Tunnel Interface of PnPVPN Client 1715
Configuring a PnPVPN Sever Using WebUI 1716
Configuring a User 1717
Configuring IKE VPN 1717
Configuring a Tunnel Interface 1720
Configuring a Route 1721
Configuring a Policy 1721
Configuring a PnPVPN Client 1721
Example of Configuring PnPVPN 1723
Requirement 1723
Configuration Steps 1725
Configuring the Server 1725
Configuring the Clients 1729

GRE 1731
Overview 1731
Configuring GRE 1731
Configuring a GRE Tunnel 1731
Specifying a Source Interface/Address 1732
Specifying a Destination Address 1732
Specifying an Egress Interface 1733
Specifying an IPsec VPN Tunnel 1733
Specifying a Verification Key 1733
Binding the GRE Tunnel to a Tunnel Interface 1734
Viewing GRE Tunnel Information 1734
Example of Configuring GRE Tunnel 1734
Requirement 1735
Configuration Steps 1735
Configuring the Center 1735
Configuring the Branch 1738
L2TP 1742
Overview 1742
Typical L2TP Tunnel Network 1742
L2TP over IPSec 1743
Configuring LNS 1744
Configuring an Address Pool 1744

Configuring the IP Range of the Address Pool 1745
Configuring the Reserved IP Address 1745
Configuring IP Binding Rules 1746
Configuring a Static IP Binding Rule 1746
Configuring a Role-IP Binding Rule 1747
Moving a role-IP Binding Rule 1747
Configuring a L2TP Instance 1748
Specifying the IP Address Assignment Method 1749
Specifying an Address Pool 1749
Configuring a DNS Server 1750
Configuring a WINS Server 1750
Specifying the Egress Interface of the Tunnel 1750
Specifying an AAA Server 1751
Specifying a PPP Authentication Protocol 1751
Specifying the Hello Interval 1752
Enabling Tunnel Authentication 1752
Specifying the Secret String 1753
Specifying the Local Name of LNS 1753
Enabling AVP Hidden 1753
Specifying the Window Size of the Tunnel Data 1754
Configuring Multi-Logon 1754
Enabling/Disabling User-Specified Client IP 1754

Specifying the Retry Times of Control Packets 1755
Referencing an IPsec Tunnel 1755
Configuring Mandatory LCP Phase 1756
Enabling/Disabling Calculating the Checksum of UDP Packet 1756
Referencing the User Going Offline Alarm Profile 1756
Binding the L2TP Instance to a Tunnel Interface 1757
Specifying the ACF Information Carried by PPP Data 1758
Kicking out a User 1759
Restarting a Tunnel 1759
Viewing L2TP Information 1759
Configuring L2TP Client 1760
Configuring Device as L2TP Client 1760
Configuring a L2TP Client Instance 1760
Specifying the Tunnel Interface 1761
Specifying IP Address of LNS 1762
Specifying Keepalive of Tunnel 1762
Configuring Auto Connect 1762
Specifying a PPP Authentication Protocol 1763
Specifying the LCP-echo Interval and Transmit Retries 1763
Specifying the User Name and Password of L2TPClient 1764
Specifying the Retry Times of Control Packets 1764
Clear L2TP Client Connection 1764

View L2TP Client Instance Information 1764
Configuring L2TPv3 Tunnel 1765
Example of Configuring L2TP 1767
Requirement 1767
Configuration Steps 1768
Configurations on LNS 1768
Configurations on the Client 1770
Creating a L2TP Dial-up Connection 1771
Configuring L2TP Dial-up Connection 1771
Modifying the Registry 1774
Connecting to LNS from the Client 1775
Example of Configuring L2TP over IPsec 1776
Requirement 1776
Configuration Steps 1777
Configurations on LNS 1777
Configurations on the Client 1780
Creating L2TP Dial-up Connection 1780
Configuring the L2TP Dial-up Connection 1781
Enabling IPsec Encryption 1782
Connecting LNS from the Client 1782
VXLAN 1782
Overview 1782

Creating a VXLAN Static Tunnel 1783
Binding the VXLAN Tunnel to a Tunnel Interface 1784
Viewing VXLAN Configuration 1785
Example of Configuring VXLAN Static Unicast Tunnel 1785
Configuration Steps 1786
VTEP1 Configuratio 1786
VTEP2 Configuration 1787
Examples of VXLAN 1788
Requirements for Networking 1788
Procedure of Requirement 1 1789
Procedure of Requirement 2 1790
Chapter 10 Zero Trust Network Access (ZTNA) 1792
Introduction 1792
Configuring ZTNA Service 1794
Configuring Endpoint Tag 1794
Creating an Endpoint Tag 1795
Configuring a Criteria Set 1796
Configuring a Condition 1796
Configuring a Tip 1797
Viewing Endpoint Tag Configuration Information 1798
Managing Endpoint Items 1800
Windows Endpoint Item Management 1801

Configuring a Custom Windows Endpoint Item 1804
Defining Registry Key as Endpoint Item 1804
Defining Running Process as Endpoint Item 1805
Defining Running Service as Endpoint Item 1805
Defining Installed Service as Endpoint Item 1806
Defining File as Endpoint Item 1807
Defining Hot Fix as Endpoint Item 1807
Viewing Windows Endpoint Item Configuration Information 1808
macOS Endpoint Item Management 1808
Configuring a Custom macOS Endpoint Item 1810
Defining AD Domain Name as Endpoint Item 1810
Defining Running Process as Endpoint Item 1811
Defining Running Service as Endpoint Item 1811
Defining Installed Service as Endpoint Item 1812
Defining File as Endpoint Item 1812
Viewing macOS Endpoint Item Configuration Information 1813
Linux Endpoint Item Management 1813
Configuring a Custom Linux Endpoint Item 1815
Defining Running Process as Endpoint Item 1815
Defining Running Service as Endpoint Item 1816
Defining Installed Service as Endpoint Item 1816
Defining File as Endpoint Item 1817

Viewing Linux Endpoint Item Configuration Information 1817
iOS Endpoint Item Management 1818
Configuring a Custom iOS Endpoint Item 1819
Defining Device Model as Endpoint Item 1819
Defining WiFi SSID as Endpoint Item 1820
Defining ZTNA Client Version as Endpoint Item 1820
Viewing iOS Endpoint Item Configuration Information 1821
Android Endpoint Item Management 1821
Configuring a Custom Android Endpoint Item 1822
Defining Device Model as Endpoint Item 1822
Defining WiFi SSID as Endpoint Item 1823
Defining ZTNA Client Version as Endpoint Item 1823
Viewing Android Endpoint Item Configuration Information 1824
ChineseOS Endpoint Item Management 1824
Configuring a Custom ChineseOS Endpoint Item 1826
Defining Running Process as Endpoint Item 1826
Defining Running Service as Endpoint Item 1827
Defining Installed Service as Endpoint Item 1827
Defining File as Endpoint Item 1828
Viewing ChineseOS Endpoint Item Configuration Information 1828
Configuring the Endpoint Monitoring Period 1829
Viewing Endpoint Monitoring Configuration Information 1830

Viewing Endpoint Information Database 1830
Configuring Application Resource/Application Resource Group 1831
Creating an Application Resource 1831
Configuring an IP-Based Application Resource Entry 1832
Configuring an IP Range-Based Application Resource Entry 1833
Configuring a Domain Name-Based Application Resource Entry 1834
Configuring Hyperlink for an Application Resource 1835
Configuring Description for an Application Resource 1836
Renaming an Application Resource 1836
Viewing Application Resource Configuration Information 1837
Viewing Application Resource Configuration Information According to Filter Conditions 1837
Viewing Reference Information of an Application Resource 1838
Creating an Application Resource Group 1839
Adding Members to an Application Resource Group 1839
Configuring Description for an Application Resource Group 1840
Renaming an Application Resource Group 1840
Viewing Application Resource Group Configuration Information 1841
Viewing Reference Information of an Application Resource Group 1841
Configuring ZTNA Policy 1842
Creating a ZTNA Policy 1844
Configuring the ZTNA Policy Name 1845

Binding an Application Resource/Application Resource Group 1845
Binding an Endpoint Tag 1846
Binding a User/User Group 1846
Configuring a Schedule 1847
Specifying the Action 1847
Enabling/Disabling a ZTNA Policy 1848
Configuring Description for a ZTNA Policy 1848
Log Management of ZTNA Policies 1848
Binding Anti-Virus Profile 1849
Binding Sandbox Profile 1850
Binding IPS Profile 1850
Binding File Filter Profile 1851
Binding File Content Filter Profile 1851
Entering Global ZTNA Policy Configuration Mode 1851
Specifying the Default Action 1852
Enabling/Disabling ZTNA Session Rematch 1852
Log Management of ZTNA Default Policy 1853
Moving a ZTNA Policy 1853
Viewing ZTNA Policy Configuration Information 1853
Viewing ZTNA Policy Statistics Information 1855
Clearing ZTNA Policy Statistics Information 1855
Configuring Access Address Pool 1856

Configuring an IPv4 Access Address Pool 1856
Configuring an IP Range of the Address Pool 1856
Configuring Reserved Addresses 1857
Configuring IP Binding Rules 1857
Binding an IP to a User 1858
Binding an IP to a Role 1858
Changing the Sequence of IP-Role Binding 1859
Configuring a DNS Server 1859
Configuring a WINS Server 1860
Viewing IPv4 Address Pool 1860
Configuring an IPv6 Access Address Pool 1861
Configuring an IP Range of the Address Pool 1862
Configuring Reserved Addresses 1862
Configuring IP Binding Rules 1863
Binding an IP to a User 1864
Binding an IP to a Role 1864
Changing the Sequence of IP-Role Binding 1864
Configuring a DNS Server 1865
Viewing IPv6 Address Pool 1865
Configuring ZTNA Instance 1868
Specifying the Service Type 1869
Specifying an Access Address Pool 1870

Specifying a Server Interface 1870
Specifying an SSL Protocol Version 1871
Specifying a PKI Trust Domain 1872
Specifying an Encryption Trust Domain 1873
Specifying a Tunnel Cipher Suite 1873
Specifying an AAA Server 1874
Specifying an SSL Port Number 1874
Configuring the Transport Protocol 1875
Configuring a ZTNA Tunnel Route 1875
Configuring a ZTNA Tunnel Route to the Specified IPv4 Network Segment 1876
Configuring a ZTNA Tunnel Route to the Specified IPv6 Network Segment 1877
Configuring a ZTNA Tunnel Route to the Specified Domain Name 1877
Enabling Dedicated ZTNA Tunnel 1878
Configuring Anti-Replay 1879
Configuring Forced Timeout 1880
Configuring Packet Fragmentation 1880
Configuring Idle Time 1881
Configuring Forced Logoff Schedule 1881
Configuring Multi-Logon 1882
Configuring Multi-Gateway Address 1883
Configuring URL Redirection 1884
URL Format 1884

Enabling/Disabling the Browser Download Function 1885
Binding Remote Access ZTNA Instance to a Tunnel Interface 1885
Authentication with USB Key Certificate 1885
Enabling USB Key Certificate Authentication 1886
Importing a USB Key Certificate to a Trust Domain 1886
Specifying a Trust Domain for the CA Certificate 1887
Configuring Two-Step Verification 1888
Enabling/Disabling Two-Step Verification 1888
Specifying the Type of Two-Step Verification 1888
Token Authentication 1889
Configuring Prompt Message 1889
SMS Authentication 1889
Modem Authentication 1889
Configuring a Mobile Phone Number for SMS Authentication 1890
Configuring Expiration Time of SMS Authentication Code 1891
Configuring the SMS Authentication Code Length 1891
Configuring the SMS Authentication Code Content 1891
Configuring a Maximum SMS Number 1892
Sending a Test Message 1892
Viewing SMS Modem Settings 1893
SMS Gateway Authentication 1893
Specifying the Default Protocol Type of SMS Gateway 1893

Creating an SP Instance 1894
Specifying the VRouter 1896
Specifying the Request Method 1896
Specifying the Charset 1897
Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol 1897
Specifying the URL 1897
Specifying the Success Code 1898
Specifying the Attributes 1898
Specifying the Gateway Address and Port Number 1900
Specifying the Template Parameter 1900
Enabling/Disabling the Sending Sign Code Function 1901
Specifying the Number to Send Auth-message 1901
Specifying the Device ID 1902
Specifying the User Name/User ID and Password 1902
Specifying a Maximum SMS Number 1903
Specifying the Company Code 1903
Specifying the AccessKeyId 1903
Specifying the AccessKeySecret 1904
Specifying Instance of SMS Gateway 1904
Specifying the Sender Name or Sign Name 1904
Specifying the Template Code 1905
Specifying the Request Type 1905

Specifying the Organization Code 1906
Specifying the SMS Service Type 1906
Specifying the Trading Code 1907
Specifying the Channel 1907
Sending a Test Message 1907
Viewing SMS Gateway Settings 1908
Viewing SMS Statistic Information 1908
Email Authentication 1908
Configuring the Email Address 1909
Specifying the Email Server 1910
Configuring the Verification Code Length 1910
Configuring the Lifetime of Email Verification Code 1910
Configuring the Sender Name 1911
Configuring the Email Verification Content 1911
Configuring Single Packet Authorization (SPA) 1912
Enabling/Disabling SPA 1912
Configuring Local Knock Port 1913
Configuring the Hidden IP and Port Number 1913
Viewing SPA Configuration Information 1914
Viewing SPA Permit Entries 1914
Managing Endpoint Tag Logs 1915
Enabling/Disabling Endpoint Tag Log 1915

Clearing Endpoint Tag Logs 1915
Sending Endpoint Tag Logs 1915
Configuring Disk Storage Space Threshold 1916
Configuring the Quota of Endpoint Tag Log Buffer 1916
Viewing Endpoint Tag Logs 1917
ZTNA Portal 1918
Other Configurations 1919
Force Disconnecting a ZTNA User 1919
Configuring the Allowed Client Types 1919
Configuring Change Password URL of the Client 1920
Configuring Forgot Password URL of the Client 1921
Configuring Client Auto-Connection 1921
General Configuration 1922
Configuring SSL Cipher Suite 1922
Allowing Password Change by Local Users 1923
Customizing Client Download Source 1924
Viewing Secure Connect Client Information 1925
Customizing the Background Picture of Client Download Page 1925
Configuring Upgrade URL for Windows Type Client 1927
Customizing the Page Title 1928
Viewing ZTNA Information 1928
Example of Configuring ZTNA 1930

Networking and Requirement 1930
Configuration Steps 1930
Chapter 11 Traffic Management 1934
QoS /iQoS 1935
Swichting iQoS/QoS 1935
iQoS 1935
iQoS Implement 1936
Function Overview 1937
Multiple-level Pipes 1937
Process of iQos 1939
Configuring iQoS 1940
Specifying Traffic Control Level 1941
Enabling/Disabling Traffic Control Level/Root Pipe/Sub Pipe 1941
Enabling/Disabling NAT IP Matching 1942
Creaing a Root Pipe 1942
Creating a Sub Pipe 1943
Configuring a Traffic Matching Condition 1944
Configuring a Traffic White List 1947
Configuring the trigger threshold for the maximum floating bandwidth 1949
Configuring Traffic Management Actions for a Root Pipe 1949
Configuring Traffic Management Actions for a Sub Pipe 1952
Configuring a Traffic Control Mode for a Root Pipe 1955

Configuring a Schedule for a Root Pipe 1956
Configuring a Schedule for a Sub Pipe 1956
Binding a Root Pipe to the QSM Moduel 1957
Viewing Configurations of Traffic Control Levels and Pipes 1957
Configuring Threshold Alarm 1957
Enabling/Disabling Threshold Alarm 1958
Specifying the Alarm Threshold 1958
Show the Status of Threshold Alarm 1958
QoS 1959
Overview 1959
QoS Implementation 1959
Classification and Marking 1960
Classification 1960
Marking 1961
802.1Q/p 1961
IP Precedence and DSCP 1961
Policing and Shaping 1962
Token Bucket Algorithm 1963
Congestion Management 1964
Congestion Avoidance 1965
Configuring QoS 1965
Configuring a Class 1965

Configuring an Application Matching Condition 1966
Configuring a DSCP Matching Condition 1967
Configuring a CoS Matching Condition 1967
Configuring an IP Range Matching Condition 1968
Configuring an Address Entry Matching Condition 1968
Configuring a QoS Tag Matching Condition 1969
Configuring an IP Precedence Matching Condition 1969
Configuring an Ingress Interface Matching Condition 1970
Configuring a Role/User/User Group Matching Condition 1970
Viewing the Class Information 1970
Configuring a QoS Profile 1971
Specifying the Minimum Bandwidth 1973
Configuring Policing 1973
Configuirng Shaping 1975
Configuring IP-based QoS (IP QoS) 1976
Configuring an IP QoS Priority 1978
Configuring LLQ 1979
Configuring Congestion Avoidance 1979
Configuring CoS 1980
Configuring DSCP 1980
Configuring IP Precedence 1981
Configuring a Matching Priority 1981

Configuring an Exception Policy 1981
Configuring Role-based QoS (Role QoS) 1983
Nesting a QoS Profile 1985
Specifying a QoS Operation for the Egress Interface 1985
Disabling a Class 1986
Binding to an Interface 1986
Viewing QoS Information of an Interface 1987
Viewing QoS Profile Information 1987
FlexQoS 1988
Configuring Global FlexQoS 1988
Configuring FlexQoS for a Class 1989
Multi-level QoS 1989
Examples of Configuring QoS 1990
Example 1: Configuring a Matching Priority 1991
Example 2: Classification and Marking 1992
Example 3: Policing and Shaping 1993
Example 4: Application QoS 1994
Example 5: CBWFQ 1995
Example 6: LLQ & Congestion Avoidance 1996
Example 7: IP QoS (1) 1998
Example 8: IP QoS (2) 1999
Solution 1 1999

Solution 2 2001
Example 9: Multi-VR Application in IP QoS 2003
Example 10: IP QoS Priority 2007
Example 11: Role QoS 2009
Example 12: Nest QoS Profile 2011
Example 13: Multi-level QoS 2014
Configuring First-level Application QoS 2015
Configuring Second-level IP QoS 2017
Example 14: Comprehensive QoS Application 2019
Requirement 2019
Configuration Steps 2020
Configuration Recommandations 2029
Load Balancing 2031
SLB 2031
Configuring Server Load Balancing 2031
Adding/Deleting SLB Server Pool 2032
Configuring Parameters for SLB Server Pool Entry 2032
Assigning an Algorithm for SLB 2034
Adding/Deleting Track Rule for SLB 2035
Configuring Minimum Working Servers 2036
Configuring Threshold Value 2037
Binding SLB Server Pool Entry to DNAT Rule 2037

Viewing SLB Status 2037
LLB 2038
Outbound Link Load Balancing 2038
Outbound Load Balancing Implementation Mechanism 2038
Configuration Method 2039
Configuring Outbound Link Load Balancing 2041
Configuring SLA Profile 2041
Enabling or Disabling SLA Function 2041
Configuring Detection Mode 2041
Configuring SLA Threshold 2043
Configuring Success Times Required For Activation 2044
Configuring Failed Times Required For Deactivation 2044
Configuring LLB Profile 2045
Viewing the Link Detection Result for a Specified Domain Name 2051
Configuring LLB Rule 2051
Viewing LLB Rule Configuration Information 2052
Viewing Link Detection Results of Specified Domain 2053
Viewing LLB Profile Configuration Information 2053
Viewing SLA Profile Configuration Information 2053
Inbound Link Load Balancing 2054
Configuring Inbound Link Load Balancing 2054
Enabling SmartDNS 2054

Configuring a SmartDNS Rule Table 2054
Creating a SmartDNS Rule Table 2055
Specifying the Domain Name 2055
Specifying the Return IP 2055
Viewing LLB Configuration 2057
Example of Configuring LLB 2059
Requirement 2059
Configuration Steps 2059
Session Limit 2062
Creating a Session Limit Rule 2062
Viewing Session Limit 2064
Pre-discarding Packets of Receiving Queue 2065
Configuring Pre-discarding Packets of Receiving Queue 2065
Viewing the Information of Pre-discarding Packets of Receiving Queue 2066
Traffic Quota 2066
Configuring Traffic Quota 2066
Creating a Traffic Quota Profile 2066
Specifying the Daily Quota/ Monthly Quota 2067
Creating a User Traffic Quota Rule 2067
Specifying the User of User Traffic Quota Rule 2068
Binding a Traffic Quota Profile to a User Traffic Quota Rule 2068
Creating a User Group Traffic Quota Rule 2068

Specifying the User Group of User Group Traffic Quota Rule 2069
Binding a Traffic Quota Profile to a User Group Traffic Quota Rule 2069
Adjusting Traffic Quota Rule Priority 2070
Enabling/Disabling the Traffic Quota Function in the Zone 2071
Resetting the User Used Traffic 2071
Viewing the Traffic Quota Profile Information 2071
Viewing the User Traffic Quota Rule Information 2071
Viewing the User Group Traffic Quota Rule Information 2071
Viewing the Zone with Traffic Quota Function Enabled 2072
Viewing the Traffic Quota Statistics 2072
Chapter 12 Threat Prevention 2073
Attack Defense 2075
Common Network Attacks 2075
IP Address Spoofing 2075
ARP Spoofing 2075
Land Attack 2075
Smurf Attack 2076
Fraggle Attack 2076
Teardrop Attack 2076
WinNuke Attack 2076
SYN Flood 2077
ICMP Flood and UDP Flood 2077

ICMP Redirect Attack 2077
IP Address Sweep and Port Scan 2077
Ping of Death Attack 2078
IP Fragment Attack 2078
IP Option Attack 2078
Huge ICMP Packet Attack 2078
TCP Flag Attack 2078
DNS Query Flood Attack 2079
DNS Reply Flood Attack 2079
TCP Split Handshake Attack 2079
SIP Flood 2079
Configuring Attack Defense 2079
Configuring IP Address Sweep Attack Defense 2081
Configuring ICMP Redirect Attack Defense 2083
Configuring IP Protocol Scan Attack Defense 2083
Configuring TCP Port Scan Attack Defense 2085
Configuring UDP Port Scan Attack Defense 2086
Configuring IP Address Spoofing Attack Defense 2087
Configuring SYN Flood Attack Defense 2088
Configuring SYN-Proxy 2089
Configuring SIP Flood Attack Defense 2090
Configuring ICMP Flood Attack Defense 2091

Configuring UDP Flood Attack Defense 2092
Configuring Flood Protection Threshold Learning 2093
Configuring Large ICMP Packet Attack Defense 2096
Configuring WinNuke Attack Defense 2097
Configuring Ping of Death Attack Defense 2097
Configuring Teardrop Attack Defense 2097
Configuring IP Option Attack Defense 2097
Configuring TCP Option Anomaly Attack Defense 2098
Configuring Land Attack Defense 2099
Configuring IP Fragment Attack Defense 2099
Configuring Smurf and Fraggle Attack Defense 2100
Configuring ARP Spoofing Attack Defense 2101
Configuring DNS Query Flood Attack Defense 2101
Configuring DNS Reply Flood Attack Defense 2103
Configuring IP Verification 2104
Configuring TCP Split Handshake Attack Defense 2105
Configuring an Attack Defense Whitelist 2106
Viewing the Attack Defense Configuration and Statistics of the Security Zone 2107
Examples of Configuring Attack Defense 2107
Example of Configuring Land Attack Defense 2107
Requirement 2107
Configuration Steps 2108

Example of Configuring SYN Flood Attack Defense 2110
Requirement 2110
Configuration Steps 2110
Example of Configuring IP Address Sweep Attack Defense 2111
Requirement 2111
Configuration Steps 2112
Anti-Virus 2114
Configuring Anti-Virus 2114
Configuring Log Aggregation and Aggregation Time 2115
Enabling/Disabling Intelligence File Engine Detection Function 2116
Enhancing Intelligence File Engine Detection Performance 2117
Specifying the Number of CPU Cores Utilized at the System Data Layer 2118
Enabling/Disabling the Multi-process Function of Intelligence File Engine 2118
Showing the Intelligence File Engine Detection Information 2119
Creating an AV Profile 2120
Enabling Malicious Website Detection 2120
Specifying Malicious Website Detection Action 2121
Specifying a Protocol Type 2122
Specifying a File Type 2124
Label Email 2125
Enabling/Disabling Label Email 2126
Configuring Email Signature 2126

Configuring Anti-Virus Whitelist 2127
Binding an AV Profile to a Security Zone 2127
Binding an AV Profile to a Policy Rule 2128
Viewing AV Profile Information 2130
Configuring Decompression Control Function 2130
Updating AV Signature Database 2130
Configuring an AV Signature Update Mode 2131
Configuring an Update Protocol 2131
Configure an Update Server 2131
Specifying an HTTP Proxy Server 2132
Specifying an Update Schedule 2132
Updating Now 2133
Importing an AV Signature File 2133
Viewing AV Signature Information 2134
Viewing AV Signature Update Information 2134
Updating AV Intelligence File Engine Database 2134
Configuring an AV Intelligence File Engine Database Update Mode 2135
Configuring an Update Protocol 2135
Configure an Update Server 2136
Specifying an HTTP Proxy Server 2136
Specifying an Update Schedule 2137
Updating Now 2138

Importing the AV Intelligence File Engine Database 2138
Viewing AV Intelligence File Engine Database Version Information 2139
Viewing AV Intelligence File Engine Database Update Information 2139
Examples of Configuring Anti-Virus 2140
Sandbox 2143
Preparation for Configuring Sandbox 2144
Configuring Sandbox 2144
Enabling/Disabling the Cloud Sandbox or the Local Sandbox 2146
Configuring the Local Sandbox 2146
Creating a Sandbox Profile 2147
Enabling White List 2147
Configuring Certificate Verification 2147
Configuring File Filter 2148
Specifying Actions for a Sandbox Profile 2149
Disabling Suspicious File Uploading 2150
Binding a Sandbox Profile to a Policy Rule 2150
Enabling Benign File 2150
Enabling the Greyware File function 2151
Configuring the File Size Limit 2151
Adding Items to the Trust List 2152
Viewing Sandbox Information 2153
Updating Sandbox Whitelist Database 2153

Configuring a Sandbox Whitelist Update Mode 2154
Configuring an Update Protocol 2154
Configure an Update Server 2154
Specifying a HTTP Proxy Server 2155
Specifying an Update Schedule 2156
Updating Now 2156
Importing a Sandbox Whitelist File 2157
Viewing Sandbox Whitelist Information 2157
Viewing Sandbox Whitelist Update Information 2157
IPS 2158
IPS Detection and Submission Procedure 2158
Signatures 2158
Updating IPS Signature Database 2159
Specifing the HTTP Proxy Server 2161
IPS Working Modes 2161
Configuring IPS 2161
Configuration Suggestions 2163
Performing IPS Detection on HTTPS Traffic 2164
IPS Commands 2166
action 2166
affected-software 2167
attack-type 2168

banner-protect enable 2168
brute-force 2169
password-protect 2170
Configuring HTTP Password Protection Information 2171
Enabling/Disabling the HTTP Plaintext Check Function 2173
bulletin-board 2173
command-injection-check 2174
confidence 2174
cc-url 2175
cc-url-limit 2176
check-weakpassword 2177
custom-password add 2178
custom-password delete 2179
deny-method 2180
disable 2181
disable protocol-anomaly 2181
disable signature 2182
domain 2182
dst-ip 2184
enable 2184
enable 2185
equal-username-check 2186

exec ips 2186
external-link 2187
external-link-check 2188
filter-class 2189
ftp-anonymous-login-check 2189
http-request-flood auth 2190
http-request-flood enable 2191
http-request-flood proxy-limit 2192
http-request-flood request-limit 2193
http-request-flood statistics 2195
http-request-flood white-list 2195
http-request-flood x-forward-for 2196
http-request-flood x-real-ip 2197
iframe-check 2198
iframe width 2199
ips buffer-capture enable 2199
ips enable 2200
ips log aggregation 2202
ips log http-proxy-ip 2203
ips mode 2203
ips profile 2204
ips signature 2206

ips sigset 2206
ips suspicious-ua-detection whitelist 2207
ips suspicious-ua-detection user-define 2208
ips whitelist 2209
issue-date 2209
length 2210
max-arg-length 2211
max-bind-length 2212
max-black-list 2214
max-cmd-line-length 2214
max-content-filename-length 2216
max-content-type-length 2217
max-failure 2219
max-input-length 2220
max-path-length 2222
max-reply-line-length 2223
max-request-length 2225
max-rsp-line-length 2226
max-scan-bytes 2228
max-text-line-length 2228
max-uri-length 2230
max-white-list 2231

min-character-type 2232
pcap 2233
protocol-check 2233
protocol 2235
referer-white-list 2236
referer-white-list-check 2236
response-bypass 2237
reverse-shell 2238
reverse-shell action 2239
reverse-shell level 2240
search-class 2241
search-condition 2242
sensitive-file-scan action 2242
sensitive-file-scan enable 2244
sensitive-file-scan warning-value 2244
serial-character-check 2245
severity 2246
signature id 2247
signature-id 2247
sigset 2248
sql-injection 2249
sql-injection-check 2249

src-ip 2251
suspicious-ua-detection 2251
suspicious-ua-detection action 2252
system 2253
vr 2254
web-acl 2254
web-acl-check 2255
web-server 2256
xss-injection 2257
xss-check enable 2258
ips http-multi-decode 2259
Configuring the IPS HTTP Multi-decode Function 2259
Enable/Disable URL Decoding 2260
Enable/Disable Unicode Decoding 2260
Configuring the Maximum Number of Times of HTTP Multiple Decoding 2261
show ips 2261
Abnormal Behavior Detection 2264
Overview 2264
Configuring Abnormal Behavior Detection 2265
Enabling/Disabling Abnormal Behavior Detection 2265
DNS Mapping 2266
Viewing the Entry of DNS Mapping 2266

Viewing Detection Status of Dos Attacks 2266
Updating Abnormal Behavior Model Database 2266
Configuring an Abnormal Behavior Model Update Mode 2267
Specifying an Automatic Update Period 2267
Updating Now 2267
Importing an Abnormal Behavior model File 2268
Viewing Abnormal Behavior Model Update Information 2268
Advanced Threat Detection 2269
Overview 2269
Configuring Advance Threat Detection 2269
Updating Malware Behavior Model Database 2270
Configuring a Malware Behavior Model Update Mode 2270
Specifying an Automatic Update Period 2270
Updating Now 2271
Importing a Malware Behavior Model File 2271
Viewing Malware Behavior Model Update Information 2272
Perimeter Traffic Filtering 2273
Overview 2273
Configuring Perimeter Traffic Filtering 2273
Enabling/Disabling Perimeter Traffic Filtering 2273
Configuring Static IP Blacklist 2274
Configuring Redundancy Check of Static IP Blacklist 2275

Configuring MAC Blacklist 2275
Configuring Blacklist Library 2276
Configuring Dynamic IP Blacklist 2280
Configuring Real IP Blacklist 2281
Configuring Static Service Blacklist 2282
Configuring Dynamic Service Blacklist 2283
Enabling the Logging Function of Blacklist 2284
Configuring Session Rematch of Blacklist 2284
Configuring Cache Time For The Hit Count Statistics Data of Blacklist 2284
Viewing the Hit Count Statistics of Blacklist 2285
Clearing the Hit Count Statistics of Blacklist 2285
Viewing the Enabled Status of the Blacklist Logging Function 2285
Enabling/Disabling IP BlackList TCP Reset 2285
Viewing the Status of IP BlackList TCP Reset 2286
Configuring IP Reputation Filtering 2286
Enabling IP Reputation Filtering 2287
Configuring an IP Reputation Update Mode 2288
Configuring an Update Protocol 2288
Configure an Update Server 2288
Specifying a HTTP Proxy Server 2289
Specifying an Update Schedule 2289
Importing an IP Reputation File 2290

Viewing IP Reputation Information 2291
Viewing Categories of IP Reputation 2291
Viewing IP Reputation Update Information 2292
Mitigation 2293
Overview 2293
Mitigation Rule 2293
Enabling/Disabling Auto Mitigation 2293
Configuring the Mitigation Rule 2294
Viewing the Status of Auto Mitigation 2294
Updating Mitigation Rule Database 2294
Configuring a Mitigation Rule Update Mode 2295
Specifying an Automatic Update Period 2295
Updating Now 2295
Importing a Mitigation Rule File 2295
Viewing Mitigation Rule Update Information 2296
Correlation Analysis 2297
Updating Correlation Analysis Engine/Rules 2297
Critical Assets 2298
Specifying Critical Asset Name 2298
Specifying Critial Asset IP Address 2299
Specifying Critial Asset Zone 2299
Enabling/Disabling Web Server Advanced Protection 2299

Renaming a Critical Asset 2300
Viewing Critical Asset Object Configurations 2300
Hot Threat Intelligence 2300
Enabling /Disabling Hot Threat Intelligence Pushing 2301
Updating Hot Threat Intelligence Manually 2301
Geolocation Information Database 2302
Overview 2302
Updating Geolocation Information Database 2302
Configuring a Geolocation Information Database Update Mode 2302
Configuring an Update Protocol 2303
Configure an Update Server 2303
Specifying a HTTP Proxy Server 2304
Specifying an Update Schedule 2304
Updating Now 2305
Importing a Geolocation Information Database File 2305
Viewing Geolocation Information Database Information 2306
Viewing Geolocation Information Database Update Information 2306
MITRE ATT&CK® Knowledge Base 2306
Updating MITRE ATT&CK® Knowledge Base 2307
Configuring a MITRE ATT&CK® Knowledge Base Update Mode 2307
Configuring an Update Protocol 2308
Configure an Update Server 2308

Specifying an HTTP Proxy Server 2309
Specifying an Update Schedule 2309
Updating Now 2310
Importing a MITRE ATT&CK® Knowledge Base File 2310
Viewing MITRE ATT&CK® Knowledge Base Information 2311
Viewing MITRE ATT&CK® Knowledge Base Update Information 2311
Botnet Prevention 2313
Preparing 2313
Configuring Botnet Prevention 2314
Creating a Botnet Prevention Profile 2314
Specifying the Outreach Type of Threat Prevention and the Corresponding Action 2315
Specifying a Protocol Type 2316
Enabling/Disabling DGA Detection 2317
Enabling/Disabling the DNS Tunnel Detection 2318
Specifying Log Aggregation Type and Aggregation Time 2319
Configuring the DNS Tunnel Log Interval 2320
Address Library Management 2321
Configuring the Custom Block List 2321
Configuring the Custom Exclude List 2322
Viewing Custom Signature Entry 2322
Configuring the Blacklist Library of Botnet Prevention 2324
Configuring the Sinkhole IP address 2328

Binding a Botnet Prevention Profile to a Security Zone 2329
Binding a Botnet Prevention Profile to a Policy Rule 2329
Viewing Botnet Prevention Profile Information 2330
Viewing Botnet Prevention Status 2330
Viewing Botnet Prevention Log Aggregation Configuration 2330
Updating Botnet Prevention Signature Database 2330
Configuring the Botnet Prevention Signature Update Mode 2331
Configuring an Update Protocol 2331
Configure an Update Server 2331
Specifying a HTTP Proxy Server 2332
Specifying an Update Schedule 2333
Updating Now 2333
Importing a Botnet Prevention Signature File 2334
Viewing Botnet Prevention Signature Information 2334
Viewing Botnet Prevention Signature Load Status 2334
Viewing Botnet Prevention Signature Update Information 2335
Encrypted Traffic Detection 2335
Encrypted Traffic Detection Configurations 2335
Enabling/Disabling the Encrypted Traffic Detection Function 2336
Configuring the IP Whitelist of Encrypted Traffic Detection 2336
Updating Encrypted Traffic Detection Database 2337
Configuring an Encrypted Traffic Detection Database Update Mode 2338

Configuring an Update Protocol 2338
Configure an Update Server 2338
Specifying an HTTP Proxy Server 2339
Specifying an Update Schedule 2339
Updating Now 2340
Importing an Encrypted Traffic Signature File 2340
Viewing Encrypted Traffic Detection Database Information 2341
Viewing Encrypted Traffic Detection Database Update Information 2341
Antispam 2342
Overview 2342
Configuring Antispam 2342
Creating an Antispam Profile 2342
Specifying a Mail Protocol Type 2343
Specifying the Spam Category 2343
Specifying the Whitelist of Sender 2344
User-defined Blacklist Spam 2344
Enabling/Disabling User-defined Blacklist 2345
Adding/Deleting User-defined Blacklist 2345
Binding an Antispam Profile to a Security Zone 2345
Binding an Antispam Profile to a Policy Rule 2346
Configuring the Mail Scan Maximum Limit 2346
Viewing Antispam Profile Information 2346

Viewing the Antispam Status Information 2347
Viewing the Global Configuration 2347
End Point Protection 2348
Configuring the End Point Protection 2349
Preparation for Configuring End Point Protection 2349
Configuring End Point Protection 2349
Configuring Endpoint Security Control Center Parameters 2349
Specifying the Name of the Endpoint Security Control Center Server 2349
Specifying the Address of the Endpoint Security Control Center Server 2350
Specifying the Port of the Endpoint Security Control Center Server 2350
Specifying the Synchronization Period 2351
Enabling/Disabling the Timeout Entry 2351
Creating an End Point Protection Profile 2351
Specifying the Protection Action 2352
Specifying the Exception Address 2353
Binding an End Point Protection Profile to a Security Zone 2353
Binding an End Point Protection Profile to a Policy Rule 2354
Manually Synchronizing the Endpoint Data Information 2354
Viewing End Point Protection Profile Information 2354
Viewing the End Point Status 2354
Viewing the End Point Information Synchronization Status 2354
Viewing the Endpoint Security Control Center Information 2355

IoT Monitor 2356
Typical Deployment Scenario 2357
Built-in Asset Identification 2358
External Asset Identification 2358
Configuration Procedure of IoT Monitor Function 2359
Deploying the Asset Identification System on the Virtual Machine 2361
Deploying the Asset Identification System on VMware ESXi 2361
Before You Start 2361
System Requirements and Limits 2362
Procedure 2362
Step 1: Log in to VMware ESXi 2362
Step 2: Create a VM 2362
Step 3: Log in to the virtual machine 2366
Step 4: Configure NIC 2366
Step 5: Install the asset identification program 2367
Deploying the Asset Identification System on Openstack 2368
Before You Start 2368
System Requirements 2368
Procedure 2369
Step 1: Import the Image File 2369
Step 2: Create a Flavor 2370
Step 3: Create a Network 2371

Step 4: Start the Instance 2371
Step 5: Log in to Virtual Machine 2372
Setp 6: Configure NIC 2373
Step 7: Install the asset identification program 2373
Configuring Identification List 2375
Creating Identification List 2375
Configuring the IP/MAC Identification List 2375
Configuring the IP Identification List 2376
Specifying IP 2376
Specifying IP Range 2377
Configuring the MAC Identification List 2378
Importing Identification List 2379
Viewing Information about the Identification List 2379
Configuring Local Asset Identification 2379
Enabling/Disabling the Local Asset Identification Function 2380
Configuring the Local Asset Identification Function 2380
Viewing the Configuration about the Local Asset Identification Function 2381
Configuring the Interval of Re-identifying IoT Devices 2382
Configuring Region and Synchronizing Endpoint to Repository 2382
Configuring Region and Sub-region 2382
Configuring an IP Segment for a Region 2383
Configuring an IP Range for a Region 2383

Viewing IoT Region Information 2384
Enabling/Disabling Automatic Synchronization of Endpoint to Repository 2385
Viewing the Enabling Status of IoT Endpoint Synchronization to Repository 2385
Configuring the IoT Monitor Function of Security Zone 2387
Binding the Identification List to Security Zone 2387
Enabling/Disabling the MAC Address Function in Referenced Traffic 2388
IoT Monitor 2388
Viewing the IoT Monitor List Information 2388
Modifying IoT Monitor List Entry 2389
Deleting IoT Monitor List Entry 2390
Device Object 2390
Configuring Device Object 2391
Creating/Deleting a Device Object 2391
Configuring the Device Type of the Device Object 2392
Configuring the Manufacturer of the Device Object 2392
Configuring the Model of the Device 2393
Configuring the OS Family of the Device Object 2393
Configuring the OS Version of the Device Object 2394
Viewing the Configuration about the Device Object 2394
Viewing the Mapping IP Address of Device 2394
Viewing the Device Object to Which the Specified IP Address Belongs 2395
Honeypot 2395

Introduction 2395
Configuring the Honeypot Function 2395
Connecting to Honeypot 2396
Entering the Honeypot Configuration Mode 2396
Enabling/Disabling the Honeypot Function 2397
Configuring the Address of the Honeypot System 2397
Configuring the Port Number of the Honeypot System 2397
Configuring the Heartbeat Detection Cycle 2398
Configuring the Virtual Router to Which the Honeypot System Belongs 2398
Configuring the Tenant ID of the Honeypot System 2399
Configuring the Authentication Key of the Honeypot System 2399
Configuring a Trap Rule 2399
Creating a Trap Rule and Entering the Trap Rule Configuration Mode 2400
Enabling/Disabling the Trap Rule 2400
Configuring the Trap Rule Name 2401
Configuring the Source Address of the Trap Rule 2401
Configuring the Disguised Address of the Trap Rule 2401
Configuring the Honeypot Template 2402
Configuring the Virtual Router to Which the Trap Rule Belongs 2402
Viewing the Configuration about the Honeypot Function 2402
Cloud-Network Collaborative DNS Protection 2404
Unknown Domain Cloud Collaborative Query 2404

Introduction 2404
Typical Application Scenario 2405
Configuring Unknown Domain Cloud Collaborative Query (Cloud Query) 2405
Enabling/Disabling Unknown Domain Cloud Collaborative Query 2406
Specifying the Unknown Domain Cloud Collaborative Query Token 2406
Configuring Cloud Query Timeout Time 2407
Querying Cloud Query Cache Data 2408
Clearing Cloud Query Cache Data 2409
Viewing Cloud Query Configuration 2409
Cloud-Based DNS Security Detection 2409
Introduction 2409
Typical Application Scenario 2410
Secure DNS 2410
Enabling/Disabling the Secure DNS Function 2411
Entering the Secure-DNS Profile Configuration Mode of a Specified Provider 2411
Configuring the DoH Server 2412
Enabling/Disabling the Function of Sending the Client Address 2412
Configuring the Health Check Interval 2412
Enabling/Disabling the Function of Generating Logs 2413
Viewing Information about Secure DNS Configuration 2413
Chapter 13 Data Security & URL Filtering 2415
Data Security 2416

Overview 2416
Introduction to Data Security 2416
Content Filter 2419
File Content Filter 2419
Configuring File Content Filter via CLI 2419
Creating a File Content Filter Profile 2420
Specifying the File Type 2420
Specifying the Keyword Category and Action 2421
Specifying the Protocol Type and Direction 2421
Binding the File Content Filter Profile to a Policy Rule 2422
Binding the File Content Filter Profile to a Security Zone 2422
Viewing File Content Filter Profile Information 2423
Web Content 2423
Configuring Web Content via CLI 2423
Creating a Web Content Profile 2423
Specifying the Keyword Category and Action 2424
Specifying the Control Range 2424
Excluding HTML Tags 2425
Binding the Web Content Profile to a Policy Rule 2425
Binding the Web Content Profile to a Security Zone 2426
Viewing Web Content Profile Information 2426
Web Posting 2426

Configuring Web Posting via CLI 2426
Creating a Web Posting Profile 2427
Specifying the Control Type and Action of Web Posting 2427
Specifying the Control Range 2428
Binding the Web Posting Profile to a Policy Rule 2428
Binding the Web Posting Profile to a Security Zone 2429
Viewing Web Posting Profile Information 2429
Email Filter 2430
Configuring Email Filter via CLI 2430
Creating a Mail Filter Profile 2430
Specifying the Control Type 2431
Controlling All the Emails and Specifying the Action 2431
Specifying the Sender/Recipient and Action 2431
Specifying the Keyword Category and Action 2432
Specifying the Control Type 2432
Specifying the Action for other emails 2433
Specifying the Account Exception 2433
Binding the Email Filter Profile to a Policy Rule 2433
Binding the Email Filter Profile to a Security Zone 2434
Viewing Email Filter Profile Information 2434
APP Behavior Control 2435
Configuring APP Behavior Control via CLI 2435

Creating an APP Behavior Control Profile 2435
Controlling FTP Application 2436
Controlling HTTP Application 2437
Controlling TELNET Application 2437
Binding the APP Behavior Control Profile to a Policy Rule 2438
Binding the APP Behavior Control Profile to a Security Zone 2438
Viewing APP Behavior Control Profile Information 2439
File Filter 2440
Configuring File Filtering 2440
Creating a File Filter Profile 2441
Creating a File Filter Rule 2441
Specifying the File Size 2442
Specifying the File Name 2442
Configuring the Description 2442
Specifying the Protocol 2443
Specifying the File Type 2443
Specifying the Action 2444
Binding the File Filter Profile to a Policy Rule 2444
Viewing File Filter Profile 2445
Configuring Decompression Control Function 2445
Enabling / Disabling Decompression Function 2445
Specifying the Maximum Decompression Layer 2446

Specifying an Action for Encrypted Compressed Files 2446
Viewing Decompression Control Configuration Information 2446
Network Behavior Record 2448
Configuring Network Behavior Recording via CLI 2448
Creating a Network Behavior Record Profile 2448
IM Audit 2449
Configuring Timeout Value 2449
Recording Web Surfing Log 2450
Binding the NBR Profile to a Policy Rule 2450
Binding the NBR Profile to a Security Zone 2451
Viewing NBR Profile Information 2451
Log Management 2452
Log Severity and Format 2452
Output Destinations 2452
Configuring Log 2452
Data Security Configuration Examples 2454
Example1: URL Filter Configuration 2455
Preparations 2455
Configuration Steps on CLI 2455
Example 2: Web Content Configuration 2457
Preparations 2457
Configuration Steps on CLI 2457

Example 3: Web Posting Configuration 2459
Preparations 2459
Configuration Steps on CLI 2459
Example 4: Email Filter Configuration 2460
Configuration Steps on CLI 2460
Example 5: Network Behavior Record Configuration 2461
Configuration Steps on CLI 2461
Object Configuration 2465
Predefined URL Database 2465
Updating the Predefined URL Database 2465
Specifying a HTTP Proxy Server 2467
User-defined URL Database 2468
URL Lookup 2469
Configuring a URL Inquiry Server 2469
Keyword Category 2470
Keyword Matching Rules 2471
Warning Page 2472
Configuring Block Warning 2472
Configuring Audit Warning 2474
Configuring the Custom Warning Page 2476
Entering the Warning Page Configuration Mode 2476
Enabling the Custom Warning Page Function 2476

Creating an Image Object 2478
Uploading a Custom Image 2478
Uploading a Custom Warning Page 2479
Viewing Information about Custom Warning Page 2479
Viewing Information about Custom Image 2480
Clearing Content on the Custom Warning Page 2480
Bypass Domain 2481
User Exception 2481
First Access of Uncategorized URL 2482
Specifying the Waiting Time of Query 2482
Enabling/Disabling the Block Action after Waiting Timeout 2483
Viewing Configurations of First Access of Uncategorized URL 2483
URL Filtering 2484
Configuring URL Filter via CLI 2484
Creating a URL Filter Profile 2484
Specifying the URL Category and Action 2485
Inspecting SSL Negotiation Packets 2485
Specifying the URL Keyword and Action 2486
Enabling Safe Search 2486
Binding the URL Filtering Profile to a Security Zone 2487
Binding the URL Filtering Profile to a Policy Rule 2488
Viewing URL Filtering Profile Information 2490

URL Blacklist/Whitelist 2491
Configuring the URL Blacklist 2491
Configuring the URL Whitelist 2492
Viewing the URL Blacklist Information 2492
Viewing URL Whitelist Information 2493
SSL Proxy 2494
Work Mode 2494
Working as Gateway of Web Clients 2496
Configuring SSL Proxy Parameters 2496
Specifying the PKI Trust Domain of Device Certificate 2497
Obtaining the CN Value 2497
Importing a Device Certificate to a Web Browser 2498
Configuring an SSL Proxy Profile 2499
Configuring the Session Reuse Function 2500
Choosing a Work Mode 2503
Specifying an Application to be Proxied by the SSL Proxy Function 2503
Setting the URL Whitelist 2504
Enabling the Root Certificate Push 2504
Configuring the Actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS Traffic 2505
Checking the SSL Protocol Version 2506
Checking the Unkown Failure 2507

Checking the Encryption Algorithm 2507
Checking Whether the SSL Server Certificate is Overdue 2508
Checking Whether the SSL Server Verifies the Client Certificate 2508
Configuring an Action When Server Certificate Verification Fails 2509
Configuring the Description 2510
Prioritizing the Low-intensity Encryption Algorithm 2510
Updating the Trusted Root Certificate Database 2510
Configuring the Update Mode of the Trusted Root Certificate Database 2511
Updating Trusted Root Certificate Database 2512
Importing a Trusted Root Certificate Database File 2512
Viewing Update Information of the Trusted Root Certificate Database 2512
Viewing Information of the Trusted Root Certificate Database 2513
Working as Gateway of Web Servers 2513
Configuring an SSL Proxy Profile 2513
Configuring the Session Reuse Function 2514
Choosing a Work Mode 2517
Specifying Trust Domain 2518
Specifying HTTP Port Number 2518
Enable Warning Page 2518
Configuring the Description 2519
Binding the SSL Proxy Profile to a Policy Rule 2519
Configuring the SSL Proxy Filter Rule 2520

Adding the SSL Proxy Filter Rule 2520
Deleting the SSL Proxy Filter Rule 2520
Viewing the SSL Proxy Filter Rule Information 2520
Configuring Asynchronous Acceleration 2521
Configuring Domain White List 2522
Configuring a User-defined Domain White List 2522
Updating SSL Proxy Domain Whitelist Signature Database 2522
Configuring a Domain Whitelist Signature Database Update Mode 2523
Configuring an Update Protocol 2523
Configure an Update Server 2524
Specifying an HTTP Proxy Server 2524
Specifying an Update Schedule 2525
Updating Now 2525
Importing a Domain Whitelist Signature File 2526
Viewing Domain Whitelist Signature Database Information 2526
Viewing Domain Whitelist Signature Database Update Information 2526
Configuring the IP Whitelist 2527
Configuring the Static IP Whitelist 2527
Configuring the Validity Time of Dynamic IP Whitelist 2527
Clearing the IP Whitelist 2528
Viewing SSL Proxy Information 2528
Chapter 14 Monitor 2530

Monitor 2531
Overview 2531
User Monitor 2532
Configuring Monitor Address Book 2532
Viewing Address Book Statistical Information 2532
Configuring Subnet Monitor Address Book 2533
Viewing Subnet Monitor Address Entry Information 2533
Viewing the Stat-set for User Monitor 2533
Application Monitor 2534
Configuring Monitor Application Group 2535
Viewing Application-based Statistical Information 2535
Viewing the Stat-set for Application Monitor 2536
Threat Monitor 2537
Viewing the Stat-set for Threat Monitor 2537
QoS Monitor 2537
Service/Network Node Monitor（For T Series） 2537
host…type dns 2537
host…type ftp 2538
host…type http 2540
host…type icmp 2541
host…type imap4 2542
host…type ldap 2543

host···type pop3 2544
host···type smtp 2545
host···type {tcp | udp} 2546
show monitor host config 2548
show monitor host status 2548
Device Monitor 2549
Viewing Interface-based Statistical Information 2549
Viewing the Stat-set for Device Monitor 2549
Viewing the Information of Hard Disk Module 2550
Viewing the Utilization of Virtual Hard Disk of CloudEdge Devices 2550
Viewing Memory Usage 2551
Viewing CPU and Memory Utilization 2551
Modifying the product name on the login page 2552
URL Hit 2553
Link Status Monitor 2553
Enabling/Disabling Link User Experience Monitor 2554
Enabling/Disabling Application Switch for Interface 2554
Specify the Description of Interface 2554
Viewing Link Configuration Information 2555
Viewing Statistics Information of Link User Experience 2555
Configuring the Link Detection Destination 2555
Entering the Link Detection Monitor Configuration Mode 2555

Configuring the Link Detection Destination of IPv4 2556
Configuring the Link Detection Destination of IPv6 2556
Configuring the Link Detection Destination of Domain 2557
Configuring a Link Detection Rule 2557
Enter the Link Detection Rule Mode 2558
Configuring the Link of the Link Detection Rule 2558
Configuring the Detection Destination of the Link Detection Rule 2558
Configuring the Packet Loss Rate Threshold of the Link Detection Rule 2559
Enabling/Disabling the Link Detection Rule 2559
Viewing the Configuration of Link Detection Rule 2559
Viewing Link Detection Monitor Configuration Information 2560
Application Block 2560
Keyword Block 2561
Authentication User 2562
show auth-user 2562
show auth-user groupname 2562
show dp-auth-user 2563
show pseudo-group 2564
show auth-user agent 2564
show auth-user dot1x 2565
show auth-user interface 2565
show auth-user ip 2566

show auth-user l2tp 2567
show auth-user mac 2567
show auth-user radius-snooping 2568
show auth-user static 2569
show auth-user scvpn 2569
show auth-user endpoint-tag 2570
show auth-user ztna 2571
show auth-user ad-scripting 2571
show auth-user ad-polling 2572
show auth-user sso-radius 2572
show auth-user sso-monitor 2573
show auth-user webauth-ntlm 2574
show auth-user xauth 2574
show auth-user webauth 2575
show auth-user vrouter 2575
User-defined Monitor 2576
Creating a Stat-set 2576
Configuring the Type of Statistical Data 2577
Configuring a Data Grouping Method 2578
Configuring a Filter 2590
Enabling/Disabling Stat-set 2593
Viewing Stat-set Information 2593

Diagnostic Center 2594
Always Collecting 5-Tuple Statistics of Packet Loss 2595
Configuring a Packet Loss Threshold 2595
Configuring a Packet Loss Growth Rate Threshold 2596
Long-term Monitor 2596
Enabling/disabling Long-term Monitor 2597
Logs 2598
Overview 2598
Log Severity 2599
Log Output 2600
Log Format 2601
Configuring System Logs 2601
Enabling/Disabling the Log Function 2602
Sending and Filtering Event Logs 2602
Configuring SMS 2604
Configuring a Mobile Phone Number 2605
Specifying the Mode of Sending SMS Messages 2605
Sending Threat Logs 2605
Sending Configuration/Operation/Debug/Network Logs 2607
Sending Debug Logs to a File 2610
Configuring the Conditions of Using the Debug Function 2610
Sending Traffic Logs 2611

Sending Data Security Logs 2612
Sending Cloudsandbox logs 2613
Sending EPP logs 2614
Sending IoT Logs 2615
Configuring the Output Log Format 2616
Configuring the Function of Storing Logs on the Hard Disk 2618
Configuring the Log Backup Server 2618
Optimizing the Function of Exporting Session Logs and NAT Logs to the Local Disk 2619
Binding the Log Processing Process and Database Storage Process to Core MAX 2619
Configuring the Speed at Which Logs are Sent to Log Processing Process 2620
Configuring a Syslog Server 2621
Creating a Syslog Server 2622
Configuring the IP Address/Host Name of the Syslog Server 2622
Specifying the Binding Method 2622
Specifying the Log Format of the Syslog Server 2623
Specifying the Protocol Type 2624
Specifying the Destination Port Number 2624
Enabling/Disabling the Syslog_Server Certificate Check Disable Function 2624
Specifying the Type of Generated Logs 2625
Specifying a Description for the Syslog Server 2625
Specifying the Sending Sourceport Number 2625
Specifying a Facility 2626

Globally Configuring the Facility Field of Log Messages 2627
Separately Specifying the Facility Field of Event Logs and Traffic Logs 2627
Viewing the Facility Field of Event Logs and Traffic Logs 2627
Displaying Hostname/Username in the Traffic Logs 2628
Displaying Username in the Threat Logs 2628
Sending Logs to an Email Account 2629
Configuring an Email Address 2629
Configuring a SMTP Server Instance 2629
Configuring PBR Log Function 2630
Enabling PBR Log Function 2630
Sending PBR Logs 2631
Displaying Hostname/Username in PBR Logs 2632
Viewing PBR Logs 2632
Configuring Log Parameter 2632
Disabling the Log Generation 2633
Configuring Log Level 2633
Enabling/Disabling the Record User Information Function for Threat Log 2634
Viewing Log Entries for Configuring Log Parameters 2634
Viewing Log Configurations 2634
Viewing Logs 2635
Exporting Logs 2636
Clearing Logs 2636

Sending Traffic Logs to Syslog Servers 2637
Example of Configuring Logs 2639
Example 1: Sending Event Logs to the Console 2639
Example 2: Sending Event Logs to the Syslog Server 2639
Example 3: Sending Traffic Logs to a Local File 2640
Diagnostic Tool 2641
Introduction 2641
Commands 2642
Packet Capture Commands 2642
Configuring Packet Capture Task 2642
packet-capture task 2642
include-self-traffic 2643
interface 2643
direction 2644
task-info 2645
filter-rule 2646
exec packet-capture 2647
export packet-capture-file 2648
clear packet-capture task 2649
Packet Capture Global Configuration 2649
packet-capture save-mem 2650
packet-capture save-time 2650

packet-capture dp-mem-max 2651
Show Commands 2652
show packet-capture status 2652
show packet-capture task 2652
Packet Path Detection Commands 2653
Emulation Packet 2653
troubleshooting packet-trace emulation-template 2653
exec troubleshooting packet-trace emulation-template 2654
exec troubleshooting packet-trace stop 2655
export troubleshooting packet-trace emulation-template 2655
Online Packet 2656
troubleshooting packet-trace filter 2656
exec troubleshooting packet-trace filter 2657
exec troubleshooting packet-trace stop 2658
export troubleshooting packet-trace packet-capture-file 2659
Imported Packet 2660
import troubleshooting packet-trace 2660
troubleshooting packet-trace filter 2661
exec troubleshooting packet-trace filter 2662
exec troubleshooting packet-trace stop 2662
NetFlow 2663
Overview 2663

Configuring NetFlow 2663
Enabling NetFlow 2663
Creating a NetFlow Profile 2663
Configuring the Template Refresh Rate 2664
Configuring the Active Timeout Value 2664
Configuring the NetFlow Server 2665
Containing the Enterprise Field 2665
Specifying the Source Interface 2665
Binding a NetFlow Profile to an Interface 2666
Viewing NetFlow Information 2666

About This Guide

This document follows the conventions below:

Content

- **Tip**: provides reference.
- **Note**: indicates important instructions for you better understanding, or cautions for possible system failure.
- **Bold font**: indicates links, tags, buttons, checkboxes, text boxes, or options. For example, "Click **Login** to log into the homepage of the Hillstone device", or "Select **Objects** > **Address Book** from the menu bar".

CLI

- Braces ({ }): indicate a required element.
- Square brackets ([ ]): indicate an optional element.
- Vertical bar (|): separates multiple mutually exclusive options.
- Bold: indicates an essential keyword in the command. You must enter this part correctly.
- Italic: indicates a user-specified parameter.
- The command examples may vary from different platforms.
- In the command examples, the hostname in the prompt is referred to as host-name.
- All the configurations should be in UTF-8 code if not particularly indicated.

WebUI

When clicking objects (menu, sub-menu, button, link, etc.) on WebUI, the objects are separated by an angled bracket (>).

Command Line Interface

Overview

A command line interface (CLI) is a mechanism for you to interact with the operating system by typing commands which instruct the device to perform specific tasks. This chapter describes how to use StoneOS command line interface.



Notes: All command keywords are not case sensitive, but user input is case sensitive.

CLI Modes and Prompts

StoneOS CLI commands and statements are organized under various hierarchical modes. Some of the CLI commands can work only under a particular mode, which can prevent accidental misoperations. For example, configuration commands can only be used in configuration modes. StoneOS uses different prompts to indicate modes.

Execution Mode

When you log in StoneOS CLI, you are in the execution mode. Execution mode prompt is a pound sign (#):

hostname#

Global Configuration Mode

Commands in the global configuration mode are used to change device settings. To enter the global configuration mode, in the execution mode, use the command configuration. The global

configuration mode prompt is shown as follows:

hostname(config)#

Sub-module Configuration Mode

StoneOS has various functional modules. Some CLI commands only work in their corresponding sub-module configuration modes. To enter a sub-module configuration mode, in the global configuration mode, type a certain command. For example, to enter interface ethernet0/0 configuration mode, type interface ethernet0/0, and its command prompt is shown as follows:

hostname(config-if-eth0/0)#

Switching between CLI Modes

When you log into StoneOS CLI, you are in the execution mode. To switch to other CLI mode, type the commands in the table below.

Mode	Command
From execution mode to global configuration mode	configure
From global configuration mode to sub-module configuration mode	The command may vary, specifically depending on the sub-module configuration mode you want to enter
Return to a higher hierarchy	exit
From any mode to execution mode	end

CLI Error Message

StoneOS CLI checks the command syntax. Only correct command can be executed. StoneOS shows error message for incorrect syntax. The following table provides messages of common command errors:

Message	Description
Unrecognized command	StoneOS is unable to find the command or keyword
	Incorrect parameter type
	Input value excesses its defined value range
Incomplete command	User input is incomplete
Ambiguous command	User input is not clear

Command Input

To simplify input operation, you can use the short form of CLI commands. In addition, StoneOS CLI can automatically list available command keywords and fill incomplete commands.

Command Short Form

You can use only some special characters in a command to shorten your typing. Most of the commands have short form. For example, you can use **sho int** to check the interface information instead of typing **show interface**, and use **conf** to enter the configuration mode to replace the complete command **configure**.

Listing Available Commands

When you type a question mark (?), the system completes the unfinished commands or gives a list of available commands.

- If you type a question mark (?) behind an incomplete command, the system gives available commands (with short description) started with the last typed letter.
- If you type a question mark (?) at any level, the system displays a list of the available commands along with a short description of each command.

Completing Partial Commands

Command completion for command keywords is available at each level of the hierarchy. To complete a command that you have partially typed, press the Tab key. If the partially typed letters begin a string that uniquely identifies a command, pressing the Tab key completes the command; otherwise, it gives a list of command suggestions. For example, type **conf** in the execution mode and press TAB, the command **configure** appears.

Using CLI

This topic describes how to view previously typed commands and how to use CLI shortcut keys.

Previous Commands

StoneOS CLI can record the latest 64 commands. To scroll the list of the recently executed commands, press the up arrow key or use Ctrl-P; to scroll forward the list, press the down arrow key or use Ctrl-N. You can execute or edit the command texts displayed in the prompt.

Shortcut Keys

StoneOS CLI supports shortcut keys to save time when entering commands and statements. The following table gives the supported shortcut keys and their functions.

Shortcut Key	Action
Ctrl-A	Moves cursor to the beginning of the command line.
Ctrl-B	Moves cursor back one letter.
Ctrl-D	Deletes the letter at the cursor.
Ctrl-E	Moves cursor to the end of the command line.
Ctrl-F	Moves cursor forward one letter.
Ctrl-H	Deletes the letter before the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.

Shortcut Key	Action
Ctrl-N	Scrolls forward the list of recently executed commands.
Ctrl-P	Scrolls backward the list of recently executed commands.
Ctrl-T	Switches the character at the cursor and the one before it.
Ctrl-U	Deletes all characters on the command line.
Ctrl-W	Deletes all characters before the cursor.
META-B	Moves cursor to the beginning of the word.
META-D	Deletes the word after the cursor.
META-F	Moves cursor to the end of the word.
META-Backspace	Deletes the word before the cursor.
META-Ctrl-H	Deletes the word before the cursor.



Tip: For the computer without the META key, press ESC first and then press the letter. For example, to use shortcut key META-B, press ESC and then press B.

Filtering Output of Show Commands

In StoneOS CLI, the show commands display device configuration information. You can filter command output according to filter conditions separated by the pipe symbol (|). The filter conditions include:

- include {filter-condition}: Shows results that only match the filter condition. The filter condition is case sensitive.
- exclude {filter-condition}: Shows results that do not match the filter condition. The filter condition is case sensitive.

- begin {filter-condition}: Shows results that match the filter condition from the first one. The filter condition is case sensitive.

CLI output filter syntax is shown as follows:

hostname# **show command** | {**include** | **exclude** | **begin**} {*filter-condition*}

In this syntax, the first pipe symbol (|) is part of the command, while other pipe symbols just separate keywords, so they should not appear in the command line.

The filter conditions comply with the format of regular expression. The table below shows some common regular expressions and their meanings.

Regular Expression	Meaning
. (period)	Represents any character.
* (star)	Indicates that there is zero or more of the preceding element.
+ (plus)	Indicates that there is one or more of the preceding element.
^ (caret)	Used at the beginning of an expression, denotes where a match should begin.
$ (dollar)	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the $ character.
[] (square bracket)	Matches a single character that is contained within the brackets.
- (hyphen)	Separates the start and the end of a range.

CLI Page Display

The output messages of a command may be more than one page. When the output texts exceed one page, the CLI shows **-- More --** at the end of a page to indicate that there are more messages. In such a situation, you can make the following operations:

- To view the next line: press **Enter**.
- To terminate the output display: press the **Q** key.
- To view the next page, press any key other than **Enter** and **Q**.

Specifying Screen Size

You can specify the width and length of the CLI output screen which determines the extent of the output displayed before **-- More --** appears. The default screen length is 25 lines and the width is 200 characters.

To change the size of output screen, use the following commands:

- Width: **terminal width** *character-number*

  character-number – Specifies the number of characters. The value range is 64 to 512.

- Length: **terminal length** *line-number*

  line-number – Specifies the number of lines. CLI displays message lines one line less than the value specified here, but if the value is 1, the screen shows one line. The value range is 0 to 256. Setting the length to 0 disables page display option, which means it displays all messages without page split.

These settings are only available for the current connection and won't be saved to the configuration file of the device. If you close the terminal and login again, the screen width and length are restored to their default values.

Specifying Connection Timeout

Specifying connection timeout value is to set the maximum time that a session (over Console, SSH or Telnet) can be idle before the user is forced to log out.

To set the timeout value, in the global configuration mode, use the following commands:

console timeout *timeout-value*

- *timeout-value* – Specifies the timeout value for Console session. The range is 0 to 60 minutes. 0 means the session will never time out. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **no console timeout**.

ssh timeout*timeout-value*

- *timeout-value* - Specifies the timeout value for SSH session. The range is from 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **no ssh timeout**.

telnet timeout *timeout-value*

- *timeout-value* - Specifies the timeout value for Telnet session. The range is 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **no telnet timeout**.

Redirecting the Output of Show Commands

StoneOS allows you to redirect the output messages of show commands to other destinations including FTP server and TFTP server.

To redirect the output of show commands, use the following command:

show command | **redirect** *dst-address*

The destination address (*dst-address*) can be one of the following formats:

- FTP – ftp://[username:password@]x.x.x.x[:port]/filename
- TFTP – tftp://x.x.x.x/filename

Periodically Refreshing the Output of Show Commands

You are allowed to refresh the output messages of show commands according to the specified schedule. To periodically refresh the output messages of show commands, use the following command:

show command | **refresh** *refresh-value*

- *refresh-value* - Specifies the schedule of output refreshing. The value range is from 1 to 86,400 seconds.

Diagnostic Commands

You can use **ping** to determine if a remote network is reachable, or use **traceroute** to trace the route to a network device.

Viewing device Processes

You can view device process information, including the CPU usage, running time, status, memory usage, and IPC queue length of different processes.

To view the information, in any mode, use the following command:

show process

Example:

```
hostname(config)# show process
Tasks: 84 total, 11 running, 73 sleeping, 0 stopped
Pid Process State Priority Cpu(%) Memory(%) Runtime Fdnum ipcRecvqlen
  (process ID, process, status, priority, CPU usage, memory usage, running time, number of open files, IPC queue length)
1674 chassisd R 18 0.6 0.4 0:05.95 13 0  (R indicates that the process is running, the length of the IPC queue indicates the length of messages pending for the process, and 0 indicates that the process currently has no pending messages .)
4491 d-plane R 0 0.2 0.5 89:30.09 8 0
1639 monitord S 0 0.0 0.4 0:16.23 10 0  (S indicates that the process is sleeping.)
```

```
1675 licensed S 20 0.0 0.7 0:10.05 9 0
```

Chapter 1 Firewall

The chapter introduces the following topics:

- Configuration Environment describes how to access a device via Console port, Telnet, SSH and WebUI.
- Application Mode describes three types of application modes: transparent mode, mix mode, and routing mode.
- Deployment Mode describes three types of deployment modes: inline mode, bypass mode, and mix mode.
- StoneOS Architeture describes the basic components of StoneOS: interface, zone, VSwitch, VRouter, policy rule, and VPN.
- Zone describes the zone. Zones divide network into multiple segments, for example, trust, untrust, and so on.You can apply proper policy rules to zones to make the devices control the traffic transmission among zones.
- Interface describes the interface. Interfaces are used to connect devices, and transmit data.
- Address describes the address book. The address book contains address information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, session limit rules, etc.
- Custom IP Geolocation: describes how to customize the geographical locations of IP addresses.
- Service and Application describes the service book and application book. All of these applications and applications groups are stored in and managed by application book. All these service and service groups are stored in and managed by service book.

- DNS describes the function of Domain Name System. It is designed for TCP/IP network to look for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.
- DDNS describes the function of Dynamic Domain Name Server. It is designed to resolve fixed domain names to dynamic IP addresses.
- DHCP describes the function of Dynamic Host Configuration Protocol. It is designed to allocate appropriate IP addresses and related network parameters for subnets.
- PPPoE describes the function of Point-to-Point Protocol over Ethernet. It combines PPP protocol and Ethernet to implement access control, authentication and accounting on clients during IP address allocation.
- NAT describes the protocol for IP address translation in an IP packet header. When the IP packets pass through a firewall or router, the device or router will translate the source IP address and/or the destination IP address in the IP packets.
- Application Layer Identification and Control describes the function of Application Layer Gate. It can assure the data transmission for the applications that use multiple channels and assure the proper operation of VoIP applications in the strictest NAT mode.
- VLAN describes the function of Virtual LAN. A physical LAN can be divided into multiple broadcast domains.
- Super-VLAN describes the function of VLAN aggregation. It allows network devices that belong to different VLANS in one physical switching network to be allocated to one IPv4 subnet, and share one default gateway, thus optimizing IP address allocation.
- RSTP describes the function of Rapid Spanning Tree Protocol. It is designed to block the redundant links to avoid broadcast storm.

- Wireless Access Mode describes the wireless access mode: WLAN and 3G. You can use the wireless mode to access the network.

Configuration Environment

Overview

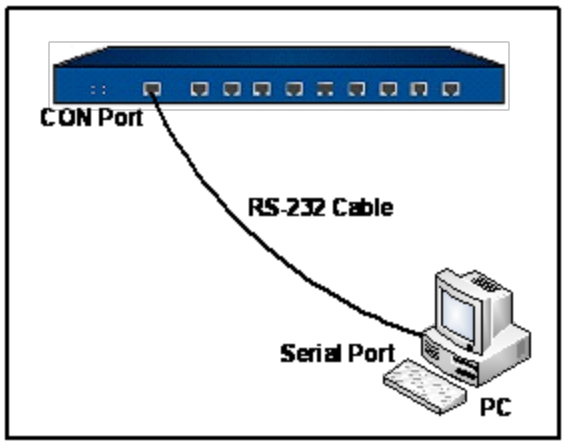
When the device has been properly installed, you need to set up an initial configuration environment before enabling the device to forward traffic. Use the following methods to set up configuration environment:

- Accessing a Device via Console Port
- Accessing a Device over Telnet
- Accessing a Device over SSH
- Accessing a Device via WebUI

Accessing a Device via Console Port

To directly connect a device using a cable inserted into the Console port, take the following steps:

1. Take a standard RS-232 cable. Connect one end of the cable to a computer's serial port, and the other end to a device's console port (labeled CON), as shown below:



2. In PC, start the terminal emulation program (HyperTerminal) and use the following parameters:

Parameter	Value
Baud	9600 bit/s **Note:**For A series, K series(except K2680 and K2380), and X8180, the default value is 115200bit/s.
Data	8
Parity	None
Stop	1
Flow Control	None

3. Power on the device and StoneOS starts up. Type the default login name (hillstone) and password (hillstone), and press Enter. Follow the prompts to change the default password, and then you can log in again with the new password.

4. You can use command line to configure the device and view its status. You can also type a question mark (?) for help.

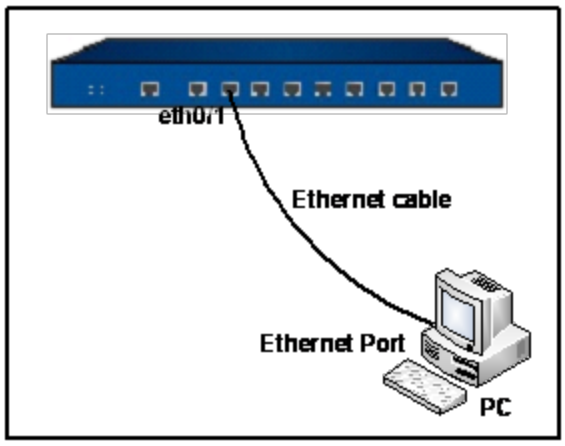
Accessing a Device via Telnet

If you want to use Telnet to connect a device, make sure the following conditions have been be established in advance:

- An IP address has been assigned to the access port with Telnet service enabled. (To enable Telnet on an interface, in the interface configuration mode, use the command **`manage telnet`**.When the Telnet service is enabled, the system will prompt that the protocol is not secure.)
- There is a correct route between the computer and the device.

To access to a device over Telnet, take the following steps:

1. Take a standard Ethernet cable. Connect one end of the cable to a PC, and put the other end into a device’s Ethernet port (or into a hub or switch), as shown below:



2. In the StoneOS command line interface, type the manage telnet command in the interface configuration mode to enable Telnet on that interface. (For more information about how to configure an interface, see Configuring an Interface Protocol).

3. Run a Telnet client program in your computer.

4. Type telnet and the IP address. If the connection is successfully established, the Telnet window shows “login”. Type the default login name (hillstone) and password (hillstone), and press Enter. Follow the prompts to change the default password, and then you can log in again with the new password.

5. You can use command line to configure the device and view its status. For help information, type a question mark (?).

Notes: If you use Telnet to configure the device, do not change the IP address used for Telnet connection. Otherwise, you cannot access the device over Telnet.

Accessing a Device over SSH

Secure Shell or SSH uses encryption to provide confidentiality and integrity for data in an insecure network environment. Hillstone device allows multiple SSH connections working

simultaneously.

To access a device over SSH, take the following steps:

1. Take a standard Ethernet cable. Connect one end of the cable to a PC, and put the other end into a device’s Ethernet port (or into a hub or switch).
2. In the StoneOS command line interface, type the command manage ssh in the interface configuration mode to enable SSH service on that interface. (For more information about how to configure an interface, see Configuring an Interface Protocol).
3. Run a SSH client software in your computer. You need to configure some SSH parameters, including IP address of the device, SSH version and RSA key, etc.
4. If the connection is successfully established, a login: prompt will appear. Enter the default administrator username “hillstone” and press Enter. Behind the prompt for password, enter the default password “hillstone” and press Enter to log in.
5. You can use command line to configure the device and view its status. For help information, type a question mark (?).

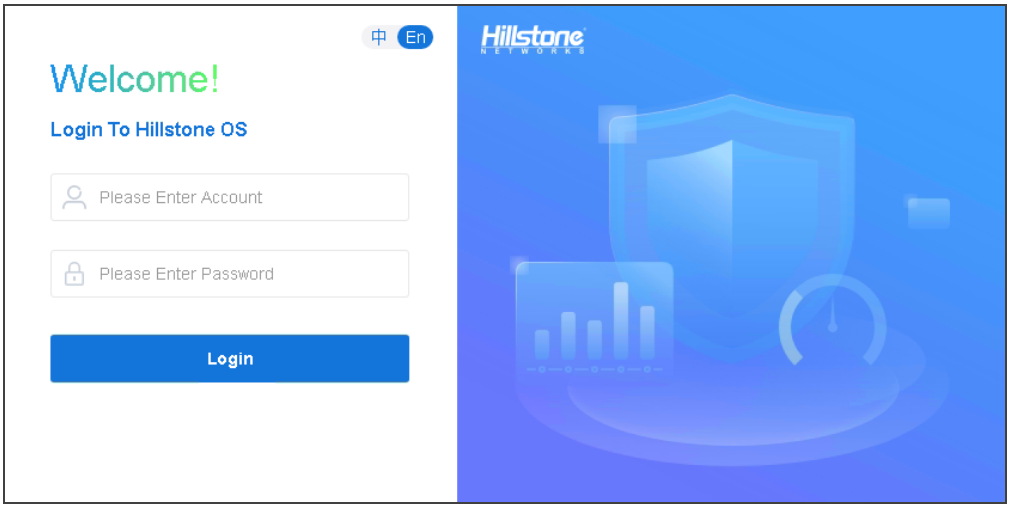
Accessing a Device via WebUI

Web User Interface (WebUI) provides a more direct and effective method for you to interact with the device and view its responses.

Interface ethernet0/0, with default IP address 192.168.1.1/24, has its SSH, PING, SNMP and HTTPS services enabled. When you use a new Hillstone device, you can visit its Web User Interface after finishing the following steps:

1. Assign an IP address to your PC. The address should be of the same subnet with 192.168.1.1/24. Use an Ethernet cable to connect your PC and the ethernet0/0 port.

2. In the PC, launch a Web browser and visit the address https://192.168.1.1. The login page is shown below.



3. In the login interface, type the default username and password: hillstone/hillstone.

4. At the first sign of address, the user needs to read and accept the EULA (end-user license agreements), click **EULA** to view the details of EULA.

5. Click **Login**, follow the prompts to change the default password, and then log in again with the new password.

Now, you can view or configure the device as needed.

Logging in by Using Certificate Authentication

To improve the security, you can log into the device by using the certificate authentication function of the client. The certificate includes the digital certificate of users and secondary CA certificate signed by the root CA.Certificate authentication is one of two-factor authentication. Two-factor authentication is not only needing the user name and password authentication, but also needing other authentication methods,such as certificate or fingerprint. After enabling this authentication method and logging into the device over HTTPS, you need to first select certificate and then enter the password.



Notes:

- The digital certificate of client is signed by root CA.
- Secondary CA certificate is trusted by root CA so that the system can authenticate user.

To enabling this authentication mehod, configure the settings in both the device side and the client side.

Configuring the Device Side

To enable the certificate authentication of the client, take the following steps:

1. To enable the certificate authentication of the client:

   In the global configuration mode, execute the **https client-auth enable**command.

2. To configure the PKI trust domain and import the CA root certificate:

   a. aIn the global configuration mode, execute the **pki trust-domain** *trust-domain-name* command to create a new PKI trust domain.

   b. In the execution mode, execute the **import pki** *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name* command to import the CA root certificate to PKI trust domain from many storages including FTP,TFTP and USB.

   c. In the global configuration mode, execute the **https client-auth trust-domain** *trust-domain-name* command to specify the trust domain of certificate authentication. The system verifies the validity of the CA signature of the certificate in the client by using the CA root certificate stored in this PKI trust domain. The trust domain is the one that you create in the above steps.

3. If needed, you can configure the CN Check function. In this case, the system checks the CN field of the client certificate when the user logs into the device. Only when the CN field of the client certificate matches the username can the user successfully log into the device..

   In the global configuration mode, execute the **https client-auth match cn**command. This function is enabled by default.

Configuring the Client Side

You may import one or two certificates into your client’ s Web browser or USB Key. If you have imported two certificates, choose one when selecting certificate.After configuring the device side, you will need to configure the client side. The steps below use the certificates in the client Web browser to authenticate as an example:

1. Import the digital certificate to the client Web browser.
   a. In the Web browser, for example, Internet Explorer, select **Tools > Internet options > Content > Certificate > Personal**.
   b. Click **Import**.
   c. In the pop-up window, follow the wizard to import the certificate.
2. In the PC, launch a Web browser and visit the address https://IP-Address(IP-Address refers to the IP address of manageable interface).
3. A dialog appears and asks you to select the proper certificate from the certificate list.
4. Click **OK**. The login page appears.
5. Enter the username and password and click Login. If you have configured the https client-auth match cn command, the username you entered must be the same as the CN value of the CA certificate.



Notes: To authenticate with the certificates in the client Web browser, you should be noted that:

- Make sure the USB Key has been inserted into the USB interface of PC before logging.
- Feitianchengxin USB Key(the authentication USB Key issued by Hillstone) comes with driver and Hillstone Usertools. After installing driver and this tool following the installation wizard, you can import digital certificates to the USB Key with Hillstone Usertools.
- You need to enter USB Key user password(1234 by default) when importing digital certificates to the USB Key.

Unfreezing the WebUI

This function can be used only for CloudEdge deployed on the e Cloud. When CloudEdge is deployed on the e Cloud, the e Cloud can manage CloudEdge via License Management System (LMS). If the authorization of CloudEdge purchased on the e Cloud expires (that is, the available period of CloudEdge authorized by the e Cloud expires), the e Cloud will freeze the WebUI of CloudEdge through LMS. During the freeze period, you cannot access the WebUI of CloudEdge. If you try to log in to the WebUI of CloudEdge with your user name and password, the login page will prompt: "Error: WebUI is frozen, cannot use WebUI". When the user renews the authorization of CloudEdge on the e Cloud (that is, renews the available period of CloudEdge), the e Cloud will unfreeze the WebUI of CloudEdge through LMS.

Usually, the freezing and unfreezing operations are automatically performed by e Cloud and LMS. When CloudEdge loses contact with LMS, the freezing and unfreezing operations will fail. In this case, you can unfreeze the WebUI via CLI.

To unfreeze the WebUI of CloudEdge, in any mode, use the command:

exec webui unfreeze

Application Mode

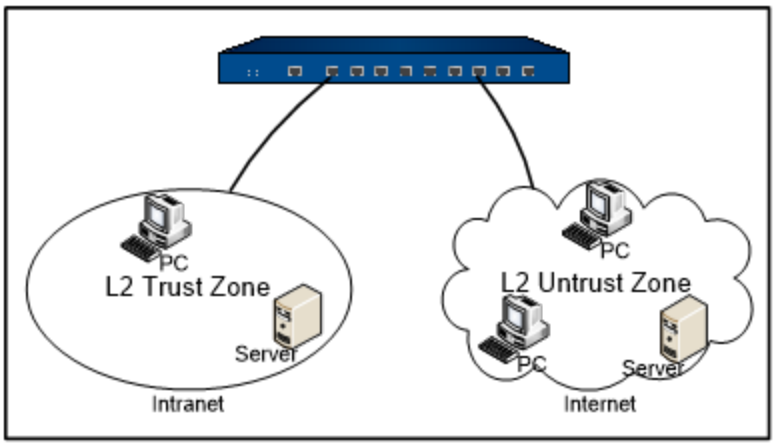
Overview

Hillstone devices support three types of application modes: transparent mode, mix mode, and routing mode. The system will choose a proper mode according to the packets received. This chapter will describe the three applications modes in details.

Transparent Mode

To build the transparent application mode, you must create some L2 zones, bind interfaces to the L2 zones and then bind the L2 zones to the VSwitch. If necessary, you can create multiple VSwitches. The transparent mode takes the following advantages:

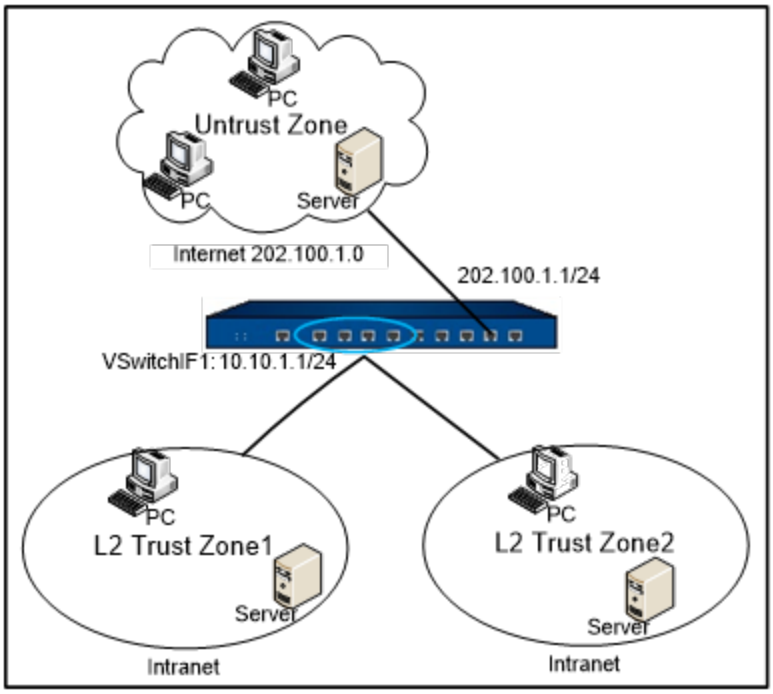
- Do not have to change the IP addresses of the protected network.
- No NAT rules are needed.



As shown above, an interface the L2 Trust Zone connects to the Intranet, and an interface in the L2 Untrust Zone connects to the Internet.

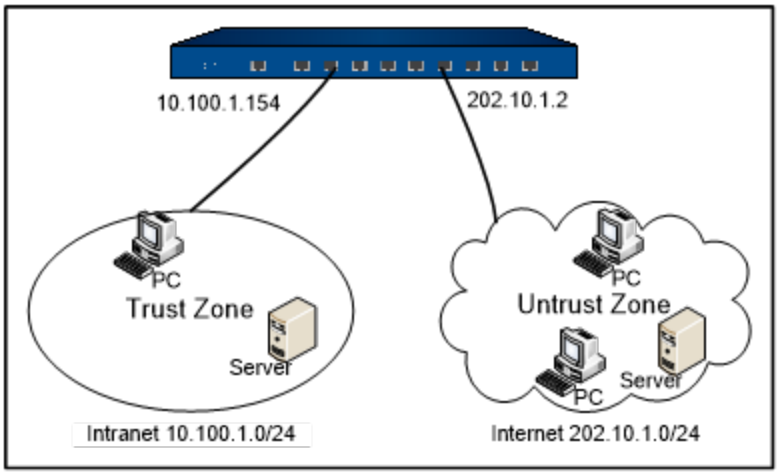
Mix Mode

To build the mix application mode, you must bind some interfaces to L2 zones and some interfaces to L3 zones, and configure IP addresses for VSwitchIF and L3 interfaces. Figure below shows the topology of the mix mode.



Routing Mode

To build the routing mode, you must bind the interfaces to L3 zones, configure IP address to the interfaces according to network topology and security requirements, and configure proper policy rules. Under the routing mode, the device performs both the routing function and the security function. And also NAT is supported under this mode. In such a case, the device is deployed between the trust zone and the untrust zone. Figure below Fshows the topology of the routing mode.



VSwitch

Hillstone devices might allow packets between some interfaces to be forwarded in Layer 2 (known as transparent mode), and packets between some interfaces to be forwarded in Layer 3 (known as routing mode), specifically depending on actual requirement. To facilitate a flexible configuration of mix mode of Layer 2 and Layer3, StoneOS introduces the concept of Virtual Switch (VSwitch). By default StoneOS ships with a VSwitch known as VSwitch1. Each time you create a VSwitch, StoneOS will create a corresponding VSwitch interface (VSwitchIF) for the VSwitch automatically. You can bind an interface to a VSwitch by binding that interface to a security zone, and then binding the security zone to the VSwitch.

A VSwitch acts as a Layer 2 forwarding zone, and each VSwitch has its own independent MAC address table, so the packets of different interfaces in one VSwitch will be forwarded according to Layer 2 forwarding rules. You can configure policy rules conveniently in a VSwitch. A VSwitchIF virtually acts as an upstream switch interface, allowing packets forwarding between Layer 2 and Layer 3.



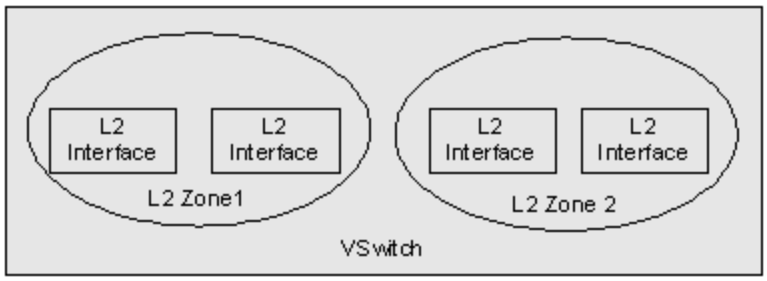
Tip: For more information about VSwitch configuration, see Interface.

Basic Concepts

This section describes two basic concepts: L2 zones and L2 interfaces.

L2 Zones

To support policy rules for VSwitches, here introduces the concept of L2 zones. When creating a zone, you have to identify whether it is a L2 zone. To bind an interface to a VSwitch, you must bind it to a L2 zone first and then bind the L2 zone to the VSwitch. Figure below shows the relationship among VSwitch, L2 zone, and L2 interface.



L2 Interfaces

A physical interface and its sub-interfaces can belong to different interfaces. An interface bound to a L2 zone is a L2 interface. But only the interface with no IP configured can be bound to a L2 zone. A VSwitchIF is a L3 interface which cannot be bound to a L2 zone.

Forwarding Rules in VSwitch

StoneOS creates a MAC address table for a VSwitch by source address learning. Each VSwitch has its own MAC address table. StoneOS handles with the packets according to the types of the packets, including IP packets, ARP packets, and non-IP-non-ARP packets.

The forwarding rules for IP packets are:

1. Receive a packet.
2. Learn the source address and update the MAC address table.
3. If the destination MAC address is a unicast address, the system will look up the egress interface according to the destination MAC address. And in this case, two situations may occur:
    - If the destination MAC address is the MAC address of the VSwitchIF with an IP configured, the system will forward the packet according to the related routes; if the destination MAC address is the MAC address of the VSwitchIF with no IP configured, the system will drop the packet.

- Figure out the egress interface according to the destination MAC address. And if the egress interface is the source interface of the packet, the system will drop the packet; otherwise, forward the packet from the egress interface.

If no egress interfaces (unknown unicast) is found in the MAC address table, jump to Step 6 directly.

4. Figure out the source zone and destination zone according to the ingress and egress interfaces.

5. Look up the policy rules and forward or drop the packet according to the matched policy rules.

6. If no egress interface (unknown unicast) is found in the MAC address table, the system will send the packet to all the other L2 interfaces. The sending procedure is: take each L2 interface as the egress interface and each L2 zone as the destination zone to look up the policy rules, and then forward or drop the packet according to the matched policy rule. In a word, forwarding of unknown unicast is the policy-controlled broadcasting. Process of broadcasting packets and multicasting packets is similar to the unknown unicast packets, and the only difference is the broadcast packets and multicast packets will be copied and handled in Layer 3 at the same time.

For the ARP packets, the broadcast packet and unknown unicast packet are forwarded to all the other interfaces in the VSwitch, and at the same time, the system sends a copy of the broadcast packet and unknown unicast packet to the ARP module to handle with.

For the non-IP-non-ARP packets, you can specify the action using the following command in the global configuration mode:

l2-nonip-action {drop | forward}

- **drop** – Drops the packet.
- **forward** – Forwards the packet.

Configuring a VSwitch

There is a default VSwitch named VSwtich1 in the system. You cannot delete VSwitch1. You can create new VSwitches according to your needs. And also you can view the VSwitch configuration information at any time.

When you create a new VSwitch, a corresponding VSwitchIF is created automatically.

To create a VSwitch, in the global configuration mode, use the following command:

vswitch vswitch*Number*

- *Number* – Specifies the numeric identification for the VSwitch. The value range varies from different platforms. For example, the command **vswitch vswitch2** creates a VSwitch named VSwitch2 and the corresponding VSwitchIF named VSwitchif2, and at the same time, you enter the VSwitch2 configuration mode. If the specified VSwitch name exists, you will enter the VSwitch configuration mode directly.

To delete the VSwitch with its VSwitchIF, in the global configuration mode, use the following command:

no vswitch vswitch*Number*

To view the configuration information of the VSwitch, in any mode, use the following command:

show vswitch [*vswitch-name*]

- *vswitch-name* – View the information of the specified VSwitch.

Viewing MAC Table Information

You can view or clear the MAC table information of all the VSwitches or specified interfaces.

To view the information, in any mode, use the following command:

show mac [**generic**] | [**interface** *interface-name*]

- **generic** – Shows the statistics of the MAC table, including how many entries in the table and how many entries are being used.
- **interface** *interface-name* – Shows the MAC entries of the specified interface.

To clear the MAC entries, in the execution mode, use the following command:

clear mac [**interface** *interface-name*]

Virtual Wire

Hillstone devices support VSwitch-based Virtual Wire. With this function enabled and Virtual Wire interface pair configured, two Virtual Wire interfaces form a virtual wire that connects the two sub-networks attaching to Virtual Wire interface pair together. The two connected sub-networks can communicate directly on Layer 2, without other sub-network's forwarding. Furthermore, controls of policy rules or other functions are still available when Virtual Wire is used.

Virtual Wire operates in two modes, which are Strict and Non-Strict mode respectively, as detailed below:

- Strict Virtual Wire mode: In this mode, Hillstone devices does not need to perform MAC address learning. Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in the mix mode. Any PC connected to the Virtual Wire interface can neither manage the device nor access Internet over this interface.
- Non-Strict Virtual Wire mode: In this mode, Hillstone can perform MAC address learning. Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Mix mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding.

Table below lists packet transmission conditions in Strict Virtual Wire and Non-Strict Virtual Wire mode. You can choose an appropriate Virtual Wire mode according to the actual requirement.

Packet	Strict	Non-Strict
Egress and ingress are interfaces of one Virtual Wire interface	Allow	Allow

Packet	Strict	Non-Strict
pair		
Ingress is not Virtual Wire's interface	Deny	Deny
Egress and ingress are interfaces of different Virtual Wire interface pairs	Deny	Deny
Ingress of to-self packet is a Virtual Wire’ s interface	Deny	Allow
Ingress is a Virtual Wire's interface, and egress is a L3 interface	Deny	Allow

Configuring a Virtual Wire

To configure the Virtual Wire function, you need to enable the Virtual Wire function of the VSwitch and configure the Virtual Wire interface pair.

Enabling Virtual Wire

By default, the Virtual Wire function of VSwitch is disabled. To enable the Virtual Wire function, in the VSwitch configuration mode, use the following command:

virtual-wire enable [**strict** | **unstrict**]

- **strict** | **unstrict** – Specifies the Virtual Wire mode. It can be strict (strict) or non-strict (unstrict). The strict mode will be used if you keep this parameter un-configured.

To disable the Virtual Wire function, in the VSwitch configuration mode, use the following command:

no virtual-wire enable

Configuring a Virtual Wire Interface Pair

A Virtual Wire interface pair forms a virtual wire to transmit the conformed L2 packets. The supported maximum number of Virtual Wire interface pairs varies from different platforms.

To configure a Virtual Wire interface pair, in the VSwitch configuration mode, use the following command:

virtual-wire set *interface-name1 interface-name2*

- *interface-name1 interface-name2* – Specifies the interface for the interface pair. The two interfaces of one Virtual Wire cannot be the same, and the same one interface cannot belong to two interface pairs.

To delete the specified interface pair, in the VSwitch configuration mode, use the following command:

no virtual-wire set *interface-name1 interface-name2*

Viewing Virtual Wire Configuration Information

In any mode, use command **show vswtich** *vswitch-name*to view the Virtual Wire status and mode. To view the configuration information of Virtual Wire interface pair, in any mode, use the following command:

show virtual-wire [**vswitch** *vswitch-name*]

- **vswitch** *vswitch-name* – Views the Virtual Wire interface pair information of specified VSwitch. All the configured Virtual Wire interface pair information will be displayed if you keep this parameter un-configured.

NSH Proxy

Only Hillstone CloudEdge virtual firewall supports the NSH proxy function. NSH (Network Service Header) is a protocol used to provide Service Chain in SFC (Service Function Chain) architecture. The definition and instantiation of an ordered set of service functions and its subsequent "forwarding" of traffic through them is called SFC. It is mainly used for end-to-end services. It adds NSH in the original messages to make the messages pass through multiple Service devices in sequence according to the specified path.

CloudEdge supports the layer 2 NSH proxy function , which can encapsulate and forward layer 2 NSH packets. Generally, there are two modes when you arrange services through SFC: two-armed

mode and one-armed mode. In the two-arm mode, packets come in and get out through different interfaces; while in the one-arm mode, packets come in and get out though the same interface.

Enabling NSH layer 2 Proxy

To enable the NSH layer 2 proxy function, in the VSwitch configuration mode, use the following command:

virtual-wire set*interface-name1 interface-name2***nsh-proxy**

- *interface-name1 interface-name2* – Specify the egress and ingress interfaces for forwarding NSH layer 2 proxy traffic. In the two-arm mode of SFC, the egress and ingress interfaces should be configured as two different interfaces. In the one-arm mode, the egress and ingress interfaces need to be configured as the same interface.

To disable the NSH layer 2 proxy function, in the VSwitch configuration mode, use the following command:

no virtual-wire set*interface-name1 interface-name2*

NSH Proxy Debugging

To enable the NSH Proxy debugging , in any mode, use the following command:

debug dp nsh

To disable the NSH Proxy debugging , in any mode, use the following command:

undebug dp nsh

Viewing the NSH Packets on Interfaces

To view the packets on the NSH proxy interfaces, in any mode, use the following command:

show nsh-proxy-counter

Viewing the NSH Sessions

To view the NSH sessions, in any mode, use the following command:

show session nsh

Viewing Virtual Wire and NSH Proxy Configurations

In any mode, you can use the command **show vswtich***vswitch-name*to view the status and mode of virtual wire . To view the configuration information of virtual wire interface pair and NSH proxy , in any mode, use the following command:

show virtual-wire [**vswitch***vswitch-name*]

- **vswitch***vswitch-name* – Displays the virtual wire interface pair and NSH proxy information of the specified VSwitch. If the parameter is not specified, all the configured virtual wire interface pair and NSH proxy information will be displayed.

VLAN Transparent in the Transparent Mode

In the transparent mode, when there are multiple VLANs on the physical interfaces,, you have to configure the corresponding sub-interfaces and multiple L2 forwarding zones (VSwitch) to transmit all the VLAN packets. In this case, the traffic can be fine-grained controlled with policy rules among different VLANs. However, the more VLANs there are, the more complex the configuration is. To simplify the configuration, the system provides the VSwitch based VLAN transparent function. With this function, you do not have to configure the sub-interfaces, and the system forwards the VLAN tagged packets transparently without tag changed.

By default, VLAN transparent in the VSwitch is disabled. To enable it, in the VSwitch configuration mode, use the following command:

forward-tagged-packet

To disable VLAN transparent, in the VSwitch configuration mode, use the following command:

no forward-tagged-packet

VSwitch supports the double-tagged VLAN transparent function in the QinQ scenario. To enable this function, in the VSwitch configuration mode, use the following command:

forward-double-tagged-packet

To disable the double-tagged VLAN transparent function in the QinQ scenario, in the VSwitch configuration mode, use the following command:

no forward-double-tagged-packet

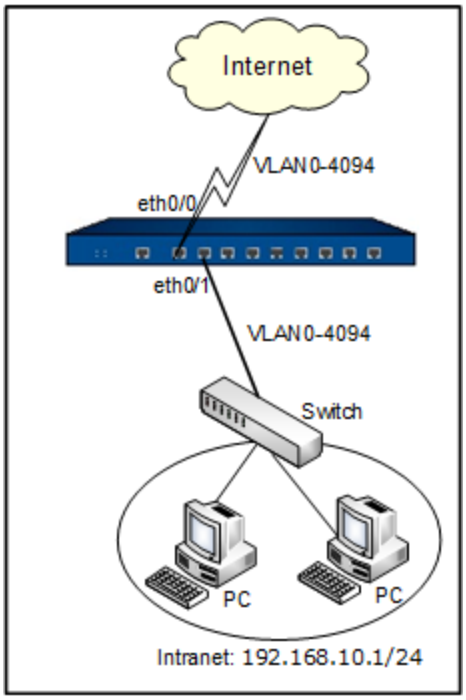
Notes: When configuring and using the VLAN transparent function, you should keep in mind that:

- VSwitch that contains sub-interfaces cannot enable VLAN transparent.
- The L2 zone in the VSwitch with VLAN transparent enabled cannot bind sub-interfaces.
- Transparently transmitted VLAN tagged packets cannot be transmitted in Layer 3.

Configuration Example

The Hillstone device is applied in the transparent mode. The interface ethernet0/0 connects to Internet, and ethernet0/1 connects the Intranet, the Intranet address is 192.168.10.1/24. Both ethernet0/0 and etherent0/1 should carry the VLAN tagged packets from 0 (means no ID) to 4094.

The goal is to specially control the VLAN packets tagged 2 by a policy rule and control other VLAN tagged packets with a common policy rule. Figure below shows the topology.



Configuration Steps

Step 1: Configure VSwitch1, and make the system forward the VLAN tagged packets (except for the packets with ID 2) transparently through VSwitch1

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# forward-tagged-packet
hostname(config-vswitch)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-untrust
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Create VSwitch2 for the VLAN packets tagged 2

```
hostname(config)# vswitch vswitch2
```

```
hostname(config-vswitch)# exit
hostname(config)# zone l2-trust2 l2
hostname(config-zone-l2-tru~)# bind vswitch2
hostname(config-zone-l2-tru~)# exit
hostname(config)# zone l2-untrust2 l2
hostname(config-zone-l2-tru~)# bind vswitch2
hostname(config-zone-l2-tru~)# exit
hostname(config)# interface ethernet0/0.2
hostname(config-if-eth0/0.2)# zone l2-untrust2
hostname(config-if-eth0/0.2)# exit
hostname(config)#
```

Step 3: Configure the policy rules

```
hostname(config)# address address1
hostname(config-addr)# ip 192.168.10.1/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from address1 to any from-zone l2-trust2 to-zone l2-untrust2 service any permit
hostname(config)# rule id 2
hostname(config-policy-rule)# src-zone l2-trust2
hostname(config-policy-rule)# dst-zone l2-untrust2
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config-policy)# rule from any to any from-zone l2-trust to-zone l2-untrust service any permit
Rule id 3 is created
hostname(config-policy)# exit
```

```
hostname(config)#
```

Configuring Transparent ARP

In the transparent application mode, ARP learning is disabled by default. You can enable or disable ARP learning manually to obtain IP-MAC binding information. To enable or disable ARP learning, in the VSwitch configuration mode, use the following command:

- Enable: **arp-l2mode**
- Disable: **no arp-l2mode**

Configuring a VRouter

There is a default VRouter in the system named trust-vr. The default VRouter cannot be deleted. After enabling the multi-VR function, you can create more VRouters according to your own needs.

Enabling and Disabling Mult-VR

By default, the multi-VR function is disabled, and you cannot create other VRs.

To enable or disable the multi-VR function, in any mode, use the following command:

- Enable: **exec vrouter enable**
- Disable: **exec vrouter disable**

After multi-VR is enabled or disabled, the system must reboot to make it take effect. After rebooting, system's max concurrent sessions might decrease if the function is enabled, or restore to normal if the function is disabled. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 835.

If multi-VR is enabled, traffic can traverse up to 3 VRs, and any traffic that has to traverse more than 3 VRs will be dropped.

Creating a VRouter

After enabling the multi-VR function and rebooting the system, to create a new VRouter and enter the VRouter configuration mode, in the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of the VRouter to be created. If the specified name exists, you will enter the VRouter configuration mode directly.

To delete the specified VRouter, in the global configuration mode, use the following command:

no ip vrouter *vr-name*

Viewing VRouter Information

To view the VRouter information, in any mode, use the following command:

show ip vrouter [*vrouter-name*]

- *vrouter-name* – View the information of the specified VRouter. Information of all the VRouters in the system will be displayed if you keep this parameter un-configured.

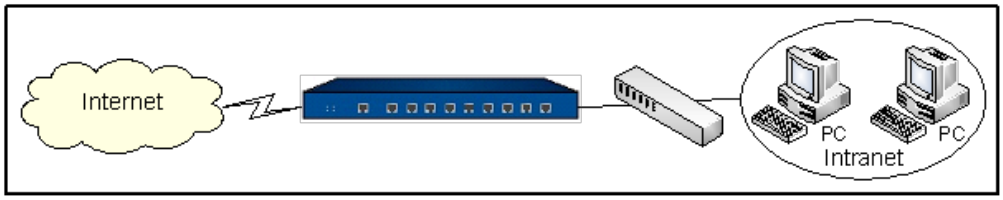
Deployment Mode

Overview

Hillstone device supports three types of deployment modes, which are inline mode, bypass mode, and mix mode. This chapter introduces the three modes in brief and describes the principle and configuration of the bypass mode in details.

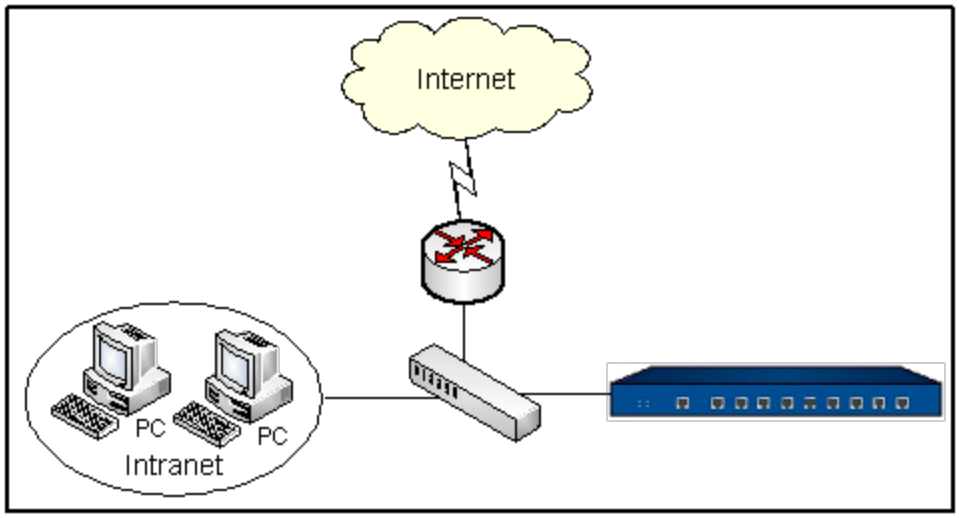
Inline Mode

In most of the situations, Hillstone device will be deployed inline mode. Under this mode, the device will analyze, control, and forward the network traffic. Figure below shows the inline mode topology.



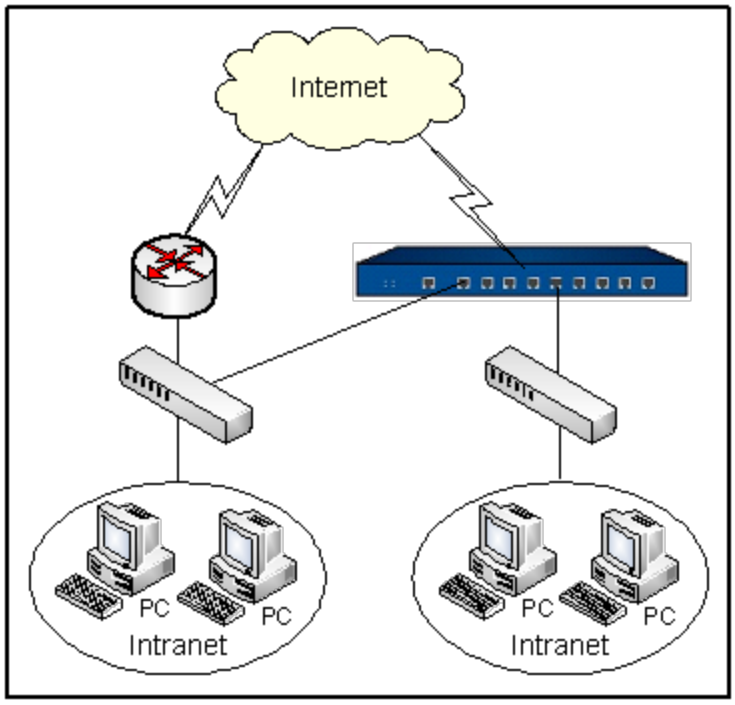
Bypass Mode

Some functions on the device can work in both the inline mode and the bypass mode, such as IPS, AV, statistics, and network behavior control. When the device is working under the bypass mode, it monitors, scans, and logs the traffic without forwarding them. In this case, the device failure will not impact the traffic transmitting in the network. The bypass mode is a better choice for the auditing-only situations. Figure below shows the bypass mode topology.



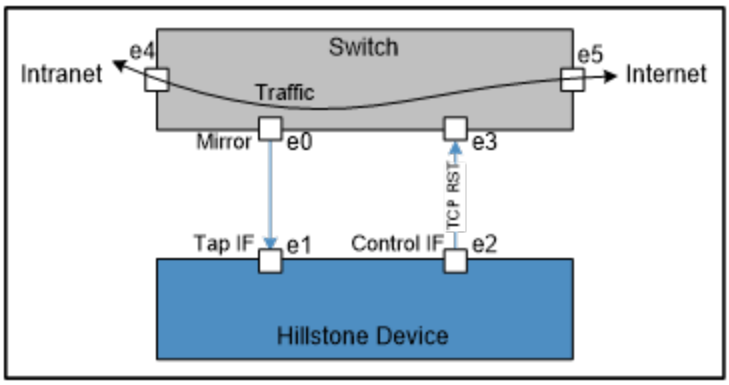
Mix Mode

Hillstone device works under the inline mode naturally. After configuring the bypass mode on the device, it works under the mix mode of inline and bypass. Figure below shows the mix mode topology.



Working Principle of Bypass Mode

The bypass mode of Hillstone device is realized by configuring related parameters on interfaces. Bind a physical interface to a Tap zone (function zone for bypass mode) to make it a bypass interface. And then the device will monitor, scan, or record the traffic received in the bypass interface. Figure below shows the working principle illustration of bypass mode.



As shown in the illustration above, the Hillstone device deployed in the network under the bypass mode. The interface e1 is the bypass interface and e2 is the bypass control interface. The interface e0 is the mirror interface of the switch.

The switch mirrors the traffic to e1 and Hillstone device will monitor, scan, and log the traffic received from e1.

After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections.

Configuring Bypass Mode

Configurations of bypass mode include:

- Creating a Tap Zone
- Binding an Interface to a Tap Zone
- Configuring a Bypass Control Interface

- Specifying a Statistical Range
- Configuring a Linkage Firewall

Creating a Tap Zone

To deploy the device in the bypass mode, you must create a Tap zone and bind a physical interface to the Tap zone.

To create a Tap zone, in the global configuration mode, use the following command:

zone *zone-name* **tap**

- *zone-name* - Specifies the name of the zone.

If the specified name exists, you will enter the zone configuration mode directly.

After configuring a Tap zone, the system will automatically create a policy rule whose source and destination zones are both the created Tap zone.

To delete the specified zone, in the global configuration mode, use the command

no zone zone-name.

Binding an Interface to a Tap Zone

An interface bound to a Tap zone is a bypass interface. A physical interface, an aggregate interface, a tunnel interface or a redundant interface can be configured as a bypass interface. A bypass interface cannot have sub-interfaces.

To bind an interface to a Tap zone, in the interface configuration mode, use the following command:

zone *zone-name*

To cancel the binding, in the interface configuration mode, use the command **no zone**.

Configuring a Bypass Control Interface

A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if

the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections.

By default, the bypass control interface is the bypass interface itself. For tunnel interfaces, if the interface itself is used as the control interface, the control message sent by the tunnel interface may not be processed correctly. It is recommended that bypass tunnel interfaces be configured with other interfaces as control interfaces. When configuring, ensure that the control interface can send messages to the switch normally.

To configure a bypass control interface, in the bypass interface configuration mode, use the following command:

tap control-interface *interface-name*

- *interface-name* - Specifies the name of the interface.

To cancel the specified bypass control interface, in the bypass interface configuration mode, use the command **no tap control-interface**.

Specifying a Statistical Range

When the statistic set grouped by IP is enabled, in order to get more precise statistical data, you can specify a LAN address, namely the statistical range. Packets whose source IP is out of the specified range will not be counted.

To specify the statistical range, in the bypass interface configuration mode, use the following command:

tap lan-address {*ipv4-address-entry* | *ipv6-address-entry*}

- *ipv4-address-entry* - Specifies the name of the IPv4 address entry. Generally speaking, this address entry should contain all the IPv4 LAN addresses on the monitored device.
- *ipv6-address-entry* - Specifies the name of the IPv6 address entry. Generally speaking, this address entry should contain all the IPv6 LAN addresses on the monitored device.

To cancel the specified statistical range, in the bypass interface configuration mode, use the command **no tap lan-address**.

Configuring a Linkage Firewall

Users can configure a linkage firewall, when current device is working in the TAP mode and the bypass interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic:

- The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service;
- The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block;
- The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the end point profile that referenced by the security policy is Block;
- The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP.

To configure a linkage firewall, in the bypass interface configuration mode, use the following command:

tap firewall {**ip** *ipv4-address* | **ipv6** *ipv6-address*} [**protocol ssh** [**port** *port-number*]] **username** *username* **password** *password* [**vrouter** *vrouter-name*]

- **ip** *ipv4-address* | **ipv6** *ipv6-address* - Specifies the IPv4 or IPv6 address of the linkage firewall.
- **protocol ssh** [**port** *port-number*] - Specifies the port number of the SSH protocol. The range is 1 to 65535. The default value is 22.

- **username** *username* **password** *password* - Specifies the username (**username** *username*) and password (**password** *password* to log in to the linkage firewall. The range of the username is 1 to 31 characters. The range of the password is 1 to 31 characters.
- **vrouter** *vrouter-name* - Specifies the VRouter of the linkage firewall. The default value is the default VRouter in the system named trust-vr.

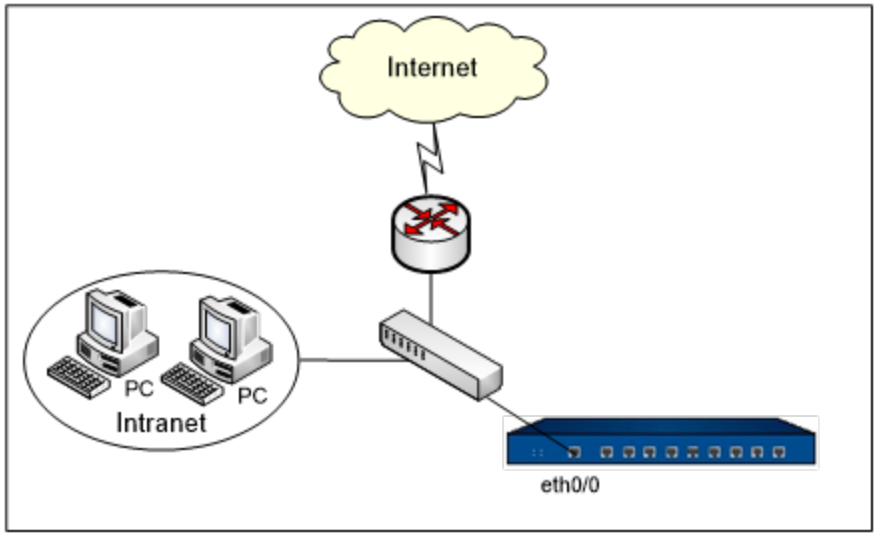
In the bypass interface configuration mode, use the command **no tap firewall** [**ip** | **ipv6**] to cancel the specified linkage firewall.

Example of Configuring Bypass Mode

This section describes a bypass mode configuration example.

Topology

A Hillstone device is deployed in the network under the bypass mode. The IPS function is enabled. The interface ethernet0/0 is configured as the bypass interface which is used to receive the mirrored traffic from the switch. Figure belowshows the topology.



Configuration Steps

Step 1: Create the Tap zone and bind an interface to the Tap zone

```
hostname(config)# zone tap1 tap
hostname(config-zone-tap1)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone tap1
hostname(config-if-eth0/0)# exit
hostname(config)#
Because etherent0/0 is configured as the bypass inter-
face, it also is the default bypass control interface
```

Step 2: Bind the IPS profile to the Tap zone

Bind the configured IPS profile named ips-profile1 to the Tap zone

```
hostname(config)# zone tap1
hostname(config-zone-tap1)# ips enable ips-profile1
hostname(config-zone-tap1)# exit
hostname(config)#
```

StoneOS Architecture

Overview

StoneOS is the firmware running on the Hillstone devices. The basic components of StoneOS include interface, zone, VSwitch, VRouter, policy rule, and VPN.

Interfaces

Interfaces allow inbound and outbound traffic to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.



Tip: For more information about interfaces, see Interface.

Zones

Zones divide network into multiple segments, for example, trust (usually refers to the trusted segments such as the Intranet), untrust (usually refers to the untrusted segments where security treats exist), and so on. You can apply proper policy rules to zones to make the devices control the traffic transmission among zones. There are eight predefined security zones in StoneOS, which are trust, untrust, dmz, L2-trust, L2-untrust, L2-dmz, vpnhub (VPN functional zone) and ha (HA functional zone).



Tip: For more information about zones and policy rules, see Zone and Policy.

VSwitches

VSwitch is short for Virtual Switch. A VSwitch functions as a switch in Layer 2. After binding a Layer 2 zone to a VSwitch, all the interfaces in the zone are also bound to the VSwitch. There is a default VSwitch named VSwitch1. By default, all Layer 2 zones will be bound to VSwitch1. You can create new VSwitches and bind Layer 2 zones to VSwitches.

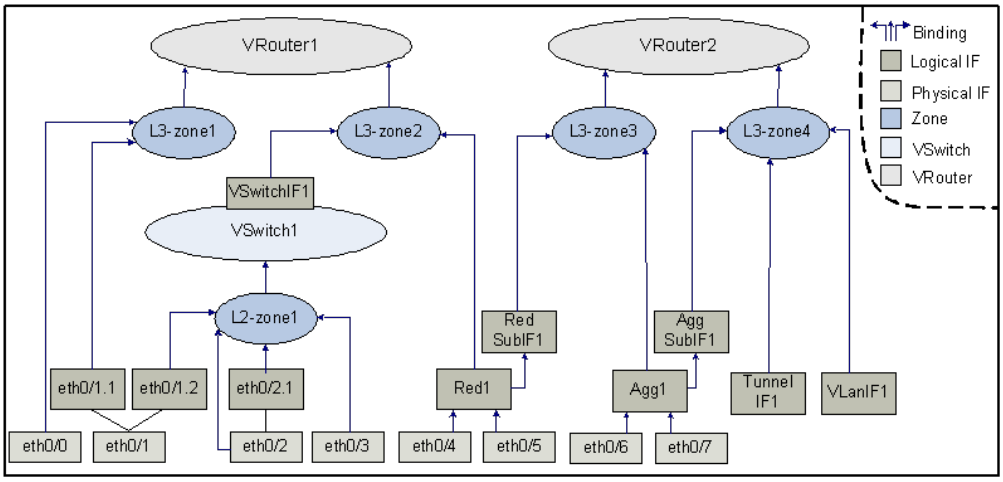
Each VSwitch is a Layer 2 forwarding zone with its own MAC address table which supports the Layer 2 traffic transmission for the device. Furthermore, the VSwitchIF helps on the traffic transmission between Layer 2 and Layer 3.



Tip: For more information about VSwitch, see Deployment Mode.

VRouter

VRouter is the short form for Virtual Router and also abbreviated as VR. A VRouter functions as a router with its own routing table. There is a default VR named trust-vr. By default, all the Layer 3 zones will be bound to trust-vr automatically. The system supports the multi-VR function and the max VR number varies from different platforms. Multiple VRs make the device work as multiple virtual routers, and each virtual router uses and maintains its own routing table. The multi-VR function allow a device to achieve the effects of the address isolation between different route zones and address overlapping between different VRs, as well as to avoid route leaking to some extent, enhancing route security of network. For more information about the relationship between interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationships among them are:

- Interfaces are bound to security zones. Interfaces bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; interface and its sub interface can belong to different security zones.
- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the predefined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the predefined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwtich or VR.

Policy

Policy is the basic function of Hillstone devices that is designed to control the traffic forwarding between security zones/segments. By default Hillstone devices will deny all traffic between security zones/segments, while the policy can identify which flow between security zones or segments will be permitted, and which will be denied, specifically based on policy rules.

VPN

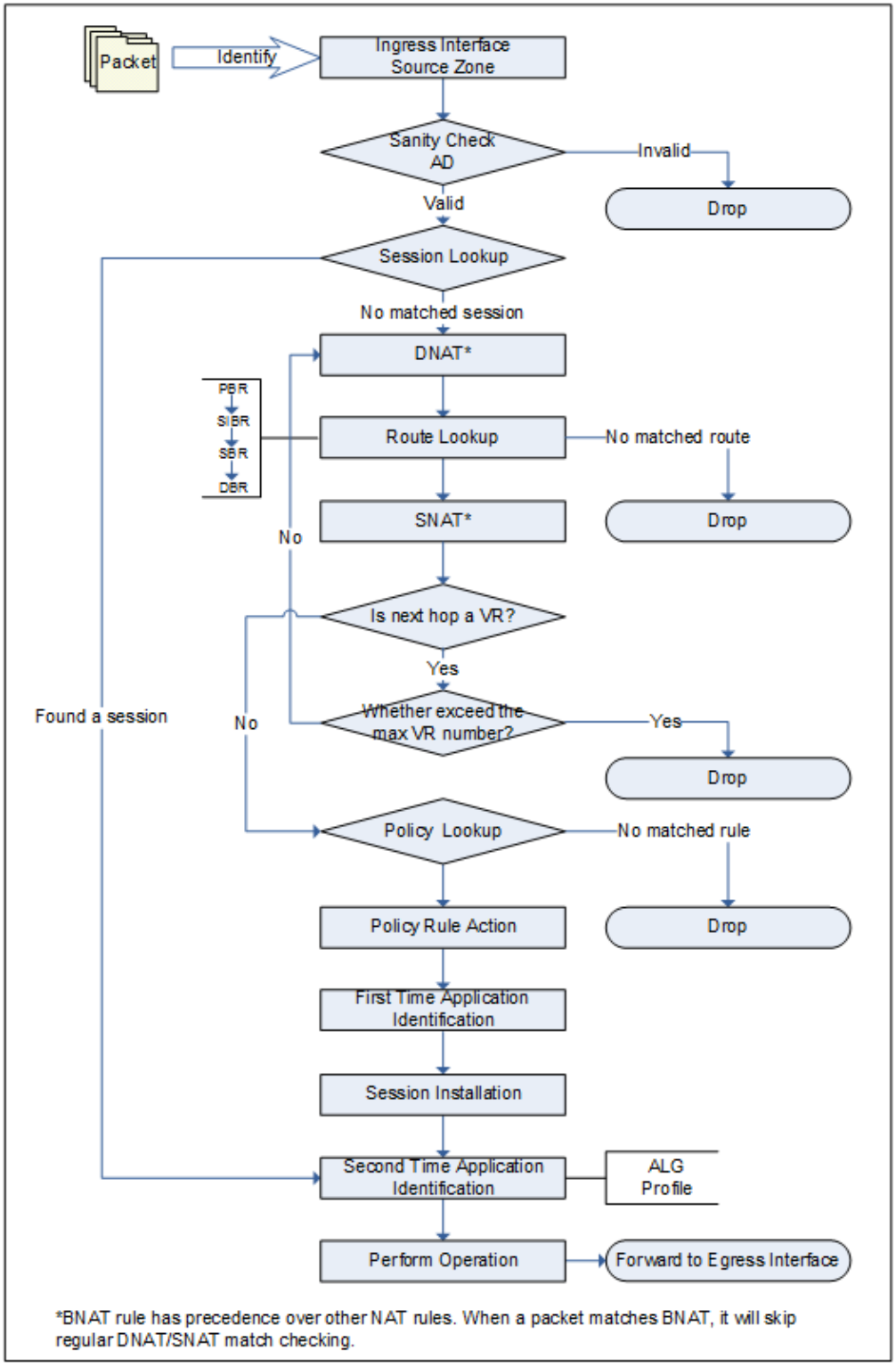
StoneOS supports IPsec VPN, SSL-based remote access solution - Secure Connect VPN (SSL VPN), dial-up VPN, PnPVPN, and L2TP VPN. You can configure VPN tunnels and choose the

VPN application mode:

- Policy-based VPN: Bind VPN tunnels to policy rules to transfer the specified traffic through tunnels.
- Route-based VPN: Bind VPN tunnels to tunnel interfaces, and then make the tunnel interface the next hop of the static routes. The specified traffic will be transmitted through VPN tunnels.

Packet Handling Process

For the information about Layer 2 packet handling process, see Forwarding Rules in VSwitch. Layer 3 packet handling process is shown below. In addition, the system supports the deny session function which will impact the handling process in both Layer 2 and Layer 3. For more information about deny session, see Deny Session.


Packet
Identify
Ingress Interface
Source Zone
Sanity Check
AD
Invalid
Drop
Valid
Session Lookup
No matched session
DNAT*
PBR
SIBR
SBR
DBR
Route Lookup
No matched route
SNAT*
Drop
No
Is next hop a VR?
Yes
Found a session
No
Whether exceed the
max VR number?
Yes
Drop
Policy Lookup
No matched rule
Policy Rule Action
Drop
First Time Application
Identification
Session Installation
Second Time Application
Identification
ALG
Profile
Perform Operation
Forward to Egress Interface
*BNAT rule has precedence over other NAT rules. When a packet matches BNAT, it will skip
regular DNAT/SNAT match checking.

1. Identify the logical ingress interface of the packet to determine the source zone of the packet. The logical ingress interface may be a common interface or a sub-interface.

2. The system performs sanity check to the packet. If the attack defense function is enabled on the source zone, the system will perform AD check simultaneously.

3. Session lookup. If the packet belongs to an existing session, the system will perform Step 11 directly.

4. DNAT operation. If a DNAT rule is matched, the system will mark the packet. The DNAT translated address is needed in the step of route lookup.
   *If BNAT rule exists, the packet will be checked if it matches any BNAT rule. When the packet matches a BNAT rule, it will follow BNAT configuration, and will not check for regular DNAT rules.

5. Route lookup. The route lookup order from high to low is: PBR > SIBR > SBR > DBR > ISP route.
   Till now, the system knows the logical egress and destination zone of the packet.

6. SNAT operation. If a SNAT rule is matched, the system will mark the packet.
   *If BNAT rule exists, the packet will be checked if it matches any BNAT rule. When packet matches a BNAT rule, it will follow BNAT configuration, and will not check for regular SNAT rules.

7. VR next hop check. If the next hop is a VR, the system will check whether it is beyond the maximum VR number (current version allows the packet traverse up to three VRs). If it is beyond the maximum number, the system will drop the packet; and if it is within the maximum number, return to Step 4. If the next hop is not a VR, go on with policy lookup.

8. Policy lookup. The system looks up the policy rules according to the packet's source/destination zones, source/destination IP and port, and protocol. If no policy rule is matched, the system will drop the packet; if any policy rule is matched, the system will deal with the

packet as the rule specified. And the actions can be one of the followings:

- Permit: Forwards the packet.
- Deny: Drops the packet.
- Tunnel: Forwards the packet to the specified tunnel.
- Fromtunnel: Checks whether the packet originates from the specified tunnel. The system will forward the packet from the specified tunnel and drop other packets.
- WebAuth: Performs WebAuth on the specified user.

9. First time application identification. The system tries to identify the type of the application according to the port number and service specified in the policy rule.
10. Establish the session.
11. If necessary, the system will perform the second time application identification. It is a precise identification based on the packet contents and traffic action.
12. Application behavior control. After knowing the type of the application, the system will deal with the packet according to the configured profiles and ALG.
13. Perform operations according to the records in the session, for example, the NAT mark.
14. Forward the packet to the egress interface.

Deny Session

The deny session function dramatically improves the system performance when the device suffers attacks. Usually, before creating a new session, the system will do some related actions to the packet, such as AD check , SNAT/DNAT mark, policy rule lookup, application identification, and so on (refer to the packet handling process in the previous section). Doing the related actions consumes lots of CPU resource which leads to a performance degrading and gives the attackers chances. To address this problem, StoneOS provides the deny session function.

Here describes the working principle of deny session. After configuring the deny session function, the system will create deny sessions for the packets that cannot create sessions for some reasons. When a packet enters the device, the system will check its 5-tuple, and if the packet matches an existing deny session, the system will drop it. Thus the system performance is improved.

The system will create deny sessions in the following situations:

- Failed in AD check (Layer 2 and Layer 3 IP address spoofing attack defense);
- Failed in policy rule matching;
- Failed in forward or reverse route matching;
- The to-self packet is denied;
- The session limitation is exceeded.

In the following situations, the deny sessions will be deleted:

- The deny sessions age out automatically. The existing deny sessions will age out when the time is up and the system will deleted the aged deny sessions. You can specify the age out time.
- If the reverse traffic is allowed to create a session, the corresponding deny session will be deleted.

Configuring the Deny Session Function

Deny session configurations can be performed in the flow configuration mode. To enter the flow configuration mode, in the global configuration mode, use the command**flow**.

Specifying the Deny Session Type

You can specify the situations to create deny sessions. In the flow configuration mode, use the following command:

deny-session deny-type {**all** | **ad** | **policy** | **route** | **self** | **session-limit**}

- **all** – Creates deny sessions in all the 5 situations the system supports.
- **ad** – Creates deny sessions when the packet fails in AD check (Layer 2 and Layer 3 IP address spoofing attack defense).
- **policy** – Creates deny session when the packet cannot find a matched policy rule or matched a deny rule.
- **route** – Creates deny sessions when the packet cannot find a forward or reverse route.
- **self** – Creates deny sessions when the to-self packet is denied.
- **session-limit** – Creates deny sessions when the packet is out of the configured session limitation.

To remove the deny session type configuration, in the flow configuration mode, use the following command:

no deny-session deny-type {**all** | **ad** | **policy** | **route** | **self** | **session-limit**}

Specifying the Maximum Number of Deny Sessions

It refers to the maximum number of deny sessions the system supports. To specify the maximum number of deny session, in the flow configuration mode, use the following command:

deny-session percentage *number*

- *number* – Specifies the percentage of deny sessions in the total sessions. The value range is 0 to 10. The value of 0 means to disable the deny session function. The default value is 2, which means up to 2% deny sessions among the total sessions can be created.

To restore the default deny session number, in the flow configuration mode, use the following command:

no deny-session percentage

Specifying the Timeout Value

The timeout value refers to the time duration after which the deny session will age out and be deleted from the system. To specify the timeout value, in the flow configuration mode, use the following command:

deny-session timeout *time*

- *time* – Specifies the timeout value. The value range is 1 to 3 seconds. The default value is 3.

To restore to the default timeout value, in the flow configuration mode, use the following command:

no deny-session timeout

Viewing the Deny Session Configuration Information

The deny session configuration information include type, maximum number, and timeout value. To view the information, in any mode, use the following command:

show flow deny-session

Viewing the Deny Session Information

To view the existing deny session information, in any mode, use the following command:

show session deny

TCP RST Packet Check

StoneOS supports TCP RST packet check. After enabling this function, if TCP RST packet is the first packet, the system will not create any session. To enable TCP RST packet check, in the flow configuration mode, use the following command:

tcp-rst-bit-check

To disable TCP RST packet check, in the flow configuration mode, use the following command: **no tcp-rst-bit-check** .

Global Network Parameters

To provide a better traffic transmission service, the device supports a set of global network parameters, including TCP MSS (Maximum Segment Size), TCP sequence number check, TCP three-way handshaking timeout check, TCP SYN packet check, IP fragment, Jumbo Frame, , and TCP packet timestamp, TSO/LRO function ,and validity check for Layer 4 protocol options.

Configuring MSS

MSS is a parameter of the TCP protocol that specifies the largest amount of data that the device can receive in a single TCP segment. You can specify the MSS value for all the TCP SYN/ACK packets or the IPsec VPN TCP SYN/ACK. A proper MSS value can reduce the number of IP fragment. To specify the MSS value, in the global configuration mode, use the following command:

tcp-mss {**all** | **tunnel**} *size*

- **all** – Specifies the MSS value for all the TCP SYN packets.
- **tunnel** – Specifies the MSS value for TCP packets of the IPsec VPN /SSL VPN/GRE/L2TP tunnel etc.
- *size* – Specifies the MSS value. The value range is 64 to 65535. The default value of TCP SYN/ACK packets is 1448. The default value of IPsec VPN TCP SYN/ACK packets is 1380.

To restore to the default MSS value, in the global configuration mode, use the following command:

no tcp-mss {**all** | **tunnel**}

TCP Sequence Number Check

The TCP sequence number check function checks the TCP sequence number of the packet, and if the sequence number exceeds the TCP window, the system will drop the packet. This function

is enabled by default. To configure the TCP sequence number check function, in the global configuration mode, use the following commands:

- Disable: **tcp-seq-check-disable**
- Enable: **no tcp-seq-check-disable**

TCP Three-way Handshaking Timeout Check

The device can check the TCP three-way handshaking time, and if the three-way handshaking has not been completed after timeout, the connection will be reset. You can configure the global TCP three-way handshaking timeout check function or configure the TCP three-way handshaking timeout check function based on policy rules. The priority of timeout settings is as follows: timeout configured based on policy rules > global timeout.



Notes: If timeout settings are configured in both the root VSYS and non-root VSYS, the priority is as follows: timeout configured based on policy rules in the non-root VSYS > global timeout settings in the non-root VSYS > global timeout settings in the root VSYS.

Configuring the Global TCP Three-Way Handshaking Timeout Check Function

To enable the global TCP three-way handshaking timeout check function and specify the timeout, in global configuration mode, use the following command:

tcp-syn-check [*timeout-value*]

- *timeout-value* – Specifies the global timeout of three-way handshaking. Valid values: 1 to 1800. Unit: seconds. Default value: 20.

By default, this function is enabled. To disable this function, in global configuration mode, use the command **no tcp-syn-check**.



Notes: By default, this function is disabled in the non-root VSYS.

Configuring the TCP Three-Way Handshaking Timeout Check Function Based on Policy Rules

By default, this function is disabled. You can enable the TCP three-way handshaking timeout check function based on policy rules as required. If traffic that hits the policy has not completed the three-way handshaking after timeout, the connection will be reset. Other policy rules that are not enabled with this function will be checked based on global timeout settings.

To enable the TCP three-way handshaking timeout check function based on a single policy and specify the timeout, in policy rule configuration mode, use the following command:

tcp-syn-check [*timeout-value*]

- *timeout-value* – Specifies the timeout of three-way handshaking. Valid values: 1 to 1800. Unit: seconds. Default value: 20.

To disable the TCP three-way handshaking timeout check function based on the specified policy rule, in policy rule configuration mode, use the command **no tcp-syn-check**.

TCP Connection State Age-time

The system uses age-time to calculate the living time of the TCP connection. And if do not receive any data within the age-time, system will delete the TCP connection. You can specify age-time for each state of TCP connection. The age time you can specified for the following TCP connection state:

- ESTABLISHED
- FIN-WAIT-1
- FIN-WAIT-2
- TIME-OUT

To specify age-time in ESTABLISHED state, in the global configuration mode, use the following command:

tcp-establish-check [*timeout-value*]

- *timeout-value* – Specifies age-time for the ESTABLISHED state. After a three-way handshake, the TCP connection moves to the ESTABLISHED state without any TCP data transmitting and use the defined age-time of this state. The value range is from 1 to 1800 seconds. If this parameter is not specified, system will use the default value 300 seconds.

To specify age-time in FIN-WAIT-1 state, in the global configuration mode, use the following command:

tcp-fin-wait-1-check [*timeout-value*]

- *timeout-value* – Specifies age-time for the FIN-WAIT-1 state. The value range is from 1 to 1800 seconds. If this parameter is not specified, system will use the default value 120 seconds.

To specify age-time in FIN-WAIT-2 state, in the global configuration mode, use the following command:

tcp-fin-wait-2-check [*timeout-value*]

- *timeout-value* – Specifies age-time for the FIN-WAIT-2 state. The value range is from 1 to 1800 seconds. If this parameter is not specified, system will use the default value 120 seconds.

To specify age-time in TIME-OUT state, in the global configuration mode, use the following command:

tcp-time-wait-check [*timeout-value*]

- *timeout-value* – Specifies age-time for the TIME-OUT state. The value is form 1 to 1800 seconds. If this parameter is not specified, system will use the default value 5 seconds.

TCP SYN Packet Check

System supports the TCP SYN packet check function, when establishing a TCP connection, the device will check the received packets:

- When the received packet is a TCP SYN packet, the TCP connection will be established.
- When the received packet is a TCP non-SYN packet, the packet will be processed according to the specified action.

This function is disabled by default. To configure this function and specify the action for TCP non-SYN packet, in the global configuration mode, use the following commands:

tcp-syn-bit-check {**drop** | **reset**}

- **drop** – When the received packet is a TCP non-SYN packet, the system will drop the packet.
- **reset** – When the received packet is a TCP non-SYN packet, the system will drop the packet and send RST packet to the peer device.

To disable TCP SYN check function, in the global configuration mode, use the following commands:

no tcp-syn-bit-check

IP Fragment

For the fragmented packets, you can specify the maximum fragment number (any IP packet that contains more fragments than this number will be dropped) and the fragment reassembling timeout value (if the device has not received all the fragments after timeout, the packet will be dropped).

To specify the maximum fragment number, in the global configuration mode, use the following command:

fragment chain *number*

- *number* – Specifies the maximum fragment number allowed by the system. The value range is 1 to 1024. The default value is 48.

To restore to the default maximum fragment number, in the global configuration mode, use the command **no fragment chain**.

To specify the reassembling timeout value, in the global configuration mode, use the following command:

fragment timeout *time*

- *time* – Specifies the timeout value. The value range is 1 to 60 seconds. The default value is 2.

To restore to the default timeout value, in the global configuration mode, use the command **no fragment timeout**.

SYN packets dropping

Enabling/Disabling SYN Packets Dropping

System supports to drop SYN packets of the same five-tuple array during the delay-deleting time of TCP sessions, which means during the delay-deleting time of TCP sessions, system drops SYN packets of the same five-tuple array. If this function is disabled, TCP sessions match and forward SYN packets during the delay-deleting time, which can lead to the loss of new packets because the they cannot match correct sessions which are already deleted.

This function is disabled by default.

In the Flow mode, use the following command to enable or disable SYN packets dropping:

- Enable: **tcp-out-of-state-syn-drop**
- Disable: **no tcp-out-of-state-syn-drop**

Show the state of the function of SYN packets dropping

In the execution mode, use the following command to show the state of the function of SYN packets dropping:

show flow tcp-out-of-state-syn-drop

Jumbo Frame

In the process of packet forwarding, if the device gets a frame that the size exceeds the MTU value of the outbound interface, the data is either fragmented into smaller frames, or dropped. With the function of Jumbo Frame enabled, the system can forward packets less than or equal to 9216 bytes as follows:

- For IPv4/IPv6 packets that are less than the MTU value of the outbound interface, forward them directly.
- For IPv4 packets that are larger than the MTU value of the outbound interface, the packets are forwarded in fragments.
- For IPv6 packets that are larger than the MTU value of the outbound interface, an "ICMPv6 Packet Too Big" error message will be sent to the source node of the packets, and the sender is urged to shorten the length of the packets.

The Jumbo Frame function is disabled by default. To enable or disable the function, in the flow configuration mode, use the following command:

jumbo-frame-transceiver {**enable** | **disable**}

- **enable** - Enable the Jumbo Frame function.
- **disable** - Disable the Jumbo Frame function.



Notes:

- When the Jumbo Frame function is enabled, the MTU configuration range of the interface will be changed. For more information about the MTU value configuration of the interface, see Configuring an Interface MTU Value and Specifying an IPv6 MTU.



- SG-6000-A7600/A6800, SG-6000-K9180/K7680/K6580/K6280-GS/K2680/K2380, SG-6000-X20812/X20803/X8180 do not support the Jumbo Frame function.

To view the status of the Jumbo Frame function, in the interface configuration mode, use the following command:

show flow jumbo_frame_transceiver

Configuring TCP Packet Timestamp

TCP timestamp is an option in the packet header, mainly used to measure Round-Trip Time (RTT) to avoid sequence wraparound. You can enable or disable TCP packet timestamp with commands. By default, TCP timestamp is enabled.

To enable or disable TCP packet timestamp, you need to enter System-control configuration mode first. To enter System-control configuration mode, in the global mode, use the following command:

system-control

To enable or disable TCP packet timestamp, in the System-control configuration mode, use the following command:

ipv4-tcp-timestamps {**on** | **off**}

- **on** – Enable TCP packet timestamp.
- **off** – Disable TCP packet timestamp.

To view the status of TCP packet timestamp, in any mode, use the following command:

show system-control ipv4-tcp-timestamps

If "0" returns after the above command, it indicates that TCP packet timestamp is disabled. If "1" is retuned, it indicates that TCP packet timestamp is enabled.

Validity Check for Layer 4 Protocol

Enabling/Disabling Validity Check for Layer 4 Protocol

Layer 4 indicates the transport layer of the OSI model, which provides end-to-end communication between devices and ensures the integrity of data transmission. By default, this function is enabled. In this case, the system checks TCP packets at Layer 4, such as checking whether the flag of TCP is valid and whether the port number is valid. If the TCP packet is abnormal, it will be dropped.

To enable/disable validity check for Layer 4 protocol, in flow configuration mode, use the following command:

- Enable: **l4-validity-check**
- Disable: **no l4-validity-check**

Checking Whether Validity Check for Layer 4 Protocol is Enabled

To check whether validity check for Layer 4 protocol is enabled, in any mode, use the following command:

show flow l4-validity-check

Example:

```
hostname# show flow l4-validity-check
Layer 4 validity check: enabled (Indicates that validity check for Layer 4 check is enabled)
```

Session Information

You can perform the following actions on the session information:

- Show session information
- Clear session information
- Delaying Deleting Session

Showing Session Information

In any mode, use the following commands to show the session information in the system:

show session [**generic** | **h323**]

- **generic** – Shows the overview of the session information.
- **h323** – Shows the H323 session information.

show session [**id** *number* [*end-id*]] [**src-ip** *A.B.C.D* [*netmask*|*wildcard*]] [**dst-ip** *A.B.C.D* [*net-mask* | *wildcard*]] [**protocol** *protocol-number*][**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]] [**src-mac** *src-mac-address*] [**dst-mac** *dst-mac-address*] [**src-zone** *zone-name*] [**dst-zone** *zone-name*] [**application** *name*] [**policy** *policy-id*] [**vrouter** *vrouter-name*] [**vsys** *vsys-name*] [**slot** *slot-number*] [**cpu** *cpu-number*] [**ipv4**] [**ipv6**] [**snat-rule** *id*] [**dnat-rule** *id*] [**bnat-rule** *id*] [**detail**] [**tcp-state-3handshake**] [**tcp-state-established**] [**tcp-state-closing**] [{**flow0-interface** | **flow1-interface**} *interface-name*]

- **id** *number* [*end-id*] – Shows the session information of the specified ID. To show the session information of a specified range of IDs, continue entering the end ID of the range.
- **src-ip** *A.B.C.D* – Shows the session information of the specified source IP address or specified range of IP addresses.
- **dst-ip** *A.B.C.D* – Shows the session information of the specified destination IP address or specified range of IP addresses.
- *netmask* | *wildcard* – Specifies the netmask or the wildcard mask.
- *protocol-number* – Shows the session information of the specified protocol number.

- **src-port** *port-number* [*port-number*] – Shows the session information of the specified source port or specified range of port.
- **dst-port** *port-number* [*port-number*] – Shows the session information of the specified destination port or specified range of port.
- **src-mac** *src-mac-address* – Shows the session information of the specified source MAC address.
- **dst-mac** *dst-mac-address* – Shows the session information of the specified destination MAC address.
- **src-zone** *zone-name* – Shows the session information of the specified source security zone.
- **dst-zone** *zone-name* – Shows the session information of the specified destination security zone.
- **application** *name* – Shows the session information of the specified application.
- **policy** *policy-id* – Shows the session information of the specified policy.
- **vrouter** *vrouter-name* – Shows the session information of the specified virtual router.
- **vsys** *vsys-name* – Shows the session information of the specified VSYS.
- **lot***slot-number* – Shows the session information of the specified slot.
- **cpu***cpu-number* – Shows the session information of the specified CPU.
- **ipv4** – Shows the session information of the IPv4 protocol.
- **ipv6** – Shows the session information of the IPv6 protocol.
- **snat-rule** *id* – Shows the session information of the specified SNAT rule.
- **dnat-rule** *id* – Shows the session information of the specified DNAT rule.
- **bnat-rule** *id* – Shows the session information of the specified BNAT rule.

- **detail** – Shows the detail session information.
- **tcp-state-3handshake** – Shows the session information of the TCP three-way handshaking state.
- **tcp-state-established** – Shows the session information of the TCP connection in the ESTABLISHED state.
- **tcp-state-closing** – Shows the session information of the TCP connection in the terminated state.
- {**flow0-interface** | **flow1-interface**} *interface-name* - Shows the session information of the ingress interface of the specified flow0 or flow 1.

Clearing Session Information

In any mode, use the following command to clear the session information in the system:

clear session [**h323**] [**id** *number* [*end-id*]] [**src-ip A.B.C.D** [*netmask* | *wildcard*]] [**dst-ip** *A.B.C.D* [*netmask* | *wildcard*]] [**protocol** *protocol-number*][**src-port** *port-number* [*port-number*]] [**dst-port** *port-number* [*port-number*]] [**vrouter** *vrouter-name*] [**vsys** *vsys-name*] [**slot** *slot-number*] [**cpu** *cpu-number*][**ipv4**] [**ipv6**] [**detail**]

- **h323** – Clears the H323 session information.
- **id** *number* [*end-id*] – Clears the session information of the specified ID. To show the session information of a specified range of IDs, continue entering the end ID of the range.
- **src-ip** *A.B.C.D* – Clears the session information of the specified source IP address or specified range of IP addresses.
- **dst-ip** *A.B.C.D* – Clears the session information of the specified destination IP address or specified range of IP addresses.
- *netmask* | *wildcard* – Clears the netmask or the wildcard mask.

- *protocol-number* – Clears the session information of the specified protocol number.
- **src-port** *port-number* [*port-number*] – Clears the session information of the specified source port or specified range of port.
- **dst-port** *port-number* [*port-number*] – Clears the session information of the specified destination port or specified range of port.
- **vrouter** *vrouter-name* – Clears the session information of the specified virtual router.
- **vsys** *vsys-name* – Clears the session information of the specified VSYS.
- **slot** *slot-number* – Clears the session information of the specified slot.
- **cpu** *cpu-number* – Clears the session information of the specified CPU.
- **ipv4** – Clears the session information of the IPv4 protocol.
- **ipv6** – Clears the session information of the IPv6 protocol.
- **detail** – Clears the detail session information.

Delay Deleting Session

To avoid abnormal increase of sessions in user's server, the system provides the function of delaying deleting sessions, i.e. when the device receives FIN/RST packets, the device will delete the sessions when the specified time before sessions are deleted is over, rather than immediately delete related sessions.

Enable delaying deleting session

By default, this function is disabled and the time before sessions are deleted is 0 seconds.

In the flow mode, use the following command to enable delaying deleting session and specify the time before sessions are deleted:

tcp-session-close-wait [*timeout-value*]

- *timeout-value* – Specify the time before sessions are deleted. The default value is 0 seconds. The value range is 0 to 30 seconds.

In the flow mode, use the negative form of the above command to disable delaying deleting sessions as below. When this function is disabled, the device will immediately delete sessions after receiving FIN/RST packets.

no tcp-session-close-wait

Show the state of the function of delaying deleting session

In the execution mode, use the following command to show the state of the function of delaying deleting session (if the state is "enabled", the time before sessions are deleted will also be shown):

show flow tcp-session-close-wait

RTO Query Optimization

The RTO query optimization includes the following functions:

- Enabling/Disabling RTO query optimization
- Displaying the state of RTO query optimization

Enabling/Disabling RTO Query Optimization

In default, the process of some devices (SG-6000-X9180/SG-6000-X10800/SG-6000-K9180) selecting modules to create new sessions is as follows:

1. Based on the configuration of the session distribution mode (use the **session-schedule-mode** command to configure in the flow configuration mode), the IOM modules will select an SSM module to create new sessions;
2. During the process of creating sessions, the system will again create new sessions on the corresponding SSM modules according to ALG or Full-cone NAT business.

When selecting again SSM modules to create new sessions, the system will conduct query on RTO. RTO (Real-time Object) refers to the information dynamically created by data packets in

the processing procedure, such as the Pinhole information, the Full-cone NAT table items and the application identification cache tables.

To improve the system performance, the user can enable the RTO query optimization. When the user disables Full-cone NAT or the Full-cone NAT business is not included in the user scenario, the system will not conduct RTO query on the HTTP new session traffic (TCP 80/8080), and will not select SSM modules again.

In default, RTO query optimization is disabled. To enable or disable this function, in the Flow configuration mode, use the following command:

- Enable: **rto-query-optimization enable**
- Disable: **no rto-query-optimization enable**

Displaying the State of RTO Query Optimization

To display the state of RTO query optimization, in any mode, use the following command:

show flow rto-query-optimization

Low Latency Mode

System support to shorten the delay by adjusting the internal send and receive packet parameters. To enable the low latency mode, in the flow configuration mode, use the following command:

low-latency-mode

To disable the low latency mode, in the flow configuration mode, use the following command:

no low-latency-mode



Notes: After enabling the low-latency mode, the throughput of device may be reduced.

To show if the low latency mode is enabled, in any mode, use the following commands:

show flow low-latency-mode

Packet Length Sanity Check

Enabling/Disabling Packet Length Sanity Check

After enabling the packet length sanity check, the system supports strict checking of the received Ethernet frame packet length. When an Ethernet frame packet with abnormal length is detected, the system will discard the packet to enhance device security. By default, the packet length sanity check is disabled. To enable or disable this function, in the Flow configuration mode, use the following command:

- Enable: **packet-length-sanity-check**
- Disable: **no packet-length-sanity-check**

Displaying the State of Packet Length Sanity Check

To display the state of packet length sanity check, in any mode, use the following command:

show flow packet-length-sanity-check

Configuring TSO/LRO Function

TCP Segmentation Offload (TSO) fragments TCP packets through the network card before forwarding them, reducing CPU load. Large Receive Offload (LRO), on the other hand, aggregates multiple TCP packets received by the network card into a larger packet, which is then passed to the network protocol stack for processing, improving the system's ability to receive TCP packets. After enabling the TSO/LRO function, packets larger than the egress interface MTU value will be fragmented or aggregated in the network card. The TSO/LRO function is disabled by default. To enable/disable the TSO/LRO function, use the following command in Flow configuration mode:

tso-lro {**enable** | **disable**}

• **enable** – Enable TSO/LRO function.

• **disable** – Disable TSO/LRO function.

To view the status of TSO/LRO function, in the interface configuration mode, use the following command:

show flow tso-lro

Application Layer Fast Forward

The application layer fast forward includes the following functions:

- Enabling/Disabling application layer fast forward
- Displaying the state of application layer fast forward



Notes: Only SG-6000-A7600, A6800, X-series, and SG-6000-K9180 devices support this function.

Enabling/Disabling Application Layer Fast Forward

To enhance the performance of device, the system supports the Application Layer Fast Forward function. After this function is enabled, when only the Intrusion Prevention function at the application layer is enabled and the protocol max scan length configured in the intrusion prevention rule is reached, traffic at the application layer will no longer be forwarded to the SSM module or CPU for parsing and processing.

By default, this function is enabled. To enable/disable this function, in global configuration mode, use the following command:

- Enable: **app-fast-fwd enable**
- Disable: **app-fast-fwd disable**

Displaying the State of Application Layer Fast Forward

To display the state of application layer fast forward, in any mode, use the following command:

show app-fast-fwd

Response Traceroute Function

The Response Traceroute function includes the following configurations:

- Enabling/Disabling the Response Traceroute Function
- Displaying the Status of the Response Traceroute Function

Enabling/Disabling the Response Traceroute Function

By default, the system will respond to traceroute traffic passing through the device. When the traceroute traffic is not sent or received by the device itself, you can disable the Response Traceroute function to prevent the device from responding to traceroute traffic that does not belong to the device itself. This way, the IP address of the device is hidden, which reduces the possibility of the device being discovered and attacked.

By default, this function is enabled. To enable/disable this function, in flow configuration mode, use the following command:

- Enable: **response-traceroute**
- Disable: **no response-traceroute**



Notes: For traceroute traffic that belongs to the device itself, whether this function is enabled does not affect the response of the device to the traffic.

Displaying the Status of the Response Traceroute Function

To display the status of the Response Traceroute function, in any mode, use the following command:

show response-traceroute

Zone

Overview

In StoneOS, zone is a logical entity. One or more interfaces can be bound to one zone. A zone with policy applied is known as a security zone, while a zone created for a specific function is known as a functional zone. Zones have the following features:

- An interface should be bound to a zone. A Layer 2 zone is bound to a VSwitch, while a Layer 3 zone is bound to a VRouter. Therefore, the VSwitch of a Layer 2 zone is the VSwitch of the interfaces in that zone, and the VRouter of a Layer 3 zone is the VRouter of the interfaces in that zone.
- Layer 2 interfaces work in Layer 2 mode and Layer 3 interfaces work in Layer 3 mode.
- StoneOS supports internal zone policies, like trust-to-trust policy rule.

Predefined Security Zone

There are 9 predefined security zones in StoneOS, which are trust, untrust, dmz, L2-trust, L2-untrust, L2-dmz, mgt, vpnhub (VPN functional zone) and ha (HA functional zone). You can also customize security zones. Actually predefined security zones and user-defined security zones make no difference in functions, and you can use them as needed.

Configuring a Security Zone

You can perform the following operations to a security zone:

- Viewing the zone information
- Creating a zone
- Specifying the description
- Binding a Layer 2 zone to VSwitch

- Binding a Layer 3 zone to VRouter
- Specifying the service type

Viewing the Zone Information

To view the zone information, in any mode, use the following command:

show zone [*zone-name*]

- *zone-name* – Specifies the zone name to view its information.

Creating a Zone

Unless it is specified as a Layer 2 zone, a new zone will be a Layer3 zone by default. To create a zone, in the global configuration mode, use the following command:

zone *zone-name* [**l2** | **tap**]

- *zone-name* - Specifies a name for the zone.
- **l2** – Specifies the zone as a Layer 2 zone.
- **tap** -Specifies the zone as a Tap zone. A Tap zone is a functional zone in Bypass mode.

If the specified zone name exists, the system will directly enter the zone configuration mode.

To delete an existing zone, in the global configuration mode, use the command

no zone *zone-name* [**l2**].



Notes: The predefined zones cannot be deleted.

Specifying the Description

To specify the description for a specific zone, use the following command in the zone configuration mode:

description *description*

- *description* – Specifies the description of the zone.

To delete the description of the zone, use the command **no description**.

Binding a Layer 3 Zone to a VRouter

If a Layer 3 zone is bound to a VRouter, all the interfaces in that zone are bound to this VRouter. All the Layer 3 zones are bound to trust-vr by default. To assign a different VRouter to a layer-3 zone, in the zone configuration mode, use the following command:

vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of the VRouter to which the Layer 3 zone are bound.

To restore to the default zone-trust-vr binding setting, in the zone configuration mode, use command **no vrouter**.



Notes: Before changing the VRouter of a zone, make sure there is no binding interface in that zone.

Binding a Layer 2 Zone to a VSwitch

If a Layer 2 zone is bound to a VSwitch, all the interfaces in that zone are bound to this VSwitch. All the Layer 2 zones are bound to VSwitch1 by default. To assign a different VSwitch to a Layer 2 zone, in the zone configuration mode, use the following command:

bind *vswitch-name*

- *vswitch-name* - Specifies the name of VSwitch to which the Layer 2 zone is bound.

To restore to the default zone-VSwtich1 binding setting, in the zone configuration mode, use command **no bind**.



Notes: When changing the VSwitch to which a zone belong, make sure there is no binding interface in the zone.

Specifying the Service Type

To specify the service type of the zone, in zone configuration mode, use the following command:

type {**wan** | **ztna**}

- **wan** | **ztna** - Specifies the service type of the zone, which can be a WAN（**wan**） or ZTNA（**ztna**） zone. When the type is set to WAN, you can ensure the accuracy of the statistics of the statistics set with IP address as the data organization. For more information about ZTNA, refer to **ZTNA Policy** in *StoneOS WebUI User Guide*.

To restore to the default service type of the zone, in zone configuration mode, use the command **no type**.

Configuration Example

The goal is to create VSwitch2 and Layer 2 zone named zone1, then bind zone1 to VSwitch2, and bind ethernet0/2 to zone1. Use the following commands:

```
hostname(config)# vswitch vswitch2
hostname(config-vswitch)# exit
hostname(config)# zone zone1 l2
hostname(config-zone-zone1)# bind vswitch2
hostname(config-zone-zone1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone1
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Interface

Overview

In StoneOS, interface is a point where packets enter and leave the device. To allow data traffic go through a zone, you must bind the interface to that zone and if it is a Layer 3 zone, you should assign an IP address to the interface. Moreover, to allow traffic forwarding among interfaces of different zones, a policy should be applied. A zone can be bound with more than one interface, but an interface can only be bound to one zone.

Interface Types

Hillstone products provide a variety of interface types. According to the nature of interface, the interfaces consist of physical interface and logical interface.

- Physical interface: Every Ethernet port on the device is a physical interface. The name of physical interface is predefined, consisting of port type, slot number and port number, e.g. ethernet2/1 or ethernet0/2.
- Logical interface: Logical interface includes BGroup interface, sub-interface, VSwitch interface, loopback interface, tunnel interface, aggregate interface, Super-VLAN interface, redundant interface, and Vif interface.

According to the binding zone, the interfaces can also be categorized into Layer 2 interface and Layer 3 interface.

- Layer 2 interface: an interface which belongs to a Layer 2 zone, a BGroup.
- Layer 3 interface: an interface which belongs to a Layer 3 zone. Only Layer 3 interface is able to work in NAT/Route mode.

Different interface has different functions. Table below describes all logical interfaces.

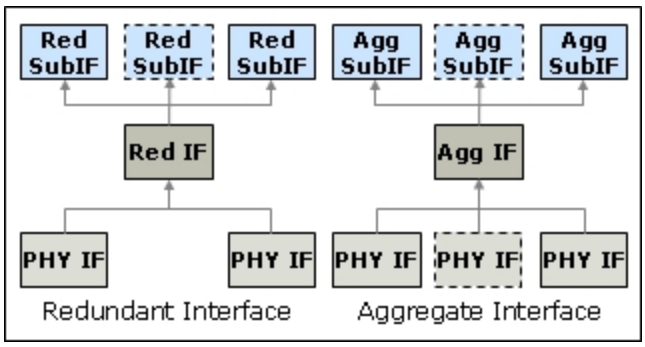
Type	Description
Sub-interface	The naming rule of sub-interface is to add an extension number to the

Type	Description
	name of its source interface, e.g. ethernet0/2.1. StoneOS supports the following types of sub-interface: Ethernet sub-interface, aggregate sub-interface, PPPoE sub-interface and redundant sub-interface. An Interface and its sub-interface can be bound to the same zone or to different zones.
VSwitch interface	VSwitch interface is Layer 3 interface. It is an assembled interface of all interfaces in VSwitch. The VSwitch interface is actually working as the upstream port of a switch, and it allows packets to be forwarded between Layer 2 and Layer 3.
Loopback interface	Loopback interface is a logical interface. As long as the device which the loopback interface belongs to is in the working status, the loopback interface is in the working status. Therefore, loopback interface is often stable.
Tunnel interface	Tunnel interface is the ingress port of VPN tunnel. Data flow accesses and leaves the VPN tunnel by going through the tunnel interface. Tunnel interface must be a Layer 3 interface.
Aggregate interface	An aggregate interface is an assembly of 1 to 16 physical interfaces. The physical interfaces equally share the data flow that passes the aggregate interface. Therefore, the aggregate interface can increase the available bandwidth for one IP address. If one of the physical interfaces malfunctions, other physical interfaces can carry on to process the data flow, only that the available bandwidth will become smaller.
Redundant interface	Redundant interface refers to the binding of two physical interfaces. A physical interface works as the master interface and processes the data flow, and the alternative interface stands by. The alternative interface will go on to process the data flow when the master interface fails to

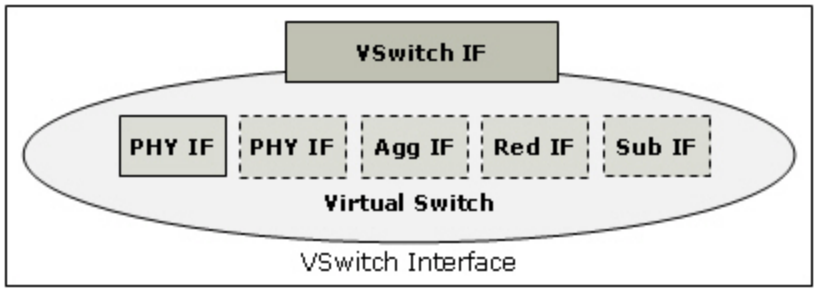
Type	Description
	function.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.
Virtual forward interface	In HA environment, the Virtual forward interface is HA group's interface designed for traffic transmission.
Vif interface	The Vif interface is a logical interface, which is used for the Multicast Service Reflection (MSR) function.

Interface Dependency

Some types of the interfaces are related to each other. The following figure illustrates the relationship of aggregate interface and its sub-interfaces and the relationship of redundant interface and its sub-interfaces. The following figure illustrates the relationship of VSwitch interface and other Layer 2 interfaces. The dotted line in the figures indicates that there can be more interfaces.



As shown in the above figure, a redundant interface (Red IF) is a binding interface of two physical interfaces (PHY IF) and it allows redundant sub-interfaces (Red SubIF) to be created. An aggregate interface (Agg IF) is a binding interface of up to 16 physical interfaces and it also allows aggregate sub-interfaces (Agg SubIF).



As shown in the above figure, a VSwitch interface represents all physical and logical interfaces in that VSwitch. Packets can be transferred in Layer 2 and Layer 3 by going through the VSwitch interface (VSwitch IF).

Viewing Interface Information

You can view the interface information in the interface list which shows all physical interfaces and other types of interfaces as long as they have been created and defined, including sub-interfaces, redundant interfaces, aggregate interfaces, BGroup interfaces and tunnel interfaces.

Viewing All Interfaces

To view all interfaces using the CLI, use the command **show interface**. The interface list will display the information by categories.

Item	Description
Interface name	Shows the name of interface.
IP address/mask	Shows the IP address of interface.
Zone name	Shows the bound zone of interface.
Vsys	Shows the VSYS name of interface.
H (Physical state)	Shows the physical availability state of interface： U: up, D: down, K: ha keep up, C: lacp down.
A (Admin state)	Shows the administration availability state of the interface: U: up, D: down, C: lacp down.
L (Link state)	Shows the link availability state of the interface: U: up, D:

Item	Description
	down, K: ha keep up, C: lacp down.
P (Protocol state)	Shows the protocol availability state of the interface: U: up, D: down, K: ha keep up, C: lacp down.
MAC address	Shows the interface MAC address.
Description	Shows the interface description.

The following description explains the meaning of H, A, L and P states, and the value of states are U: up, D: down, K: ha keep up, C: lacp down:

- H (Physical state): the physical connectivity state of the interface. The UP state indicates that the interface is physically connected, while the DOWN state means otherwise, in HA mode, the ha keep up state indicates that the HA interface is keep connected.
- A (Admin state): the manageability state of the interface. To enable an interface, use the command no shutdown command; to disable an interface, use the command shutdown. If an interface’ s A status is UP, it a manageable interface, and DOWN state means otherwise.
- L (Link state): the linking state of the interface. The link state depends on the states of H and A. If both H and A states are UP, the L state is UP, in HA mode, the ha keep up state indicates that the HA interface is keep connected.
- P (Protocol state): the protocol state of the interface. When the L state is UP and the interface has been allocated with an IP address, the P is UP, in HA mode, the ha keep up state indicates that the HA interface is keep connected.

Here is an example of the show interface command:

```
SG-6000(config)# show interface

H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down;K:ha keep up;C:lacp down
N:Not shared;S:Shared;E:Exported to vsys;V:Vsys interface
=============================================================================================================================================
Interface name       IPv4 address/mask    IPv6 address/prefix                       Zone name     Vsys     H A L P MAC address    F Description
---------------------------------------------------------------------------------------------------------------------------------------------
vswitchif1           0.0.0.0/0            N/A                                       trust         root     D U D D 001c.5457.67c2 S ------
ethernet0/0          0.0.0.0/0            N/A                                       trust         root     U U U D 001c.5457.6799 S ------
ethernet0/1          88.1.2.1/24          123::1/64                                 trust         root     U U U U 001c.5457.679a S ------
ethernet0/2          0.0.0.0/0            N/A                                       NULL          root     D U D D 001c.5457.679b N ------
ethernet0/2-pppoe1   0.0.0.0/0            N/A                                       trust         root     D U D D 001c.5457.67ce S ------
ethernet0/2.3        15.6.6.6/24          N/A                                       trust         root     D U D D 001c.5481.e0e8 S ------
ethernet0/3          0.0.0.0/0            N/A                                       NULL          root     D U D D 001c.5457.679c N ------
ethernet0/4          0.0.0.0/0            FE80::21C:54FF:FE57:679D/64               trust         root     D U D D 001c.5457.679d S ------
                                          FE80:1::21C:54FF:FE57:679D/64
ethernet0/5          0.0.0.0/0            N/A                                       NULL          root     D U D D 001c.5457.679e N ------
ethernet0/6          0.0.0.0/0            N/A                                       trust         root     D U D D 001c.5457.679f S ------
ethernet0/7          0.0.0.0/0            N/A                                       NULL          root     D U D D 001c.5457.67a0 N ------
ethernet0/8          0.0.0.0/0            N/A                                       NULL          1        D U D D 001c.5457.67a1 E ------
ethernet0/8.1        0.0.0.0/0            N/A                                       1-trust       1        D U D D 001c.5457.67a1 V ------
ethernet0/9          0.0.0.0/0            N/A                                       trust         root     D U D D 001c.5457.67a2 S ------
```

Viewing a Specific Interface

To view the information about a specific interface, type the interface name after the command **show interface**, i.e. **show interface** *interface-name*. Figure below gives an example of the command **`show interface ethernet0/0`**.

```
hillstone# show interface ethernet0/0
------------------------------------------------------------------
Interface ethernet0/0
description:
                Physical down                   Admin up
                Link down                       Protocol down
                Interface ID:4
                IP address:192.168.1.1
                IP address mask:255.255.255.0
                MAC address:001c.5400.02ec
                Ip mtu:1500
                ARP learn:enable
                ARP timeout:1200
                Speed mode:10
                Duplex mode:half
                downstream bandwidth is 1000000000
                upstream   bandwidth is 1000000000
                Bind to zone trust
                Belong to vsys root
                manage service:SSH;TELNET;PING;SNMP;HTTP;HTTPS;
                Secondary ip address0: 0.0.0.0 mask:0.0.0.0
                Secondary ip address1: 0.0.0.0 mask:0.0.0.0
==================================================================
```

Configuring an Interface

To configure an interface, you need to enter into one of the seven interface modes below as needed:

- Route mode: Interface in router mode is a Layer 3 interface bound to a Layer 3 zone.
- VSwitch mode: Interface in VSwitch mode is a Layer 2 interface bound to a Layer 2 zone.
- VLAN mode: Interface in VLAN mode is a Layer 2 interface bound to a Layer 2 zone.
- Super-VLAN mode: Interface in super-VLAN mode is a Layer 2 interface bound to a Layer 2 zone.
- Aggregate mode: Interface in aggregate mode belongs to an aggregate interface and cannot be bound to any zone.
- Redundant mode: Interface in redundant mode belongs to a redundant interface and cannot be bound to any zone.
- BGroup mode: Interface in BGroup mode belongs to a BGroup interface and cannot be bound to any zone.
- Tunnel mode: Interface in tunnel mode is a Layer 3 interface bound to a Layer 3 zone.

This section introduces the basic interface configuration and operation, including:

- Binding an interface to a zone
- Configuring an interface IP address
- Configuring an interface MTU value
- Configuring interface force shutdown
- Specifying the Track Object
- Configuring interface ARP timeout
- Configuring an interface protocol
- Configuring interface proxy ARP
- Configuring interface mirroring

- Configuring traffic mirroring
- Configuring an interface reverse route
- Configuring interface backup
- Configuring a loopback interface
- Configuring an Ethernet interface
- Configuring a VSwitch interface
- Configuring a VLAN interface
- Configuring a super-VLAN interface
- Configuring an aggregate interface
- Configuring a redundant interface
- Configuring a tunnel interface
- Configuring a PPPoE sub-interface
- Bypassing the device
- Configuring the keepalive function of interface
- Disabling Recording Interface IP Address Conflict Log Triggered by DAD Mode ARP Packets
- Configuring Local ARP Proxy for Interfaces
- Configuring 10 G Interface Auto Tuning

Binding an Interface to a Zone

A physical interface can be bound to an existing Layer 2 or Layer 3 zone. To bind the interface to a zone, in the interface configuration mode, use the following command:

zone *zone-name*

To unbind the interface from a zone, use the command **no zone**. Before unbinding a Layer 3 interface, you need to clear the IP address of the interface first.



Notes: When binding an interface to a zone, note that:

- To make the interface work in Layer 2, you need to bind the interface to a Layer 2 zone.
- To change a Layer 2 interface to a Layer 3 interface, you need to clear the IP address of that interface first.

Specifying the Description

To specify the description of the interface, use the following command in the interface configuration mode:

description *description*

- *description* – Specifies the description of the interface.

To delete the description, use the command in the interface configuration mode **no description**.

Configuring an Interface IP Address

The IP addresses of interfaces on a device must belong to different subnets. You can assign a static IP address to the interface, or use DHCP or PPPoE for the interface to get a dynamic address.

To configure the IP address for an interface, in the interface configuration mode, use the following command:

ip address {*ip-address/mask* | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

- *ip-address/mask* – Specifies the static IP address for the interface.
- **dhcp** [**setroute**] – Specifies the IP address which is allocated by DHCP. If setroute is configured, the system will set the gateway address provided by DHCP server as the default gateway route.
- **pppoe** [**setroute**] – Specifies the IP address which is allocated by PPPoE. If setroute is configured, the system will set the gateway address provided by PPPoE server as the default gateway route.

Here is an example of IP address configuration. To assign IP address 1.1.1.1 to interface ethernet0/0, use the following commands:

```
Enter the interface ethernet0/0 configuration mode:
hostname(config)# interface ethernet0/0
Configure the primary IP address for ethernet0/0:
hostname (config-if-eth0/0)# ip address 1.1.1.1/24
Exit the interface ethernet0/0 configuration mode:
hostname(config-if)# exit
```

Pay attention to the following two points:

- StoneOS supports two styles of subnet mask, i.e. 1.1.1.1/24 can also be represented as 1.1.1.1 255.255.255.0.
- To have an IP address, the interface must be bound to a zone.

To clear the IP address of an interface, use the command **no ip address** [*ip-address/mask* | **dhcp** | **pppoe**].

Configuring Interface Secondary IP

A static IP address can have up to 32 secondary IP addresses.

To assign a secondary IP address to an interface, in the interface configuration mode, use the following command:

ip address *ip-address/mask* **secondary**

- *ip-address/mask* – Specifies the secondary IP address.

To clear the secondary IP address, use the command **no ip address** *ip-address/mask* **secondary**. If you want to delete the IP address of a primary interface, you need to clear its secondary IP addresses first.



Notes: The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.

Configuring an Interface MTU Value

To set the Maximum Transmission Unit (MTU) value, in the interface configuration mode, use the following command:

ip mtu *value*

- *value* - Specifies the MTU value. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (The max MTU may vary on different platforms.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Jumbo Frame.

To restore to the default value, use the command **no ip mtu**.

Configuring Interface Force Shutdown

You can not only enforce to shut down a specific interface, but also control the time of shutdown by schedule, or control the shutdown according to the link status of tracked objects.

To shutdown an interface via CLI, in the interface configuration mode, use the following command:

shutdown [**track** *track-object*] [**schedule** *schedule-name*]

- **shutdown** – Shut down the interface immediately.
- **track** *track-object* – Specifies the name of tracked object. If this parameter is specified, the interface will shut down when the track object fails to work. For information on the tracked object, see Configuring a Track Object of System Management.
- **schedule** *schedule-name* – Specifies a schedule. If this parameter is specified, the interface will remain shut during the schedule time. For information on the time schedule, see Creating a Schedule of System Management.

To cancel force shut-down and clear all previous shutdown settings, use the command **no shut-down**.

Specifying the Track Object

The track object is used to monitor the working status of the interface. When the interface cannot work normally, the system will take the corresponding action. To specify the track object, in the interface configuration mode, use the following command:

monitor track *track-object-name*

- *track-object-name* – Specifies the name of the track object configured in the system.

To cancel the track object, in the interface configuration mode, use **no monitor** command.

Configuring Interface ARP Timeout

By default, the interface ARP timeout value is 1200 seconds. This can be changed within the range from 5 to 65535 seconds when necessary.

To change the ARP timeout value, in interface configuration mode, use the following command:

arp timeout *value*

To restore to the default value, use the command **no arp timeout**.

Configuring an Interface Protocol

To manage and configure devices through an interface using SSH, Telnet, Ping, SNMP, HTTP, HTTPS, FTP, Traceroute, or NETCONF, you need to enable the corresponding protocol first.

To enable a protocol above, in the interface configuration mode, use the following command:

manage {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp** | **traceroute** | **netconf**}

- **ssh** - Enables the SSH protocol on the interface.
- **telnet** - Enables the Telnet protocol on the interface.
- **ping** - Enables the Ping protocol on the interface.
- **snmp** - Enables the SNMP protocol on the interface.
- **http** - Enables the HTTP protocol on the interface.
- **https** - Enables the HTTPS protocol on the interface.
- **ftp** - Enables FTP protocol on the interface.
- **traceroute -** Enables Traceroute service of UDP on the interface. When enabled, the device can be tracked by other vendors' devices via the traceroute command.
- **netconf** - Enables the NETCONF protocol on the interface.

To disable a protocol, use the corresponding command **no manage** {**ssh** | **telnet** | **ping** | **snmp** | **http** | **https** | **ftp** |**traceroute**}.

Configuring FTP on the Interface

You can obtain log and configuration information via the FTP service on the interface. If the interface is enabled with FTP, you can create an FTP user and modify the FTP port number.

To create an FTP user, in the global configuration mode, use the following command:

ftp user *user-name* **password** *password*

- **user** *user-name* – Specifies the username for FTP.
- **password** *password* – Specifies the password for FTP.

You can configure up to three FTP users. To cancel the FTP user configuration, in the global configuration mode, use the command **no ftp user** *user-name*.

To modify the FTP port number, in the global configuration mode, use the following command:

ftp port *number*

- *number* – Specifies the FTP port number. The value range is 1 to 65535. The default value is 21.

To restore to the default FTP settings, in the global configuration mode, use the command **no ftp port**.

After the default FTP port is modifies, if the client logs in with the passive mode, then you need to enable application identification for the security zone the interface belongs to. In the security zone configuration mode, use the command **application-identify**.

To view the FTP configuration, in any mode, use the following command:

show ftp {**port** | **user**}

- **port** – Shows the FTP port number.
- **user** – Shows the FTP username, password and login status.

Configuring Port Mirroring

The device is designed with port mirroring on Ethernet interfaces. The port mirroring function forwards mirrored traffic based on the switch chip. Interfaces within the same switch chip belong to the same mirroring group. In this group, you can forward traffic from one or more source interfaces to another interface, enabling a traffic analysis device to monitor and analyze the traffic. This facilitates rapid fault location when a network issue occurs. The one or more source interfaces are called the "source interface of port mirroring", and the other interface is called the "destination interface of port mirroring".

Limits and Precautions

- The source and destination interfaces needs to be Ethernet interfaces. To serve as a destination interface, an Ethernet interface cannot not be bound to a security zone.
- Traffic mirroring can only occur between interfaces within the same mirroring group: the source and destination interfaces need to belong to the same group. Cross-group mirroring is not supported.
- Only one destination interface is allowed, but there is no limit on the number of source interfaces.
- An interface cannot simultaneously serve as both a source and a destination interface.
- The destination interface needs to be directly connected to the packet analysis device.
- MGT and HA interfaces do not support the port mirroring function.
- Port mirroring does not support IPv6.
- Enabling the port mirroring function will consume the bandwidth resources of the device, degrading the performance of the device in handling traffic. It is recommended to disable the function promptly after use.

Destination interface of port mirroring supported on Ethernet interfaces:

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules
SG-6000-A7600/A6800	No	No

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
SG-6000-A5800/A5600 /A5555/A5255/A5155	Yes (E0/0-E0/7 and XE0/8-XE0/9 belong to the same mirroring group; XE0/10-XE0/23 and XLE0/24-XLE0/25 belong to the same mirroring group)	No	
SG-6000-A5500/A5200 /A5100	Yes (except XE0/26-XE0/29)	No	
SG-6000-A3815/A3615 /A2815/A2715	Yes	IOC-A-F-4SFP+ IOC-A-F-8SFP+	Yes (Ethernet interfaces on the expansion module and on the

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			front panel belong to two different mirroring groups.)
		IOC-A-F-8GE	Yes (Ethernet interfaces on the expansion module and on the front panel belong to the same mirroring groups.)
SG-6000-A3800/A3700	Yes	No	
SG-6000-A3600/A3000 /A2800/A2700/A2600 /A2000/A1100/A200	Yes	Expansion module is not supported.	

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
A1000	Yes	Expansion module is not supported.	
SG-6000-K9180	Expansion module is not supported.	SIOM-P100-300ZKA	Yes (Port mirroring across expansion modules is not supported.)
SG-6000-K6580	No	No	
SG-6000-K6280/K6280-GS/K5680/K3680/K3680-GS/K3280/K2680/K2580/K2560/K2380/K1280	No	No	
SG-6000-X25812/X25803	N/A	SIOM-P100-400	Yes (Port mirroring across expansion modules is not supported.)
SG-6000-X10800/X9180	N/A	IOM-P40-300 IOM-P100-300 SIOM-P40-300	Yes (Port mirroring across expansion

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
		SIOM-P100-300 SIOM-P100D-300	modules is not supported.)
SG-6000-X8180	N/A	SIOM-P100-260 SIOM-P100H-260	Yes (Port mirroring across expansion modules is not supported.)
SG-6000-E2800/E2300 /E1700/E1606/E1600/E1100	No	Expansion module is not supported.	
SG-6000-E3968/E3960 /E3668/E3662/E3660 /E2868/E2860	Yes	IOC-8SFP-M	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
		IOC-8GE-M	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-4GE-B-M	Yes (Ethernet interfaces on the front panel and on expansion modules belong to the same mirroring group.)
SG-6000-E5568/E5560 /E5268/E5260/E5168/E3965	Yes	IOC-8SFP-M	Yes (Ethernet interfaces on the

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			expansion module and on the front panel belong to two different mirroring groups.)
		IOC-8GE-M	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-4GE-B-M	Yes (Ethernet interfaces on the front panel and on expansion mod-

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			ules belong to the same mirroring group.)
		IOC-8SFP+	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-4SFP+	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			groups.)
		IOC-2SFP+-Lite	When IOC-2SFP+-Lite is inserted in Slot4, XE4/0 does not support port mirroring. However, XE4/1 supports port mirroring and belongs to the same mirroring group as Ethernet interfaces on the front panel.
SG-6000-E5960/E5760/E5660	Yes	IOC-8SFP-M	Yes (Ethernet interfaces on the expansion module and on the

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			front panel belong to two different mirroring groups.)
		IOC-8GE-M	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-4GE-B-M	Yes (Ethernet interfaces on the front panel and on expansion modules belong to the same mir-

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			roring group.)

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
		IOC-8SFP+	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-4SFP+	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-2SFP+-Lite	When IOC-2SFP+-Lite is

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
			inserted in Slot2, port mirroring is not supported. When IOC-2SFP+-Lite is inserted in Slot 4, port mirroring is supported. Meanwhile, Ethernet interfaces on this module belong to the same mirroring group as those on the front panel.
SG-6000-E6368/E6360 /E6168/E6160	No	IOC-8SFP-M	yes
		IOC-8GE-M	yes

To configure a destination interface of port mirroring (also called analytic interface), in the global configuration mode, use the following command:

mirror to *interface-name*

- *interface-name* – Specifies the name of the destination interface of port mirroring. The destination interface must have no other configuration, such as binding to a zone.

To enable interface mirroring, in the interface configuration mode, use the following command:

mirror enable {**both** | **rx** | **tx**}

- **both** | **rx** | **tx** – Specifies traffic type to be mirrored. **both** indicates the ingress and egress traffic, **rx** indicates the ingress traffic (traffic entering the interface), and **tx** indicates the egress traffic (traffic exiting the interface). The default value is **both**.

To cancel the interface mirroring settings, in the interface configuration mode, use the command **no mirror**.

Configuring Mirror Filter

The interface with mirroring configured will mirror all the traffic to the analytic interface. Under heavy traffic, the mirroring might fail due to high load. To address this problem, the system is designed with mirror filter that allows user to filter the traffic to be mirrored, thus reducing the load.

The system supports the following filtering conditions:

- Source IP, source port
- Destination IP, destination port
- Protocol type
- Traffic direction (upstream/downstream)

To configure a mirror filter rule, in the global configuration mode, use the following command:

mirror filter interface *interface-name* {[**src-ip** *address-entry*][**src-port** *port-num*][**dst-ip** *address-entry*][**dst-port** *port-num*][**proto** {**icmp** | **tcp** | **udp** | *protocol-number* }] [**direct** {**down** | **up**}]}

- **interface** *interface-name* – Specifies the interface that enables mirror filter.
- **src-ip** *address-entry* – Specifies the source IP of the traffic. The system only mirrors traffic originating from the IP address to the analytic interface.
- **src-port** *port-num* – Specifies the source port of the traffic. The value range is 1 to 65535. The system only mirrors traffic originating from the port to the analytic interface.
- **dst-ip** *address-entry* – Specifies the destination IP of the traffic. The system only mirrors traffic destined to the IP address to the analytic interface.
- **dst-port** *port-num* – Specifies the destination port of the traffic. The value range is 1 to 65535. The system only mirrors traffic destined to the port to the analytic interface.
- **proto** {**icmp** | **tcp** | **udp**| *protocol-number*} – Specifies the protocol type. The system will only mirror traffic over the specified protocol to the analytic interface. You can specify the protocol type directly, namely icmp, tcp and udp, or specify the protocol number in the range of 1 to 255.
- **direct** {**down** | **up**} – Specifies the traffic direction. The system only mirrors the upstream (up) or downstream (down) traffic to the analytic interface.

After creating a mirror filter rule by the above command, the system will assign a rule ID for the new rule. To view the rule ID and related configuration information, in any mode, use the command **show mirror filter**.

To delete the specified mirror filter rule, in the global configuration mode, use the following command:

no mirror filter id *id*

- **id** *id* – Specifies the ID of the mirror filter rule to be deleted.

Notes:

- The system supports to configure at most 64 mirror filter rules.
- The expansion module of IOC-A-F-4SFP+ and IOC-A-F-8SFP+ supports to filter mirror traffic only by traffic direction (**mirror filter interface***interface-name***direct** {**down** | **up**}), but not by source IP address, source port, destination IP address, destination port, or protocol type.
- For the same interface, if **mirror enable** {**both** | **rx** | **tx**} is configured first and then a mirror filter rule is configured, traffic mirror follows the mirror filter rule.
- Not all platforms support mirror filter. Refer to the actual product for the application of the function.
- NAT interfaces do not support mirror filter.
- The mirrored traffic should not exceed the workload of the analytic interface.
- The logical interfaces do not support the mirror filter.

Configuring Traffic Mirroring

Notes: After you configure mirror Profile, the data forwarding performance of the device will be affected. Exercise caution when you run this command. Since networking complexity varies with users, we recommend that you contact the technical engineers from Hillstone before you enable the function. If you do not have requirements or finish location debugging, disable the function as soon as possible.

By configuring a mirror profile in the device and binding it to a policy, StoneOS can achieve the traffic mirroring function. This function can mirror the traffic that matches the specified policy to the particular interface or IP address. Generally, configuring policy-based traffic mirroring, take the following two steps:

1. Configure a mirror profile. The mirror profile defines the interface/IP address that the traffic is mirrored to.

2. Bind the mirror profile to the policy.

Configuring a Mirror Profile

To configure a mirror profile, in the global configuration mode, use the following command to enter the mirror profile configuration mode first.

mirror-profile *mirror-profile-name*

- *mirror-profile-name* - Enter the name of the mirror profile. After executing this command, StoneOS will create a mirror profile and enter the mirror profile configuration mode. If the entered name already exists, StoneOS will enter the mirror profile configuration mode. One mirror profile can include eight rules of the same type.

In the global configuration mode, use the following command to delete the specified mirror profile:

no mirror-profile *mirror-profile-name*

In the mirror profile configuration mode, you can specify the action for the traffic that matched the policy. If you want to mirror the traffic to the interface, you need to specify the destination interface and the direction of the traffic; if you want to mirror the traffic to the IP address, you need to specify the destination IP address, egress interface, next-hop address, and the direction of the traffic.

Mirroring Traffic to an Interface

StoneOS can mirror traffic that matches the policy to the specified interface (including ethernet or tunnel interface) . By default, bidirectional traffic that matches the policy will be mirrored to the interface. Besides, you can filter the traffic based on the direction. You can specify a direction option, including forward, backward, or bidirectional. Then the traffic of the specified direction will be mirrored to the interface. In the mirror profile configuration mode, use the following command to specify the interface and configure the filter settings:

destination interface {*interface-name* | *tunnel-interface* [*tunnel-gateway-ip*]} [**direction** { **forward** | **backward** | **bidirection**}]

- *interface-name* - Specify the interface name. The traffic that matches the policy will be mirrored to this interface.
- *tunnel-interface* [*tunnel-gateway-ip*]- Specify the destination tunnel interface name for the mirrored traffic.Tunnel gateway IP (tunnel-gateway-ip) can also be specified as needed to distinguish between different GRE tunnels bound to the same tunnel interface.
- **direction** {**forward** | **backward** | **bidirection**} - Use **forward** to only mirror the forward traffic to the specified interface; use **backward** to only mirror the backward traffic to the specified interface. Use **bidirection** to mirror both forward traffic and backward traffic to the specified interface.

To delete this rule, use the following command in the mirror profile configuration mode:

no destination interface *interface-name*

Mirroring Traffic to an IP Address

StoneOS can mirror traffic that matches the policy to the specified destination IP address. By default, bidirectional traffic that matches the policy will be mirrored to the IP address. Besides, you can filter the traffic based on the direction. You can specify a direction option, including forward, backward, and bidirectional. Then the traffic of the specified direction will be mirrored to the destination IP address. In the mirror profile configuration mode, use the following command to specify the interface and configure the filter settings:

destination {**ip***dest-ipv4-address* | **ipv6***dest-ipv6-address*} *interface-name* [*nexthop-ipv4-address* | *nexthop-ipv6-address*] [**direction** {**forward** | **backward**}]

- **ip***dest-ipv4-address* | **ipv6***dest-ipv6-address* – Specify the destination IP address of mirrored traffic, which can be IPv4 or IPv6 address. The device will replace the destination address of packets based on the specified destination IP address.
- *interface-name* – Specify the egress interface of the traffic that matches the policy.

- *nexthop-ipv4-address* | *nexthop-ipv6-address* – Specify the next-hop address of mirrored traffic, which can be IPv4 or IPv6 address. The address type needs to be the same as that of the specified destination IP address (*dest-ipv4-address* | **ipv6***dest-ipv6-address*).
- **direction** {**forward** | **backward**} – Use **forward** to only mirror the forward traffic to the specified IP address; use **backward** to only mirror the backward traffic to the specified IP address. Use **bidirection** to mirror both forward traffic and backward traffic to the specified IP address.

To delete this rule, use the following command in the mirror profile configuration mode:

no destination {**ip***dest-ipv4-address* | **ipv6***dest-ipv6-address*}

Binding a Mirror Profile to a Policy

After configuring a mirror policy, you need to bind it to a policy to make it take effect. To bind a mirror profile to a policy, use the following command in the policy configuration mode:

mirror *profile-name*

- *profile-name* - Specify the name of the mirror profile. This profile will be bound to the policy.

To cancel the binding settings, in the policy configuration mode, use the following command:

no mirror *profile-name*

Viewing Mirror Profile Information

To view the mirror profile information, use the following command in any mode:

show mirror-profile [*mirror-profile-name*]

- *mirror-profile-name* – Enter the mirror profile name. The information of this profile will be displayed. Without name specified, information of all mirror profiles will be displayed.

Interface Reverse Route

Reverse route is used for forwarding the reverse path data. A reverse path is in the opposite direction in relation to the initial data flow direction. It only works on Layer 3 interfaces.

To enable reverse route on an interface, use the following command:

reverse-route {**force** | **prefer**| **direct-forward** [**per-packet**]}

- **force** – Forces to use reverse route. If the reverse path is found, forward the reverse data by reserve route; if not, drop the packet. By default, reverse route is forced on Layer 3 interfaces.
- **prefer** – Uses reverse path in preference to other route. If the reverse route is found, use it to forward data; if not, use the original return path (i.e. the current interface).
- **direct-forward** - Disable the reverse route. All the reverse data backtracks and no reverse route check is carried out.
- **per-packet** - Enable per-packet check. When the reverse route is disabled and this parameter is specified, the per-packet check is enabled and the system check the MAC information of session by packet. If the MAC information of session is not consistent with the source MAC information of the forward data, the MAC information of session will be modified according to the source MAC information of the forward data. By default, this function is disabled.

To disable the reverse route, use the command **no reverse-route**. All the reverse data backtracks and no reverse route check is carried out.



Notes: If the egress and ingress interfaces of the reverse route are not in the same zone, packets will be discarded.

Configuring Interface Backup

If an interface is specified as a backup to another one, it will replace the primary interface to take over its traffic when the schedule takes effect or track object fails, and stops working when the configured condition expires so that the traffic are processed by the primary interface again.

To specify an interface as the backup interface, in the interface configuration mode, use the following command:

backup-interface *interface-name* {**schedule** *schedule-name* [**overlap-time** *time*] | **track** *track-object-name* [**schedule** *schedule-name* [**overlap-time** *time*]]}

- *interface-name* – Specifies which interface is the backup interface.
- *schedule-name* – Specifies the schedule. During the specified schedule time period, data flow is directed to the backup interface.
- *time* - The migrating time before data being completely switched to the backup interface. The value range is 1 to 60 seconds. The parameter is disabled by default, i.e. all data flow is transferred to the backup interface immediately without migrating time.
- *track-object-name* – Specifies the track object. If the track object fails to response, data flow will be migrated from the primary to backup interface. If the object tracking is restored to normal, data flow will be switched back to the primary interface.

To cancel the backup interface settings, use the following command:

no backup-interface

Configuring Hold Time

A physical interface can be in two connection states: up and down. During the hold time, the state switches of the physical layer between the two states will not be notified to the system; after the hold time, if the state is not restored, the change will be notified to the system. This function can avoid instable network problems caused by frequent changes of physical interface states within a short period.

To configure hold time, in the interface configuration mode (only applicable to physical interfaces), use the following commands:

- **holddown** *time* - Specifies the holddown time. With this parameter configured, the system will not determine the up state unless the state of an interface is switched from down to up and keeps for X seconds (X is specified by time). The value range is 1*500 to 3600* 500 milliseconds. For example, parameter holddown 10 indicates the holddown time is 5 seconds.
- **holdup** *time* - Specifies the holdup time. With this parameter configured, the system will not determine the down state unless the state of an interface is switched from up to down and

keeps for X seconds (X is specified by time). The value range is 1*500 to 3600* 500 milliseconds. For example, parameter holdup 10 indicates the holdup time is 5 seconds.

To cancel the specified hold time, in the interface configuration mode, use the command **no hold-down** or **no holdup**.

Configuring the Keepalive Function of Interface

After the system use PPPoE for the interface to get a dynamic address, if PPPoE function is not used for a long time, the interface address will age out automatically and then be deleted. The keepalive function prevent the aging out of PPPoE interface and keep the interface alive.

To configure the keepalive function, in the interface configuration mode, use the following command:

keepalive *IP-address*

- *IP-address* – Specifies the IP address of PPPoE server.

To cancel the keepalive function, in the interface configuration mode, use the following command:

no keepalive

Configuring the Interface Group

The interface group function binds the status of several interfaces to form a logical group. If any interface in the group is faulty, the status of the other interfaces will be Down. After all the interfaces return to normal, the status of the interface group will be Up. The interface group function can binds the status of interfaces on different expansion modules.

To create an interface group and enter the interface group configuration mode, in the global configuration mode, use the following command:

interface-group *group-name* **type linkage**

- *group-name* – Specifies the name of the interface group. The length is 1 to 31 characters.

To add interfaces to the interface group, in the interface group configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the interface name which will be added to the interface group. The maximum number of interfaces is 16.

For example, adding ethernet0/0 and ethernet0/1 to the interface group test to achieve the interface linkage, in the global configuration mode, use the following command:

```
hostname(config)# interface-group test type linkage
hostname(config-if-group)# interface ethernet0/0
hostname(config-if-group)# interface ethernet0/1
```

In the global configuration mode, use the no form to delete the specified interface group:

no interface-group *group-name*

To view the status of the specified interface group, in any mode, use the following command:

show interface-group *group-name*

Disabling Recording Interface IP Address Conflict Log Triggered by DAD Mode ARP Packets

DAD （Duplicate Address Detection） mode ARP packets is a special type of gratuitous ARP packets, its source IP is 0.0.0.0, and the destination IP is the specific IP address of packets detection. It is mainly used to detect address conflict.

By default, system will determine whether the received the ARP packets is a DAD mode ARP packet. If it is DAD mode ARP packet, and its destination IP address is in conflict with the interface IP address or the address in the NAT address pool, system will record the interface IP address conflict log. To improve device performance and reduce device memory utilization and false positives, you can disable the function of recording interface IP address conflict logs triggered by DAD mode ARP packets.

To disable the function of recording interface IP address conflict log, in the interface configuration mode, use the following command:

no dad-alarm

To re-enable the function of recording interface IP address conflict log, in the interface configuration mode, use the following command:

dad-alarm

Configuring Local ARP Proxy for Interfaces

When the device interface receives an ARP request with a destination IP of the same network segment, the local ARP proxy function allows the device to reply with its own MAC address as the source address. This implements communication between users within the same network segment during port isolation.

Local ARP proxy is applicable only to Layer-3 interface. To enable local ARP proxy, use the following command in interface configuration mode:

proxy-arp local

To disable local ARP proxy, use the **no proxy-arp local** command.

To check whether ARP proxy is enabled for interface, use the following command in any mode:

show proxy-arp

Configuring 10 G Interface Auto Tuning

The system supports 10 G Interface Auto Tuning. The specified 10 G interface or all 10 G interfaces are automatically and periodically detected. If the interface status is abnormal, such as frequent Physical Up/Down or a large number of error packets, the interface parameters can be adjusted through Auto Tuning to effectively reduce the bit error ratio (BER) of the receiving end.

To configure 10 G interface Auto Tuning, in the interface configuration mode, use the following command:

auto_tune {**on** | **off** | **interval***interval-time*}

- **on** – Enable automatic detection of Auto Tuning for the specified 10 G interface. Once conditions are met, the interface will perform Auto Tuning. The detection is enabled by default.
- **off** – Disable automatic detection of Auto Tuning for the specified 10 G interface.

- **interval** *interval-time* – Specifies the interval between two automatic detection. The value ranges from 3 to 10 seconds.

To force specified 10 G interface to perform Auto Tuning, in the interface configuration mode, use the following command:

auto_tune once

Once the command is configured, the interface will immediately perform one-time Auto Tuning.

To configure Auto Tuning for all 10 G interfaces, in the global configuration mode, use the following command:

auto_tune {**on** | **off** | **interval** *interval-time*}

- **on** – Enable automatic detection of Auto Tuning for all 10 G interfaces. Once conditions are met, all interfaces will perform Auto Tuning. The detection is enabled by default.
- **off** – Disable automatic detection of Auto Tuning for all 10 G interfaces.
- **interval** *interval-time* – Specifies the interval between two automatic detection. The value ranges from 3 to 10 seconds.

Enabling/Disabling the First Data Proxy Function of Interface

After you enable the First Data Proxy function of interface, you can obtain and log the domain information of HTTP/HTTPS packets in the interface traffic. By default, the First Data Proxy function of interface is disabled.

To enable/disable the First Data Proxy function of interface, in interface configuration mode, use the following command:

- Enable: **first-data-proxy enable**
- Disable: **no first-data-proxy enable**

Configuring Interface Proxy ARP

When the device receives ARP request with a destination IP of a different network segment, proxy ARP feature allows the device to reply with its own MAC address as the source address.

Proxy ARP can work only on Layer-3 interface.

To enable proxy ARP, in the interface configuration mode, use the following command:

proxy-arp [**dns**]

- **proxy-arp** – Enables proxy ARP on the interface.
- **dns** – This parameter is for PnP IP

To disable proxy ARP, use the command **no proxy-arp**.

To view the IP address of the ARP proxy, in any mode, use the following command:

show proxy {**arp**|**nd**} [**vrouter**]

- **arp** - Displays the IPv4 address of the ARP proxy.
- **nd** - Displays the IPv6 address of the ARP proxy.
- **vrouter** - Displays the proxy address of the specified VRouter.

If an interface has been enabled with proxy ARP (with the parameter dns configured) and DNS proxy, it is a plug-and-play (PnP) interface, which means the internal computers with dynamic IP and DNS are able to access to the Internet through this interface. However, you should keep in mind that:

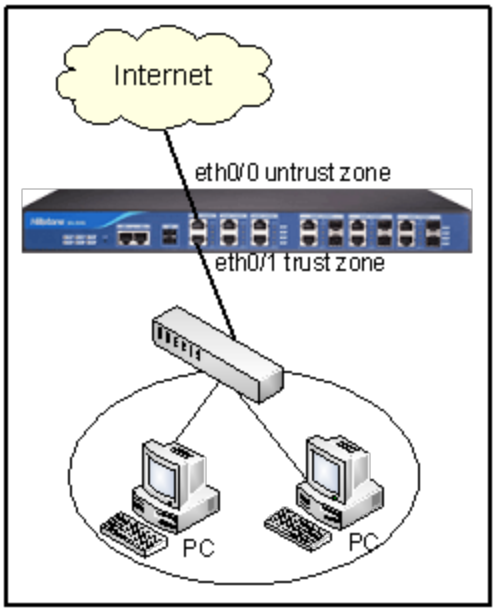
- If a computer and the PnP interface are in the same network segment, to allow the computer to visit the Internet, make sure that the computer uses the interface IP address as its gateway. For instance, an interface IP is 192.168.1.1/24 and a computer IP is 192.168.1.55/24. In order to allow the computer to visit the Internet through this interface, make the computer gateway address as 192.168.1.1.

- It is suggested to assign an unusual IP address with 32 bit mask to a PnP interface, like 10.199.199.199/32, which can ensure that there will be no identical IP address in the subnet.

> **Tip:** For information on DNS proxy configuration, see Configuring a DNS Proxy.

PnP IP Configuration Example

The goal is to enable the PnP IP function on an interface to allow LAN users to visit the Internet. The topology is shown in Figure below: ethernet0/0 is connected to the Internet; ethernet0/1 is connected to the Intranet; DNS server IP is 202.106.1.1.



Take the following steps:

Step1: Configure an interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
```

```
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure a DNS server

```
hostname(config)# ip name-server 202.106.1.1
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/1
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.1.1
hostname(config-dns-proxy-rule)# exit
```

Step 3: Configure the PnP IP feature (i.e. DNS proxy and proxy ARP)

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# dns-proxy
hostname(config-if-eth0/1)# proxy-arp dns
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service any permit
hostname(config-policy)# exit
hostname(config)#
```

Configuring Local Property

Sytem supports to configure an editable Local property for all interfaces (except VSwitch) to avoid the duplicate MAC address when managing huge amount of HA devices in the same Layer 2 Network. The sub-interface and virtual forward interface don’ t need to configure Local property, which inherit the primary interface directly. If you configure Local property foran interface , the system will not synchronize this configuration with the backup device. In the interface configuration mode, use the following command:

local

To delete HA Local property, in interface configuration mode, use command **no local**.

Configuring a Loopback Interface

As a logical interface, loopback interface always remains in working state until the device shuts down. The naming rule for loopback interface is loopbackNumber (Number is an integer number from 1 to 256). The unique identifier for a loopback interface is its name.

Creating a Loopback Interface

To create a loopback interface, in the global configuration mode, use the following command:

interface loopback*Number*

• *Number* – The ID number of the loopback interface.

If loopback interface already exists, this command leads you into the interface configuration mode directly.

For example, to create a loopback named loopback1, in the global configuration mode, use the following command:

```
hostname(config)# interface loopback1
hostname(config-if-loo1)#
```

To delete a loopback interface, in the global configuration mode, use the command **no interface loopback***Number*.

Configuring an Ethernet Interface

All the Ethernet interfaces of Hillstone devices are gigabit interfaces. Gigabit Ethernet interface conforms to 1000Base-T physical layer specifications. They can work under the rate of 10Mbit/s, 100Mbit/s and 1000Mbit/s. Both full-duplex and half-duplex modes are supported, but Gigabit half-duplex mode is not supported.

Configuring an Ethernet Sub-interface

Ethernet interface is allowed to have sub-interfaces.

To create a sub-interface, in the global configuration mode, use the following command:

interface ethernetm/n.*tag*

- *.tag* – Specifies a number to mark the sub-interface. The value range is 1 to 4094. For example, the command **interface ethernet0/0.1** creates a sub-interface named ethernet0/0.1 for interface ethernet0/0.

If the sub-interface exists, this command leads you into the interface configuration mode directly.

To delete a sub-interface, use the command **no interface ethernetm/n**.*tag*.

The Ethernet sub-interface supports PPPoE. One Ethernet interface can only be bound to one PPPoE instance.

Entering the Ethernet Configuration Mode

You must the enter Ethernet configuration mode in order to configure settings like interface speed, duplex modes and Combo type, etc.

To enter the Ethernet configuration mode, in the global configuration mode, use the following command:

interface *ethernetm/n*

- *ethernetm/n* – Specifies the Ethernet interface.

Configuring an Interface Duplex Mode and Speed

- Gigabit Ethernet copper interface: can work under full and half duplex mode, and can adapt to link speed of 10Mbit/s, 100Mbit/s and 1000Mbit/s.
- Gigabit Ethernet fiber-optic interface: It can work only in full duplex mode. The default speed is 1000Mbit/s, which can be backward switched to 100Mbit/s. **Note**: Therefore, please do not configure the working mode and speed of the Gigabit Ethernet fiber-optic interface.

To configure a duplex mode and speed for an interface, in interface configuration mode, use the following command:

duplex*method* [**speed***value*]

- *method* - This parameter can be auto, full (for full-duplex mode) or half (for half-duplex mode). When it is specified as auto, the interface rate will will automatically be auto. You don't need to continue to specify the rate. At this time, the system will automatically select the best duplex mode and rate.The default duplex method is auto, which means the system assigns a proper mode for the interface.
- *value* - This parameter can be auto, 10, 100 or 1000. auto is the default value, which means the system automatically detects and assigns a proper link speed. The link speed specified here must conform to the actual network link speed of this end and of the peer device.

To restore to the default value, use the command **no duplex**.



Notes: For the SFP+ interface of the device, after you use the command **channel-speed 1000** to switch to 1G working mode, the interface works in forced mode, full duplex mode, and 1000Mbit/s rate by default. You do not need to use the command **duplex full speed 1000** to set the interface to a fixed full-duplex working mode and a fixed rate of 1000Mbit/s. To change the mandatory mode to auto-negotiation, use the command **duplex auto**. Other duplex modes and rates are not supported.

To backward switch the speed of **Gigabit Ethernet fiber-optic interface** to 100Mbit/s, in interface configuration mode, use the following command:

speed 100basefx

To restore the speed of the interface to the default value 1000Mbit/s, in interface configuration mode, use the following command:

no speed



Notes: Only the following devices allows you to backward switch the speed of Gigabit Ethernet fiber-optic interface: SG-6000-A5500, A5200, A5100, A3800, A3700, A3600, A3000, A2800, and A2700. When you set to the 100 Mbps working mode, the fiber-optic interface can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers.

Cloning a MAC Address

To clone a MAC address to the Ethernet sub-interface, in the Ethernet sub-interface configuration mode, use the following command:

mac-clone *H.H.H*

- *H.H.H* – Specifies the MAC address.

To delete the specified MAC address, in the Ethernet sub-interface configuration mode, use the command **no mac-clone**.

If the MAC address changes after the PPPoE connection has been established, you need to re-connect the PPPoE client to make the new MAC address take effect.

Configuring a Combo Type

A Combo port is the combination of a fiber-optic port and a copper port. By default, if both of the ports have cables connected, fiber-optic port has the priority. If the copper port was used at first, after restarting the device, the fiber-optic port will be activated and used to transfer data if it is connected with cable. You can also select one of the two ports via CLI.

To select a copper or fiber-optic port, in the interface configuration mode, use the following command:

combo {**copper-forced** | **copper-preferred** | **fiber-forced** | **fiber-preferred**}

- **copper-forced** – Forces to use the copper port.
- **copper-preferred** – Prioritizes the copper port.
- **fiber-forced** – Forces to use the fiber-optic port.
- **fiber-preferred** – Prioritizes the fiber-optic port. When this parameter is configured, the data flow will switch from the copper port to the fiber-optic port automatically and there is no need to restart device.

To resume to the default setting, use the command **no combo**.

Configuring a VSwitch Interface

VSwitch interface is a Layer-3 interface. It is an assembly of all interfaces in the VSwitch. When you create a VSwitch, its corresponding VSwitch interface is automatically created.

Creating a VSwitch Interface

To create a VSwitch interface, in the global configuration mode, use the following command:

vswitch vswitch*Number*

- *Number* - Specifies a number as the identifier of the VSwitch and its interface. The value range may vary from different platform models.

To clear the VSwitch and its corresponding interface, use the command **no vswitch vswitch***Number*.

Configuring an Aggregate Interface

An aggregate interface is an assembly of two or more physical interfaces. The data flow passing through the aggregate interface is shared equally by its physical interfaces. This method can increase the usable bandwidth. If one of the interfaces fails to work, other interface(s) can take over its data flow and process data, but bandwidth is reduced. The following sections introduce basic configurations of aggregate interface.

Creating an Aggregate Interface and Sub-interface

To create an aggregate interface, in the global configuration mode, use the following command:

interface aggregate*Number*

- *Number* - Specifies the ID of the aggregate interface. For different product models, the range of Number is different. For example, the command interface aggregate2 creates an aggregate interface named "aggregate2".

This command leads you into the aggregate interface configuration mode. If the specified interface exists, you will enter its configuration mode directly.

To delete an aggregate interface, in the global configuration mode, use the command **no interface aggregate***Number*. Before deleting it, you must clear all the settings and zone referencing of the interface.

To create a sub-interface for an aggregate interface, in the global configuration mode, use the following command:

interface aggregateNumber*.tag*

- *.tag* – Specifies the ID of the sub-interface. The parameter is an integer number from 1 to 4094. For example, the command interface aggregate2.1 creates a sub-interface named aggregate2.1 for aggregate interface named aggregate2.

To delete an aggregate sub-interface, in the global configuration mode, use the command **no interface aggregateNumber***.tag*. Before deleting an interface, you should clear all settings of it, including the binding and referencing with other interfaces and zones, etc.

Adding a Physical Interface

An aggregate interface includes two or more physical interfaces.

To add a physical interface to an aggregation interface, in the physical interface configuration mode, use the following command:

aggregate *aggregatenumber*

- *aggregatenumber* - Specifies the name of the aggregation interface to which the physical interface is added. Ensure that the physical interface does not belong to any other interface or zone.

To remove a physical interface from the aggregation interface, in the physical interface configuration mode, use the command **no aggregate**.

Example of Configuring an Aggregate Interface

Here is a configuration example. The goal is to create aggregation interface aggregate2, and add ethernet0/3 and ethernet0/4 to the aggregate2, then delete ethernet0/3 from it.

Use the following commands:

```
hostname(config)# interface aggregate2
hostname(config-if-agg2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# aggregate aggregate2
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# aggregate aggregate2
hostname(config-if-eth0/4)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# no aggregate
```

Configuring a Redundant Interface

A redundant interface consists of two physical interfaces, one of which works as the primary interface processing the traffic flow through the redundant interface, the other one stands by and substitutes the primary interface to process data flow when it fails to work.

Creating a Redundant Interfaces and Sub-interface

To create a redundant interface, in the global configuration mode, use the following command:

interface redundant *Number*

- *Number* - Specifies the ID of the redundant interface. For example, the command interface redundant2 creates a redundant interface named redundant2.

This command takes you into the redundant interface configuration mode. If the specified interface exists, you will directly enter its configuration mode.

To delete a redundant interface, in the global configuration mode, use the command **no interface redundant** *Number*.

Before deleting it, you should clear all settings, including the binding and referencing with other interfaces and zones, etc.

To create a sub-interface for an existing redundant interface, in the global configuration mode, use the following command:

interface redundant Number *.tag*

- *.tag* – Specifies the ID of the sub-interface. This parameter should be an integer from 1 to 4094. For example, the command interface redundant2.1 creates a sub-interface called redundant2.1 for the redundant interface named redundant2.

To delete a redundant sub-interface, in the global configuration mode, use the command **no interface redundant Number** *.tag*.

Adding a Physical Interface

To add a physical interface to a redundant interface, in the physical interface configuration mode, use the following command:

redundant *interface-name*

- *interface-name* – Specifies the name of the redundant interface to which the physical interface is added. Make sure that the physical interface does not belong to any other interface or zone.

To remove a physical interface from a redundant interface, use the command **no redundant**. If the deleted interface serves as the primary interface, you need to clear the master interface setting first.

Specifying the Primary Interface

To specify a physical interface in the redundant interface as the primary interface, in the redundant interface configuration mode, use the following command:

primary *interface-name*

- *interface-name* - Specifies the name of the primary interface.

To cancel the primary interface, in the redundant interface configuration mode, use the command **no primary**.

Enabling/Disabling alarm logs of ARP loops

After an interface receives ARP packets, system will judge whether the source MAC address of packets is consistent with the MAC address of the interface. If it's consistent, system will form a loop. If the alarm logs feature of ARP loops is enabled, the alarm logs of ARP loops will be generated frequently. You can enable or disable the alarm logs by the following commands.

By default, the alarm logs feature of ARP loops in the interface is enabled. To disable the feature for the redundant interface, in the redundant interface configuration mode, use the following command:

arp-loop-alarm-disable

To restore default values, in the interface configuration mode, using the following command:

no arp-loop-alarm-disable

Example of Configuring a Redundant Interface

Here is a configuration example. The goal is to create a redundant interface named redundant1, add the interface ethernet0/4 and interface ethernet0/5 to redundant1, and to make ethernet0/4 as the primary interface, then remove ethernet0/5 from redundant1.

Use the following commands:

```
hostname(config)# interface redundant1
hostname(config-if-red1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# redundant redundant1
```

```
hostname(config-if-eth0/4)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# redundant redundant1
hostname(config-if-eth0/5)# exit
hostname(config)# interface redundant1
hostname(config-if-red1)# primary ethernet0/4
hostname(config-if-red1)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# no redundant
```

Configuring a Tunnel Interface

Tunnel interface serves as the entrance of VPN tunnel and the VPN traffic goes through the tunnel interface. Tunnel interface is a Layer-3 interface.



Notes: Non-root VSYS does not support to create the tunnel interface.

Creating a Tunnel Interface

To create a tunnel interface, in the global configuration mode, use the following command below:

interface tunnel*Number*

- *Number* - Specifies the ID of the tunnel interface. For example, the command interface tunnel2 creates the tunnel interface named tunnel 2.

This command leads you to the tunnel interface configuration mode. If the tunnel interface of the specified name exists, you will directly enter the tunnel interface configuration mode.

To delete a tunnel interface, use the command **no interface tunnel***Number*.

Binding a Tunnel

You can bind a tunnel interface to an IPsec VPN, GRE, SSL VPN, L2TP tunnel, IPv6 over IPv4 tunnel, IPv4 over IPv6 tunnel, or ZTNA instance. A tunnel interface can be bound to multiple IPsec VPN or GRE tunnels, but only one SSL VPN tunnel, L2TP tunnel, IPv6 over IPv4 tunnel, IPv4 over IPv6 tunnel, or ZTNA instance.

To bind a tunnel to the tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel {**ipsec***tunnel-name* [**gw** {*ipv4-address* | *ipv6-address*}] | **gre***tunnel-name* [**gw** {*ipv4-address* | *iv6p-address* | *ipv4-addressipv6-address*}] | **scvpn***instance-name* | **l2tp***tunnel-name* | **ipv4-over-ipv6***tunnel-name* | **ipv6-over-ipv4***tunnel-name* | **ztna***instance-name*}

- **ipsec***tunnel-name* – Specifies the tunnel type and its name.
- **gw**{*ipv4-address* | *ipv6-address*} – Specifies the next hop IP address of the tunnel interface, which can be the IP address of the peer tunnel interface or the IP address of the egress interface on the other end. This parameter is only valid for an interface which binds to multiple IPsec VPN tunnels.
- **gre** *tunnel-name* – Specifies the tunnel type and its name.
- {*ipv4-address* | *ipv6-address* | *ipv4-address ipv6-address*} – Specifies the next hop IP address of the tunnel interface, which can be the IP address of the peer tunnel interface or the IP address of the egress interface on the other end. This parameter is only valid for an interface which binds to multiple GRE tunnels. The next hop IP addresses can be specified to IPv4 and/or IPv6 addresses.
- **scvpn***instance-name* – Specifies the name of SSL VPN instance bound to this interface. A tunnel interface can be bound to only one SSL VPN instance.
- **l2tp** *tunnel-name* – Specifies the name of L2TP tunnel bound to this interface. A tunnel interface can be bound to only one L2TP tunnel.

- **ipv4-over-ipv6***tunnel-name* – Specifies the name of IPv6 over IPv4 tunnel bound to this interface. A tunnel interface can be bound to only one IPv6 over IPv4 tunnel.
- **ipv6-over-ipv4***tunnel-name* - Specifies the name of IPv4 over IPv6 tunnel bound to this interface. A tunnel interface can be bound to only one IPv4 over IPv6 tunnel.
- **ztna***instance-name* - Specifies the name of remote access ZTNA instance bound to this interface. A tunnel interface can be bound to only one remote access ZTNA instance.

Repeat this command to bind more IPsec VPN tunnels or GRE tunnels.

To cancel the binding relationship, use the command **no tunnel** {**ipsec***vpn-name* | **gre***tunnel-name* | **scvpn***instance-name* | **l2tp***tunnel-name* | **ipv4-over-ipv6***tunnel-name* | **ipv6-over-ipv4***tunnel-name* | **ztna***instance-name*}.

Cloning a MAC Address

Only CloudEdge supports this function. When the VXLAN tunnel is bound to Layer 3 zone, CloudEdge supports to specify the same MAC address for multiple Layer 3 tunnel interfaces by using MAC address cloning. This reduces resource consumption caused by MAC table learning for Layer 3 tunnel interfaces.

To clone a MAC Address, in tunnel interface configuration mode, use the following command:

mac-clone*H.H.H*

- *H.H.H* - Specifies the MAC address of the tunnel interface, which cannot be a broadcast MAC address, multicast MAC address, or all-zero MAC address.

In tunnel interface configuration mode, use the **no mac-clone** command to delete the specified MAC address.

Multi-tunnel OSPF

In some site-to-site VPN connections, a tunnel interface binds with multiple tunnels. If OSPF dynamic routing is used to manage data exchange among different sites, you need to enable point-to-multipoint tunnel interface (the default tunnel interface is point-to-point network type).

To configure point-to-multipoint type, in the tunnel interface configuration mode, use the following command:

ip ospf network point-to-multipoint

To restore to the default point-to-point type, use the following command:

no ip ospf network point-to-multipoint

Borrowing an IP Address (IP Unnumbered)

In some cases, like when tunnel interface is used to forward packets which go through the device, configuring an IP address is not required for that interface. In situation like that, you can use the IP address borrowing feature (IP unnumbered) to borrow IP addresses from other interfaces.

To enable the IP address borrowing feature, in the tunnel interface configuration mode, use the following command:

ip address unnumber *interface-name*

- *interface-name* – Specifies the name of the interface from which the IP address is borrowed.

To clear the borrowed IP, use following command:

no ip address unnumber



Notes: Interfaces on the two ends of the tunnel are not allowed to use borrowed IP address at the same time.

Viewing Tunnel Information

To view tunnel information, in any mode, use the following command:

show interface bind-tunnels *tunnel-name*

- *tunnel-name* – Specifies the name of the tunnel interface to be shown.

Configuring a PPPoE Sub-interface

One physical interface can have multiple PPPoE sub-interfaces so that multiple ISPs can be accessed through this one interface.

To create a PPPoE sub-interface, in the global configuration mode, use the following command:

interface ethernet*X/Y***-pppoe***Z*

- **ethernet***X/Y* – Specifies the name of the Ethernet port. For instance, ethernet0/5.
- **-pppoe***Z* – Specifies the name of PPPoE sub-interface. Z indicates the ID of the PPPoE sub-interface. The value range varies with platforms.

To clear a PPPoE sub-interface, in the global configuration mode, use the following command:

no interface ethernet*X/Y***-pppoe***Z*



Notes: Non-root VSYS does not support to create the PPPoE interface.

Configuring a Vif Interface

The Vif interface is a logical interface, which is used for Multicast Service Reflection (MSR). On the Vif interface, you can configure the IGMP Join-group function to direct multicast traffic to the MSR device, and then convert the original multicast streams (S1, G1) into new multicast streams (S2, G2) based on the address mapping configured on the MSR device.

Creating a Vif Interface

To create a Vif interface, in global configuration mode, use the following command:

interface vif1

To delete the specified Vif interface, in global configuration mode, use the following command:

no interface vif1

Link Aggregation

Link aggregation combines multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

The device supports forced link aggregation and LACP (Link Aggregation Control Protocol). The forced link aggregation is implemented by the aggregate interface. For more information, see Configuring an Aggregate Interface. This section mainly describes the usage of LACP.

LACP

LACP (Link Aggregation Control Protocol) is designed to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that is also enabled with LACP).

Hillstone devices use the aggregate interface to implement the LACP function. The aggregate interface with LACP enabled is named as aggregate group, and the physical interfaces in the aggregate group is the member of the aggregate group. After enabling LACP on an aggregate interface, the member interface sends the LACPDU packets to the peer to notify its system priority, system MAC address, port priority, port number, and operating key. The peer receives the LACPDU and compare the information with the local information to select a proper member interface, thus the both sides can decide which link will be used to transfer data.

Member Status in an Aggregate Group

There are four statuses for the member interfaces in an aggregate group:

- Unselected: The interface is selected by the aggregate group and cannot forward traffic. This status is usually caused by physical reasons, e.g., the interface mode is non-duplex, rates of both sides are inconsistent, physical connection failure, etc.
- Selected: The interface is in aggregate group, but its peer is not ready, so the interface cannot forward traffic. When it receives LACPDU packets from the peer, and learns the status of its peer is Selected, the status of the interface will switch to Active. The interface in Active status can forward traffic.
- Standby: The interface is a backup interface, and cannot forward traffic. If the LACP priority of the interface is promoted, the interface will replace the existing Selected interface and change its own status to Selected, and the status of the replaced interface will switch to

Standby. When other interfaces become Unselected, the Standby interface will change to Selected interface automatically.

- Active: The interface is aggregated successfully and forwards traffic. If the interface has not received LACPDU packets from the peer in three LACPDU timeouts, it will be concluded as link down. In such a case, the status of the interface will switch to Selected, and the interface will stop forwarding traffic.

Configuring LACP

The configurations of LACP include:

- Enabling/Disabling LACP
- Specifying LACP System Priority
- Specifying Interface LACP Priority
- Specifying LACP Timeout
- Specifying the Maximum Active Links
- Specifying the Minimum Active Links
- Specifying Load Balance Mode

Enabling/Disabling LACP

LACP can be enabled on the aggregate interfaces (aggregate sub-interface, aggregate virtual forward interface do not support LACP). To enable/disable LACP, in the aggregate interface configuration mode, use the following commands:

- Enable: **lacp enable**
- Disable: **no lacp enable**

Specifying LACP System Priority

LACP system priority is used to determine the priority between devices in both sides. The interface with higher LACP system priority will be defined as the standard selected interface. The smaller the number is, the higher the priority will be. If both sides have the same LACP system priority, the system will choose the interface with smaller MAC address to be the standard selected interface.

To configure the LACP system priority, in the aggregate interface configuration mode, use the following command:

lacp system-priority *value*

- *value* – Specifies the LACP system priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default LACP system priority, in the aggregate interface configuration mode, use the following command:

no lacp system-priority

Specifying Interface LACP Priority

Interface LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.

To configure the interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

lacp port-priority *value*

- *value* – Specifies the interface LACP priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

no lacp port-priority

Specifying LACP Timeout

The LACP timeout refers to the time interval for the members waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. The system supports short timeout (1 second) and long timeout (30 seconds, the default value).

To specify the LACP timeout for the member interface, in the configuration mode of the interface in the aggregate group, use the following command:

lacp period-short

To restore to long timeout, in the configuration mode of the interface in the aggregate group, use the following command:

no lacp period-short

Specifying the Maximum Active Links

The number of maximum active link refers to the maximum Active interface number. When the Active interface number reaches the maximum number, status of other legal interfaces will become Standby. For instance, there are 4 Active interfaces in the aggregate group. If the maximum active links is specified to 2, system will choose two interfaces as the Active interfaces according to the priority, and the status of the other two interfaces with lower priority will become Standby. When the Active interface down causes the link down, system will switch the status of the Standby interface to Active, thus the LACP works as the redundant way.

To specify the maximum active links, in the aggregate interface configuration mode, use the following command:

lacp max-bundle *number*

- *number* – Specifies the number of the maximum active links. The value range is 1 to 16. The default value is 16.

To restore to the default maximum active link number, in the aggregate interface configuration mode, use the following command:

no lacp max-bundle

Specifying the Minimum Active Links

The number of minimum active link refers to the minimum Active interface number. When the number of Active interface is less than the minimum active link number in the aggregate group, status of all the legal interfaces in the aggregate group will become Standby. The minimum active links must be less than the maximum active links.

To specify the minimum active links, in the aggregate interface configuration mode, use the following command:

lacp min-bundle *number*

- *number* – Specifies the number of the minimum active links. The value range is 1 to 8. The default value is 1.

To restore to the default minimum active link number, in the aggregate interface configuration mode, use the following command:

no lacp min-bundle

Specifying the Load Balance Mode

You can specify the load balance mode for the aggregate group. System supports flow-based load balance and 7-tuple based load balance. When the members of the aggregate group is Layer-2 interfaces, the system can only support the load balance mode based on the source MAC address and destination MAC address. For instance, if the source IP is specified to be the load balance condition, all the packets with the same source IP will be forwarded by the same interface in the aggregate group. When the physical interfaces in the aggregation interface belong to different modules, the system supports the forwarding from the interface of the module where the packet is sent.

To specify the load balance mode, in the aggregate interface configuration mode, use the following command:

load-balance mode {flow | tuple {dest-ip dest-mac dest-port protocol src-ip src-mac src-port} | adjacency-port}

- **flow** – Gets the load balance mode from the traffic. It is the default mode.
- **tuple** [**dest-ip dest-mac dest-port protocol src-ip src-mac src-port**] – Uses tuples as the load balance condition. It can be one of the 5 tuples or the combination of the tuples.
- **adjacency-port** – Specify the load balance mode as forwarding from the interface of the module where the packet is sent. Only some devices (X series devices, K9180, K20803) are supported.

To restore to the default load balance mode, in the aggregate interface configuration mode, use the following command:

no load-balance

Viewing Aggregate Group Information

You can view the LACP aggregate information in any CLI mode. To view the aggregate group information, use the following command:

show lacp *aggregate-name*

- *aggregate-name* – Specifies the name of the aggregate group you want to view.

Bypassing the Device

Some of Hillstone models are designed with bypass functionality. To reduce the risk of single point of failure, bypassing the device can ensure network continuity during device reboot, power failure or other malfunctions. When a bypass module is working, the networks accessed to the security device are physically connected by the bypass module.



Notes:

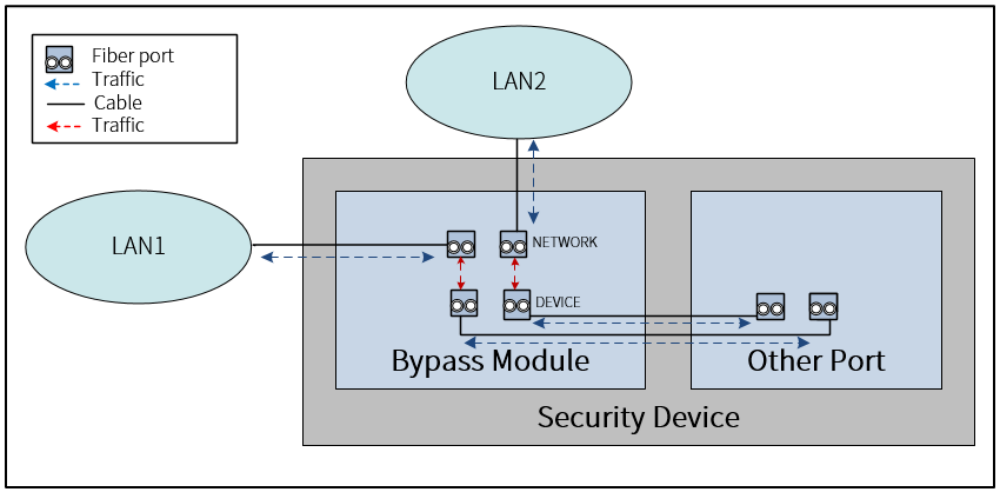
- Not all Hillstone platforms support bypass functionality.

Network Layout with Bypass Module

Bypass is classified into two types: the device interface support the Bypass function, and the Bypass extension module.

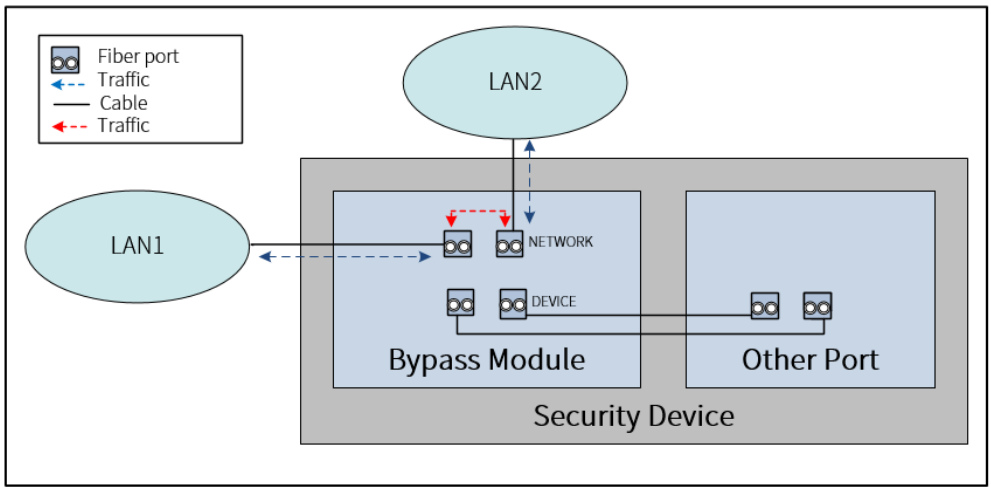
- If the device interface supports the Bypass function, you only need to connect two inter-connected Lans (such as LAN1 and LAN2) to one Bypass interface pair. For example, eth0/2 and eth0/3 are Bypass interface pairs. You only need to connect eth0/2 and eth0/3 to LAN1 and LAN2 respectively.

- For the Bypass extension module, install it into the expansion slot of the device according to the installation manual. Then connect the two ports marked with NETWORK on the panel to different LANs (as shown in Figure LAN1 and LAN2). Connect the two ports marked with DEVICE on the panel to other ports on the device. For details, see the following figure. Solid black lines indicate cable connection. ((As follows, take the IOC-A-2MM-BE/2SM-BE Bypass extension as an example)



However, in particular situations like power failure or device rebooting, the device is

bypassed and LAN1 and LAN2 are physically connected through the bypass module.



Enable / Disable Forced Bypass

Only A , K series firewalls or bypass module IOM-8MM-B-260 (for X 8180) support this functions. When a device fails to forward network traffic normally in a certain state (such as system restart, abnormal operation, device power off), the system will enter the Bypass state. In the Bypass state, the interface pairs (for example, eth0/0 and eth0/1 are Bypass interface pair 0 defaultly, which is identified in the front panel.) are physically directly connected like a cable, and traffic flows directly through them. Bypass interface pairs do not connect when the device is in normal operation, but forward traffic normally according to the functions configured by the interface.

Example for bypass interface pairs: E0/0 and E0/1 are Bypass interface pair 0 defaultly, which is identified in the front panel. The IOM-8MM-B-260 module has 16 optical ports which can group four Bypass pairs, including pair0 (port 0' and port 1'), pair1 (port 2' and port 3'), pair2 (port 4' and port 5') and pair3 (port 6' and port 7').

If you need to enable the forced Bypass function of the interface when the device is running normally, and system can enter the Bypass interface pair mode by using the following commands:

bypass slot *slot-id* **pair** *pair-id*

To enable the forced Bypassed function, use the following commands:

force-bypass

To disable the forced Bypassed function, use the following commands:

no force-bypass.



Notes:

- You can not enable the forced bypass function and HA function at the same time.
- When device restart and system configuration information not be loaded completely , the device is in Bypass mode and Bypass interface pairs may still forward traffic to each other like a cable .

Monitor the Status of Ports

The IOM-8MM-B-260 module has four Bypass pairs which can monitor the interfaces on other expansion modules separately. For example, port0 is connected to "interface1" on another expansion module and port1 is connected to "interface2" on the module. Port0 and port1 will be connected directly when system monitors "interface1" or "interface2" cannot work normally, which means the firewall is bypassed.

1. In the global configuration mode, use the following command to enter the Bypass interface pair mode:

   bypass slot *slot-id* **pair** *pair-id*

2. In the Bypass interface pair mode, use the following command to enable or disable the monitor function:

   - **monitor** *interface1 interface2* - Disable this function.
   - **no monitor** - Enable this function.

Address

Overview

In StoneOS, IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, StoneOS supports address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only reference the name during configuration. Address book is the database in StoneOS that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

Address Entry

StoneOS provides a global address book. You need to specify an address entry for the global address book. In an address entry, you can replace the IP range with a DNS name. You can use them for NAT conveniently. Furthermore, an address entry also has the following features:

- All address books contain a default address entry named Any. The IP address of Any is 0.0.0.0/0, i.e., any IP address. Any can neither be edited nor deleted.
- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, StoneOS will update other modules that reference the address entry automatically.

Configuring an Address Book

You can perform the following operations on an address book through CLI:

- Global configuration of address book
- Adding or deleting an address entry
- Specifying the IP range of an address entry
- Specifying the excluding address entries

- Specifying the IP address of an ordered address entry
- Moving a member of the ordered address entry
- Renaming an address entry
- Viewing the reference address of an address entry
- Viewing the address book information

Global Configuration of Address Book

The global configuration of the address book is used to enable or disable the ordered address book function. In the ordered address book, the address members can be stored in the configured sequence of IP addresses. In some specific business scenarios, when there are multiple IP addresses that need to be NATed, the administrator requires a one-to-one mapping of IP addresses, traditionally achieved by creating multiple NAT rules and individually translate each IP address. To enhance the O&M efficiency, you can directly reference the ordered address book in NAT rules, allowing multiple IP addresses within a single NAT rule to be translated one-to-one based on the specified order of IP address. Referencing the ordered address book in NAT rules not only improves the execution efficiency and accuracy of NAT rules but also enables you to modify a single NAT rule when changing the business, reducing maintenance complexity.

Entering the Global Configuration Mode of Address Book

Before you enable or disable the Ordered Address Book function, you need to enter the global configuration mode of address book:

To enter the global configuration mode of address book, in global configuration mode, use the following command:

address-global

Enabling/Disabling Ordered Address Book Function

Before you configure an ordered address book entry, you need to enable the ordered address book function. By default, this function is disabled.

To enable or disable the Ordered Address Book function, in global configuration mode of address book, use the following command:

- Enable: **ordered**
- Disable: **no ordered**



Notes: When the configuration of ordered address book exists in the system, you cannot disable the Ordered Address Book function. To disable this function, use the **no address** *address-entry* command to delete the ordered address book configured in the system first.

Adding or Deleting an Address Entry

To add an address entry to the address book and enter the address configuration mode, in the global configuration mode, use the following command:

address *address-entry* [**ipv6**] [**ordered**]

- *address-entry* - Specifies the name of the address entry that will be added.
- **ipv6** - Specifies the address entry as the type of IPv6. If not specified ,it will be the type of IPv4.
- **ordered** - Specifies the address entry as the ordered address entry. Note: To specify the **ordered** keyword, enable the Ordered Address Book function.

To delete the specified address entry from the address book, in the global configuration mode, use the following command:

no address *address-entry*



Notes: The address entry being referenced by other modules or address entries can not be deleted. To delete it, remove the reference first.

Specifying the IP Range of an Address Entry

In StoneOS, the IP range of an address entry is the collection of all the IP members within the range. The members of the address entry consist of the following types:

- IP address: includes two types. One is IPv4 address/subnet mask or IPv6 address/subnet mask, such as 10.100.2.0/24 or 2001::1/64; the other is IPv4 address with a wildcard mask or IPv6 address with a wildcard mask, such as 192.168.0.1 255.255.0.255 or 2001::10 FF00::FFFF.
- Host name, such as host1.hillstonenet.com. Support the host name which contains the wildcard, such as *.baidu.com.
- IP range, such as 10.100.2.3 - 10.100.2.100 or 2001::1 - 2001::10.
- Country or region: A set of IP addresses that belong to a country or a region.
- Other address entries

To add an IP member to the specified address entry, or delete the specified member from the address entry, in the address configuration mode, use the commands with the keywords **ip** or **wildcard**.



Notes: When you add an IP wildcard address member, using the command with the keyword **ip** has some limits. We recommend that you use the command with the keyword **wildcard**.

To add/delete an IP address member of IPv4 address/subnet mask or IPv4 address with a wildcard mask, use the following commands:

- **ip** {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*} [**description***description-text*]
  - *ip-address* – Specifies the IP address of the IP member.
  - *netmask* / *wildcardmask* – Specifies the subnet mask/wildcard mask. StoneOS does not support the wildcard mask which has more than 8 zeros (consecutive or non-consecutive) before the first 1 from the right side of its binary form. For example, 255.0.0.255 is an invalid wildcard mask, while 255.0.255.0 and 255.32.255.0 are valid wildcard masks.
  - *ip/netmask* – Specifies the IP and netmask of the IP member.
  - *description-text* – Add a description for the specified address member.
- **no ip** {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*}

  Note: After you add a description for the specified address member, you can use the **ip** {*ip-address* {*netmask* | *wildcardmask*} | *ip/netmask*} command to delete this description.
- **wildcard***ip-addresswildcardmask* [**description***description-text*]
  - *ip-addresswildcardmask* – Specifies the IPv4 address (*ip-address*) and wildcard mask (*wildcardmask*) of the IP member.

    Wildcard mask: When a wildcard mask is converted to binary, the bits set to '1' indicate the IP address bits that need to be matched, while the bits set to '0' indicate those that can be ignored. Take the wildcard "192.168.0.1 255.255.0.255" as an example, in which "255.255.0.255" is the wildcard mask. The binary form of 255.255.0.255 is 11111111 11111111 00000000 11111111, which matches IP addresses in the form '192.168.*.1'. Using a wildcard mask to configure an IP address allows you to cover multiple network segments with a single configuration. For example, when configuring the IP address as "192.168.15.0 255.255.15.0", it includes multiple network segments such as 192.168.15.0/24, 192.168.31.0/24, and 192.168.47.0/24.
  - *description-text* – Add a description for the specified address member.

- **no wildcard***ip-addresswildcardmask*

  Note: After you add a description for the specified address member, you can use the **wildcard***ip-addresswildcardmask* command to delete this description.

To add/delete an IP address member of IPv6 address/subnet mask or IPv6 address with a wildcard mask, use the following commands:

- **ip***ipv6-prefix/prefix-length* [**description***description-text*]

  - *ipv6-prefix/prefix-length* – Specifies the IPv6 address prefix and prefix length of the IP member. The value range of the prefix length is 0 to 128.

  - *description-text* – Add a description for the specified address member.

- **no ip***ipv6-prefix/prefix-length*

  Note: After you add a description for the specified address member, you can use the **ip***ipv6-prefix/prefix-length* command to delete this description.

- **wildcard***ipv6-addresswildcardmask* [**description***description-text*]

  - *ipv6-addresswildcardmask* - Specifies the IPv6 address (*ipv6-address*) and wildcard mask (*wildcardmask*) of the IP member. The 128bit wildcard mask must consist of consecutive 8 (or integer multiples of 8) zeros or consecutive 8 (or integer multiples of 8) 1s, such as FF00::FFFF.

  - *description-text* – Add a description for the specified address member.

- **no wildcard***ipv6-addresswildcardmask*

  Note: After you add a description for the specified address member, you can use the **wildcard***ipv6-addresswildcardmask* command to delete this description.

To add a host member to an address entry or delete the specified member, in the address configuration mode, use the following commands:

- **host***host-name*[**vrouter***vrouter-name*] [**description***description-text*]
  - *host-name* – Specifies the host name. Support the host name which contains the wild-card. You can specify up to 255 characters.
  - *vrouter-name* -Specifies the VRouter of the host.
  - *description-text* – Add a description for the specified address member.
- **no host***host-name* [**vrouter***vrouter-name*]

  Note: After you add a VRouter of the host and a description for the specified address member, you can use the **host***host-name*[**vrouter***vrouter-name*] command to delete the description, and use the **host***host-name* command to delete both the VRouter and description.

To add an IP range member to an address entry, or delete the specified member from the address entry, in the address configuration mode, use the following commands:

- **range***min-ip*[*max-ip*][**description** *description-text*]
- **no range***min-ip*[*max-ip*]

  Note: After you add a description for the specified address member, you can use the **range***min-ip*[*max-ip* command to delete this description.

To add a set of IP addresses that belong to a country or a region, in the address configuration mode, use the country command. To delete this member from the address entry, use the no form of this command.

- **country** *country-name* [**province***province-name* [**city***city-name*]] [**description***description-text*]
  - *country-name* - Optional. You can press the **Tab** key after the country keyword to see the available values of the country-name parameter.
  - **province***province-name* - Specifies the province that will be added to the address entry. This parameter is available only when the country-name parameter is set to CN. You

can press the **Tab** key after the province keyword to see the available values of the province-name parameter. **Note**: This parameter is not available in the version controlled by the license outside China.

- **city***city-name* - Specifies the city that will be added to the address entry. This parameter is available only when the country-name parameter is set to CN and the configured province contains corresponding cities. You can press the **Tab** key after the city keyword to see the available values of the city-name parameter. **Note**: This parameter is not available in the version controlled by the license outside China.
- *description-text* – Add a description for the specified address member.

- **no country***country-name* [**province***province-name* [**city***city-name*]]

  Note: After you add a description for the specified address member, you can use the**country** *country-name* [**province***province-name* [**city***city-name*]] command to delete this description.

To add another address entry to an address entry, or delete the specified address entry from the address entry, in the address configuration mode, use the following commands:

- **member** *address-entry* [**description***description-text*]
  - *address-entry* - Specifies the name of the address entry that will be added.
  - *description-text* - Add a description for the specified address member.
- **no member***address-entry*

  Note: After you add a description for the specified address member, you can use the **member** *address-entry* command to delete this description.

Notes:

- The country or region member is supported in the address entry of the IPv4 type.
- Only the security policy, policy-based route, and PTF dynamic IP blacklist support the address entry with the country or region member added.
- The address entry with the country or region member added does not support the exclude range min-ip max-ip settings in Excluding Address Entries.
- In the IP geography database supported by StoneOS 5.5R10F2 and later F versions, StoneOS 5.5R11 and later, the territorial information of IP addresses within China is annotated at the provincial and city levels. In addition, Hong Kong S.A.R. (China), Macao S.A.R. (China), and Taiwan (China) are adjusted to provinces of China. After you upgrade the device system (authorized by the license outside China) to a version above, the existing address book configurations of Hong Kong S.A.R. (China), Macao S.A.R. (China), and Taiwan (China) are automatically deleted.
- In a device, you can use wildcard for up to 128 host members.
- A maximum of 8 address members of the IPv4 address with a wildcard mask type or the IPv6 address with a wildcard mask type are allowed to be configured in each address book entry.
- Only the security policy and the IPv6 address book support the address entry with the IPv6/Wildcard member added.

Excluding Address Entries

Both IPv4 and IPv6 address entries are supported in address books. By configuring the excluded entries, you can rule out IPv4 or IPv6 addresses from an address book. The types of address

entries that can be excluded are the following two types:

- IP address: IPv4 type: both IP/netmask (e.g. 10.100.2.0/24) and IP/wildcard netmask (192.168.0.1 255.255.0.255) can be excluded; IPv6 type, like 2001::1/64, is also supported.
- IP range: a range of IP addresses, e.g. 10.100.2.3 – 10.100.2.100 or 2002::0-2002::10.



Notes: The maximum percentage of excluded members is 10% of the total number in this address book.

Exlcuding an IPv4 Address Entry

To exclude an IPv4 address entry, under address book configuration mode, use the following command:

exclude ip*ip-address* {*netmask* | *wildcardmask*}[**description** *description-text*]

- *ip-address* – Specifies the IP address to be excluded.
- *netmask* / *wildcardmask* – Specifies the netmask or wildcard mask. Wildcard netmask is to signify a sequence of less than 8 wildcard characters (i.e. less than eight zeros) in a binary netmask (the last binary number of the netmask must be 1, not 0). For example, 255.0.0.255 is not supported in this wildcard netmask format; 255.0.255.0 and 255.32.255.0 are legitimate.
- *description-text* – Add a description for the specified address member.

To resume an IPv4 address entry, use the **no exclude ip***ip-address* {*netmask* | *wildcardmask*} command.

Note: After you add a description for the specified address member, you can use the **exclude ip***ip-address* {*netmask* | *wildcardmask*} command to delete this description.

To exclude an IP range address entry, under address book configuration mode, use the following command:

exclude range*min-ip max-ip*[**description** *description-text*]

- *min-ip max-ip* – Specifies the start and end IP addresses.
- *description-text* – Add a description for the specified address member.

To resume an exclude address range, use the **no exclude range***min-ip max-ip* command.

Note: After you add a description for the specified address member, you can use the**exclude range***min-ip max-ip*command to delete this description.

Excluding IPv6 Address Entries

To exclude IPv6 address entries from an address book, under this address book's configuration mode, use the following command:

exclude ip*ipv6-prefix/prefix-length*[**description** *description-text*]

- *ipv6-prefix / prefix-length* – Specifies the IPv6 prefix and its length. The range is 65 to 128.
- *description-text* – Add a description for the specified address member.

To resume an excluded IPv6 address entry, use the **no exclude ip***ipv6-prefix / prefix-length* command.

Note: After you add a description for the address member, you can use the**exclude ip***ipv6-prefix/prefix-length*command to delete this description.

To exclude IPv6 range address entry from an address book, under address book configuration mode, use the following command:

exclude range*min-ipv6-addressmax-ipv6-address*[**description** *description-text*]

- *min-ipv6-address* – Specifies the start IPv6 address.
- *max-ipv6-address* – Specifies the end IPv6 address.
- *description-text* – Add a description for the specified address member.

To resume an excluded IP range back to address book, use the **no exclude range***min-ipv6-address max-ipv6-address* command.

Note: After you add a description for the address member, you can use the **exclude range***min-ipv6-addressmax-ipv6-address* command to delete this description.

Specifying the IP Address of an Ordered Address Entry

When you configure an ordered address entry, you need to specify the IP address contained in the ordered address entry. You can repeatedly use the following command to specify multiple IP addresses. These IP addresses will be saved based on the configuration sequence.

To specify the IP address of the ordered address entry, in address configuration mode, use the following command:

ip {*ip_address* | *ipv6_address*} [**description***description*]

- *ip_address* - Specifies the IPv4 address of the ordered address entry.
- *ipv6_address* - Specifies the IPv6 address of the ordered address entry.
- **description***description* - Specifies the description for the ordered address entry.

Moving a Member of the Ordered Address Entry

To move a member of the ordered address entry, in address configuration mode, use the following command:

move ip *ip_address* {**bottom** | **to** *number* | **top**}

- *ip_address* - Specifies the IP address of the member that you want to move, including IPv4 address and IPv6 address.
- **bottom** - Move the member to the bottom of the list.
- **to** *number* - Move the member to the specified row of the member list. Valid values: 1 to 3000. For example, if you sets the row number to 2, the member will be moved to the second row of the member list.
- **top** - Move the member to the top of the list.

Renaming an Address Entry

To rename an existing address entry, in the address configuration mode, use the following command:

rename *name*

- *name* - Specifies the new name for the address entry. If the name is repeated with an existing one, the command will void.

Viewing the Reference Address of an Address Entry

In StoneOS, an address entry can be referenced by other modules, such as policy rules, NAT rules or session limit rules. To view the reference of an address entry by other modules, i.e., the reference address of the address entry, in any mode, use the following command:

show reference address *address-entry*

- *address-entry* - Shows the reference address of the specified address entry.

Example:

```
hostname(config)# show reference address 10.101.0.194
==========================================================
Name: | 10.101.0.194  (name of the address entry)
----------------------------------------------------
Address: | -  (referenced by other address entries)
----------------------------------------------------
Policy rule: | policy 20 src-addr (referenced by policy rules)
----------------------------------------------------
SNAT rule: | - (referenced by SNAT rules)
----------------------------------------------------
```

```
DNAT rule: | - (referenced by DNAT rules)
-------------------------------------------------
Statistics: | - (referenced by stat-sets)
-------------------------------------------------
Session limit: | rule 1  (referenced by session limit rules)
-------------------------------------------------
PBR: | -  (referenced by PBR rules)
-------------------------------------------------
QoS: | - (referenced by QoS rules)
-------------------------------------------------
ExStats: | - (referenced by extended stat-sets)
-------------------------------------------------
Share Access: | -  (referenced by Share Access)
-------------------------------------------------
LanAddress: | -  (referenced by LAN Address)
-------------------------------------------------
SSO Monitor: | -  (referenced by SSO Monitor)
-------------------------------------------------
SSO Web: | -  (referenced by SSO Web)
-------------------------------------------------
SSO AC: | -  (referenced by Agile Controller)
=================================================-
=
```

Viewing the Address Book Details

To view the details of the global address book, including the entries of the address book, number of the members, and detailed information of the members, and the address entries that are not

referenced by other function modules, in any mode, use the following command:

show address [**filter-ip** *A.B.C.D* [**filter-unreferenced**][**filter-ordered** | **filter-unordered**]| **filter-ordered** | **filter-unordered**] |**name** *address-entry* | **filter-ordered** | **filter-unordered** | | [**filter-unreferenced**][**filter-ordered** | **filter-unordered**]]

- **show address** - Shows the information of all the address entries in the address book.
- **filter-ip** *A.B.C.D* - Shows the information of address entries that contain the specified IP address.
- **name** *address-entry* - Shows the information of specified address entry.
- **filter-unreferenced** - Shows the information of the address entries that are not referenced by other function modules.
- **filter-ordered** - Shows the information of ordered address entries of the ordered address book.
- **filter-unordered** - Shows the information of the other address entries excluding the ordered address book.

To check where the IP address is from, in any mode, use the following command:

show country ip *A.B.C.D*

- *A.B.C.D* – Enter the IP address to check which country or region this IP address belongs to.

You can use the following command to view the geographic location of the specified IP address in any mode:

show geoip-info*A.B.C.D* [**dp**]

- *A.B.C.D* - Enter the IP address whose geographic location you want to view.
- **dp** - View the geographic location of the IP address cached at the data-plane (DP) level.

Address Book Configuration Example

Configuration Example 1

The goal is to create address entries named address1 and address2 for the address book; add the following members to address1: 10.200.1.0/16, 192.168.1.0/24, 192.168.0.1/255.255.0.255 and hillstonenet.com; add the following members to address2: 10.100.3.1 to 10.100.3.10 and address1. Use the following commands:

```
hostname(config)# address address1
hostname(config-addr)# ip 10.200.1.0/16
hostname(config-addr)# ip 192.168.1.0 255.255.255.0
hostname(config-addr)# ip 192.168.0.1 255.255.0.255
hostname(config-addr)# host hillstonenet.com
hostname(config-addr)# exit
hostname(config)# address address2
hostname(config-addr)# range 10.100.3.1 10.100.3.10
hostname(config-addr)# member address1
hostname(config-addr)# exit
hostname(config)#
```

Configuration Example 2

Users can configure the host name which contains the wildcard in address book. To specify a host name as *.baidu.com, use the following commands:

```
hostname(config)# addr baidu
hostname(config-addr)# host *.baidu.com
```

Custom IP Geolocation

IP geolocation indicates geographical location of IP address, such as the country or region where the IP address resides. The IP geolocation database of the system provides the mapping between IP addresses and their geolocations. In addition, the system supports the custom IP geolocation function. You can customize the geographical location of IP addresses. For example, when the geographical location of the IP address is invalid, you can customize this information.



Notes:

- You can configure custom IP geolocation for only public IPv4 address.
- When you query the geographical location of IP addresses, the system preferentially queries the custom geographical location.

Configuring Custom IP Geolocation

To configure custom IP geolocation, in global configuration mode, use the following command:

user-ip-geolocation [**id** *id*] **start-ip** *ip-address* [**end-ip** *ip-address*] **country** *country-name* [**province** *province-name* [**city** *city-name*]]

- **id** *id* - Specifies the ID of custom IP geolocation. Valid values: 1 to 256. If the ID is not specified, the system automatically assigns an ID to the configured custom IP geolocation.
- **start-ip** *ip-address* [**end-ip** *ip-address*] - Specifies the start IP address (**start-ip***ip-address*) and end IP address (**end-ip** *ip-address*) of the IP address of custom geolocation. If no end IP address is specified, it indicates that the IP address of custom geolocation is a single IP address.
- **country** *country-name* - Specifies the country/region where the IP address resides. You can use the TAB key next to the **country** keyword to view the countries/regions that can be selected.

- **province** *province-name* - Specifies the province where the IP address resides. This option is available only when the country/region is set to CN. **Note**: This option is not available for devices of the overseas version.
- **city** *city-name* - Specifies the city where the IP address resides. This option is available only when the country/region is set to CN and the configured province contains corresponding cities. You can use the TAB key next to the **city** keyword to view the cities that can be selected. **Note**: This option is not available for devices of the overseas version.

In global configuration mode, use the **no user-ip-geolocation id** *id* command to cancel the configuration of custom IP geolocation.



Notes: You can configure up to 256 custom IP geolocation entries in the system.

Viewing Custom IP Geolocation

In any mode, you can use the following command to view the configured custom IP geolocation, including the ID, start IP address, end IP address, the country/region, province, and city where the IP address resides, and whether the information is redundant. "*" indicates that the information is redundant. In other words, the custom IP geolocation is consistent with the geolocation of the IP address in the IP geolocation database.

show user-ip-geolocation

Service and Application

This chapter introduces the following topics:

- Service
- Application

Service Overview

Service is information stream designed with protocol standards. Service has some specific features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple StoneOS modules including policy rules, NAT rules, etc. StoneOS ships with over 100 predefined services and over 10 service groups. Besides, you can also customize user-defined services and service groups as needed. All these services and service groups are stored in and managed by StoneOS service book. Each service in the service book contains its specific service entry.

Viewing Service or Service Group Information via CLI

To view service information, in any mode, including the service type, name, protocol, destination port, source port, and the service entries that are not referenced by other function modules, in any mode, use the following command:

show service [[**predefined** | **userdefined** | **name** *service-name* [unreferenced] | **unreferenced**]

- **predefined** – Shows the predefined service information.
- **userdefined** – Shows the user-defined service information.
- **name** *service-name* - Shows the information of the specified service.
- **unreferenced** - Shows the information of the service entries that are not referenced by other function modules.

show service protocol {**tcp** | **udp**} [**dst-port** {*port-number* | **range** *min-port max-port*}] [**src-port** {*port-number* | **range** *min-port max-port*}]

- **tcp** | **udp** – Shows the service information with the protocol type of TCP or UDP.
- **dst-port** {*port-number* | **range** *min-port max-port*} – Shows the service information of the specified destination port. *port-number*is a single destination port number. If the destination port number is in a range, *min-port* is the minimum destination port number, *max-port* is the maximum destination port number, and the range is 0 to 65535.
- **src-port** {*port-number* | **range** *min-port max-port*}- Shows the service information of the specified source port. *port-number*is a single source port number. If the source port number is in a range, *min-port* is the minimum source port number, *max-port* is the maximum source port number, and the range is 0 to 65535.

show service protocol {**icmp** | **icmpv6**} [**type** *type-number* [**code** {*code-number* | **range** *min-code max-code*}]]

- **icmp** | **icmpv6** – Shows the service information with the protocol type of ICMP or ICMPv6.
- **type** *type-number* – Shows the service information with the specified ICMP type or ICMPv6 type.
- [**code** {*code-number* | **range** *min-code max-code*}] - Shows the service information of the policy rule with the specified ICMP code or ICMPv6 code. *code-number*is a single code. If the code is in a range, *min-code*is the minimum code, *max- code*is the maximum code. The code value of ICMP Protocol type ranges from 0 to 15, and that of ICMPv6 protocol type ranges from 0 to 255.

show service protocol *protocol-number*

- *protocol-number* – Shows the service information with the specified protocol number. The protocol number is from 1 to 255.

To view service group information, including predefined service groups, user-defined service groups, and the service group entries that are not referenced by other function modules, in any mode, use the following command:

show servgroup [**predefined**] | [**userdefined**] | [**name** *servicegroup-name*] | [**unreferenced**]

- **predefined** - Shows the predefined service group information.
- **userdefined** - Shows the user-defined service group information.
- **name** *servicegroup-name* - Shows the information of the specified service group.
- **unreferenced** - Shows the information of the service group entries that are not referenced by other function modules.

Viewing Service Information That Contains Specified Keywords

A service contains information such as protocol type and port number. You can filter service by service content such as name, protocol type, and port number with a fuzzy search.

To view service information that contains specified keywords, in any mode, use the following command:

show service [**predefined** | **userdefined**] **keyword***string*

- **predefined** – Shows the predefined service information.
- **userdefined** – Shows the user-defined service information.
- *string* – Specifies the keyword, which needs to be 1 to 95 characters in length.

Viewing Service References

In StoneOS, a service can be referenced by other modules, such as policy rules, NAT rules or session limit rules. To view the reference of a service or service group by other modules, i.e., the service or service group address, in any mode, use the following command:

show reference service *service-name*

- *service-name* – Shows the reference of the specified service or service group.

Example:

```
hostname(config)# show reference service ftp
==========================================================
==
Name: | ftp   (name of the service or service group)
----------------------------------------------------
Service group: | SRV_INTERNET_PROTOCOL (reference by other service
groups)
----------------------------------------------------
Policy rule: | policy 105 , policy 100   (reference by policy rules)
----------------------------------------------------
DNAT rule: | - (reference by DNAT rules)
----------------------------------------------------
SNAT rule: | -   (reference by SNAT rules)
----------------------------------------------------
Statistics: | -    (reference by stat-sets)
----------------------------------------------------
Policy route: | - (reference by PBR rules)
----------------------------------------------------
iQoS map: | - (reference by iQoS map)
----------------------------------------------------
iQoS white-map: | - (reference by iQoS white-map)
==========================================================
=
```

Predefined Services

StoneOS provides more than 100 predefined services. To view all the predefined services supported by the current version, use the above **show** command or WebUI.

The following section describes several common predefined services.

RSH

RSH ALG (Remote Shell) allows authenticated users to run shell command on the remote host. Hillstone device supports RSH services of transparent mode, NAT mode and router mode.

Sun RPC

Sun RPC (Sun Remote Procedure Call) allows the program running on a host to call the programs running on other hosts. Because of the large number of RPC services and the requirement for broadcasting, RPC services' transmission addresses are dynamically negotiated based on the number and version of the services. You can define some binding protocols to map the number of RPC programs and service versions to the transmission addresses.

Hillstone devices support a predefined Sun RPC service for users to permit or deny traffic according to policies configured. You can define a policy rule to permit or deny all the RPC requests. For example, if you need to use the network file system (NFS), then configure a policy rule that allows Sun RPC services.

MS RPC

Microsoft Remote Procedure Call (MS RPC) is the RPC implementation of the Microsoft distributed computing environment. MS RPC allows the program running on a host to call programs running on other hosts. Because of the large number of RPC services and the requirement for broadcasting, RPC services' transmission addresses are dynamically negotiated based on the UUID (Universal Unique Identifier) of the server.

Hillstone devices support a predefined MS RPC service for users to permit or deny traffic according to policies configured. You can define a policy rule to permit or deny all the RPC requests. For example, if you need to use the Outlook/Exchange or MSqueue service, configure a policy rule that allows MS RPC services.

Predefined Service Group

The predefined service group includes some associated predefined services to facilitate users' configuration. StoneOS provides more than 10 predefined service groups. The service group that contains dynamically identified predefined services is known as a dynamically identified predefined service group, and such a service group needs to be configured individually. When the dynamically identified predefined services are updated by the signature database, the corresponding dynamically identified predefined service group will also be updated. You can view and use the predefined service groups, but cannot edit or delete them.

To view the predefined service group, in any mode, use the following command:

show servgroup predefined

User-defined Service

Besides the above predefined services, you can also create your own user-defined services. The parameters that you can specify for the user-defined service entries are:

- Name
- Protocol type
- The source and destination port for TCP or UDP service, type and code value for ICMP service.
- Timeout

Creating/Deleting a User-defined Service

To create a service and add it to the service book via CLI, or to delete the specified service, in the global configuration mode, use the following commands:

service *service-name*

no service *service-name*

- *service-name* – Specifies the name of the user-defined service. The length is 1 to 95 characters. The name must be unique in the entire system. After executing the command, the CLI will enter the configuration mode of created service.

If you need to enable the long connection, in the global mode, use the *longlife-sess-percent* command to configure the percent of long connection. The default value is 0.

Adding/Deleting a User-defined Service Entry

The command that is used to add a service entry may vary from different protocol types of the service entries.

To add a service entry of TCP or UDP type, in the service configuration mode, use the following command:

{**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]] [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- **dst-port** *min-port* [*max-port*] – Specifies the destination port number of the user-defined service. If the destination port number is a number range, then *min-port* is the minimum destination port number, and *max-port* is the maximum destination port number. The value range is 0 to 65535, and the destination port number should not be a single 0. For example, the destination port number can be 0 to 20, but cannot only be 0.
- **src-port** *min-port* [*max-port*] – Specifies the source port number of the user-defined service. If the source port number is a number range, then *min-port* is the minimum source port number, and *max-port* is the maximum source port number. The value range is 0 to 65535.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

To add a service entry of ICMP type, in the service configuration mode, use the following command:

icmp type *type-value* [**code** *min-code* [*max-code*]] [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- *type-value* – Specifies the ICMP type value of the user-defined service. The value range is 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information) and any (all the above type values).
- **code** *min-code* [*max-code*] – Specifies the ICMP code value for the user-defined service. The value range is 0 to 5.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

To add a service entry of other types, in the service configuration mode, use the following command:

protocol *protocol-number* [**timeout** *time-out-value* | **timeout-day** *time-out-value*]

- *protocol-number* – Specifies the protocol number of the user-defined service. The value range is 1 to 255.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-day** *time-out-value* – Specify the timeout value of the persistent connection. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the

timeout. You need to set the persistent connection percent before configuring the timeout value of the persistent connection in the global mode.

To delete the specified service entry, use one of the following commands. The service entries can only be deleted but cannot be edited.

- **no** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]
- **no icmp type** *type-value* [**code** *min-code* [*max-code*]]
- **no protocol** *protocol-number*

Renaming a User-defined Service Entry

To rename an existing user-defined service entry, in the service configuration mode, use the following command:

rename *new-name*

- *new-name* – Specifies the new name for the user-defined service entry.

You can also rename the user-defined service entry in the global configuration mode, use the following command:

rename service*old-name new-name*

- *old-name* – Specifies the old name for the user-defined service entry.
- *new-name* – Specifies the new name for the user-defined service entry.

Configuration Example

The goal is to create a user-defined service named my-service, and add the following 3 service entries to my-service:

- A service of TCP type, the destination port is 2121, and the source port is 80.
- A service of ICMP type, the type is 8, the code is 0.
- A service of other types, the protocol number is 47.

Use the following commands:

```
hostname(config)# service my-service
hostname(config-service)# tcp dst-port 2121 src-port 80
hostname(config-service)# icmp type 8 code 0
hostname(config-service)# protocol 47
hostname(config-service)# exit
hostname(config)#
```

Service Group

You can organize some services together to form a service group, and apply the service group to StoneOS policies directly. The service group of StoneOS has the following features:

- Each service of the service book can be used by one or more service groups.
- A service group can contain both predefined services and user-defined services.
- A service group can contain another service group. The service group of StoneOS supports up to 8 layers of nests.

The service group also has the following limitations:

- Service and service group should not use the same name.
- The service group being used by any policy cannot be deleted. To delete such a service group, you must first end its association with other modules.
- If a user-defined service is deleted from the service group, the service will also be deleted from all the service groups using it.

Creating/Deleting a Service Group

To create a service group and add the service group to the service book via CLI, in the global configuration mode, use the following command:

servgroup *servicegroup-name*



Notes: The name of the service group must be unique.

After executing this command, the CLI will enter the service group configuration mode.

To delete a service group, in the global configuration mode, use the following command:

no servgroup *servicegroup-name*

Adding/Deleting a Service/Service Group

The member of the service group can be either a service or a service group. To add a service to the service group or delete a service from the service group, in the service group configuration mode, use the following commands:

service {*service-name* | *servicegroup-name*}

no service {*service-name* | *servicegroup-name*}

When adding a service or service group to the service group, note that:

- Service in the service group must be unique.
- Different devices support different number of members. To view the maximum number of members that the device can have, use the following command: **show capacity stateful-firewall**.
- One service group supports up to 8 layers of nests of another service group.

Adding/Deleting Description to a Service/Server Group

To add description to a service/service group, in the service/service group configuration mode, use the following command:

description *description*

- *description* – Specifies the description of the service/service group.

Use no description to delete the description information.

Renaming a Service Group

To rename an existing service group, in the service group configuration mode, use the following command:

rename*new-name*

- *new-name* – Specifies the new name for the service group.

You can also rename the service group in the global configuration mode, use the following command:

rename servgroup *old-name new-name*

- *old-name* – Specifies the old name for the service group.
- *new-name* – Specifies the new name for the service group.

Application Overview

Application has some specific features, like corresponding protocol, port number, application type, etc. Application is an essential element for the configuration of multiple StoneOS modules including policy rules, NAT rules, application QoS management, etc. StoneOS ships with over 6000 predefined applications and over 60 predefined application groups (when installed with the APP DB license). Besides, you can also customize user-defined application and application groups as needed. All these applications and application groups are stored in and managed by StoneOS application book.

If IPv6 is enabled, IPv6 applications will be recognized by StoneOS.

Predefined Application

StoneOS provides more than 100 predefined applications. You can view all the supported predefined applications by using the **show application predefined** command. On the **Object** > **Application Book** > **Application** page of the WebUI, deprecated predefined applications are marked with a strikethrough, which cannot be edited or deleted. If a deprecated predefined application is referenced by other functional module, an error is returned.

Predefined Application Groups

The predefined application group includes some associated predefined applications to facilitate users' configuration. Upgrading the signature database will dynamically identify the predefined applications. Currently, StoneOS provides more than 60 predefined application groups. You can view and use the predefined application groups, but cannot delete or edit them.



Tip: For more information about upgrading signature database and dynamical identification, see Application Identification.

Userdefined Application

Besides the above predefined applications, you can also create your own user-defined applications. By configuring the customized application signature rules, StoneOS can identify and manage the traffic that crosses into the device, thus identifying the type of the traffic.

Configurations of user-defined application groups include the following items:

- Creating/Deleting the user-defined applications
- Configuring the category/subcategory of user-defined applications
- Configuring the technology used by user-defined applications
- Configuring signatures for user-defined applications
- Creating/Deleting the application signature rules
- Configure the entry of the application signature rule
- Configure the application timeout value
- Modifying the order of the user-defined application signature

Creating/Deleting the User-defined Applications

To create a user-defined application and add this newly-created one to the application book, use the following command in the global configuration mode:

application *application-name*

After executing this command, the system enters the application configuration mode.

To delete the user-defined application, use the following command:

no application *application-name*

Configuring the Category/Subcategory of User-defined Applications

The categories and subcategories of applications are maintained by the application signature database. The category corresponds to the application group of level 1 in the signature database and the subcategory corresponds to the application group of level 2 under level 1. When you configure the category and subcategory of user-defined applications in the CLI, the system lists all supported categories. The following table describes the supported categories and subcategories. If any update occurs, the new table prevails. By default, user-defined applications are not configured with a category.

Category	Subcategory
APP_BUSINESS	APP_BUSINESS_ERP APP_EMAIL APP_BUSINESS_DATABASE APP_INDUSTRY APP_MEDICAL APP_IOT
APP_COMMUNICATION	APP_IM APP_MOBILE_IM APP_VOIP
APP_GAME	APP_PUZZLE_GAME APP_MMO_GAME

Category	Subcategory
	APP_MOBILE_GAME
APP_INTERNET	APP_SPEEDTEST
	APP_REMOTE_DESKTOP
	APP_GENERAL
	APP_P2P
	APP_INTERNET_UTILITY
	APP_MOBILE_INTERNET_UTILITY
	APP_FILE_SHARING
	APP_SOCIAL_NETWORK
	APP_MOBILE_SOCIAL_NETWORK
	APP_PROXY
	APP_SECURITY
	APP_STOCK
	APP_SHOPPING_PLATFORM
	APP_MOBILE_SHOPPING_PLATFORM
	APP_LIVING_SERVICE
	APP_MOBILE_LIVING_SERVICE
	APP_NEWS_READING
	APP_MOBILE_NEWS_READING
	APP_EBANK
APP_MEDIA	APP_VIDEO_SURVEILLANCE
	APP_MULTIMEDIA
	APP_P2P_STREAM
	APP_WEB_VIDEO
	APP_MOBILE_WEB_VIDEO
	APP_ONLINE_MUSIC

Category	Subcategory
	APP_MOBILE_ONLINE_MUSIC
APP_NETWORK	APP_DIRECTORY_SERVICE APP_VPN APP_ROUTING_PROTOCOL APP_NETWORK_MGMT APP_COMMON_PROTOCOL
APP_OTHER_CATEGORY	APP_DATA_TRANSFER APP_ONLINE_INTERACTIVE

To configure the category and subcategory of user-defined applications, use the following command in application configuration mode:

category *category-name* [**subcategory** *sub-category-name*]

- *category-name* - Specifies the category name of applications. Valid values of the category are the application group of level 1 in the application signature database.
- *sub-category-name* - Specifies the subcategory name of applications. Valid values of the subcategory are the application group of level 2 under level 1 specifies by *category-name*.

To delete the category and subcategory configuration of user-defined applications, use the following command in global configuration mode:

no category

Configuring the Technology Used by User-defined Applications

The technologies used by applications are maintained by the application signature database. You can configure one of the following technologies for applications. If any update occurs, the new technologies prevails. By default, user-defined applications are not configured with a technology.

To configure the technology used by user-defined applications, use the following command in application configuration mode:

- **technology browser-based**: Sets the technology used by applications to **browser-based**.
- **technology client-server**: Sets the technology used by applications to **client-server**.
- **technology network-protocol**: Sets the technology used by applications to **network-protocol**.
- **technology peer-to-peer**: Sets the technology used by applications to **peer-to-peer**.

To delete the configuration of technology used by user-defined applications, use the following command in application configuration mode:

no technology

Configuring Signatures for User-defined Applications

The signatures of applications are maintained by the application signature database. You can configure one or more of the following signatures for user-defined applications. If any update occurs, the new signatures prevails. By default, user-defined applications are not configured with a signature.

To configure signatures for user-defined applications, use the following command in application configuration mode:

- **used-by-malware** {**yes** | **no**}: Sets the signature of applications to **used by malware** or **not used by malware**.
- **evasive** {**yes** | **no**}: Sets the signature of applications to **evasive** or **non-evasive**.
- **prone-to-misuse** {**yes** | **no**}: Sets the signature of applications to **prone to misuse** or **not prone to misuse**.
- **excessive-bandwidth** {**yes** | **no**}: Sets the signature of applications to **consume excessive bandwidth** or **not consume excessive bandwidth**.
- **widely-used** {**yes** | **no**}: Sets the signature of applications to **widely used** or **not widely used**.
- **file-transfer** {**yes** | **no**}: Sets the signature of applications to **be able to transfer files** or **not be able to transfer files**.

- **tunnels-other-apps** {**yes** | **no**}: Sets the signature of applications to **be used by other applications** or **not be used by other applications**.
- **known-vulnerabilities** {**yes** | **no**}: Sets the signature of applications to **known vulnerabilities exist** or **no known vulnerabilities exist**.

Viewing the Configuration of User-defined Applications

To view the configuration of a specified user-defined application, use the following command in any mode:

show application userdefined [*application-name*]

- *application-name* - Specifies the name of the user-defined application.

To view the configuration of all user-defined applications, use the following command in any mode:

show application userdefined

Enabling the User-defined Application Signature Configuration Mode

To enable the user-defined application signature configuration mode, use the following command in the global configuration mode:

app-signature

Creating/Deleting the User-defined Application Signature Rule

System supports create an user-defined application signature rule in two configuration mode:

- User-defined application signature configuration mode: Configure all signatures of an user-defined application.
- Application signature rule configuration mode: Configure any signature of an user-defined application.

Configuring Rules in User-defined Application Signature Configuration Mode

In user-defined application signature configuration mode, use the following command:

signature from { *src-addr* | *src-ip* } **to** { *dst-addr* | *dst-ip* } **protocol** {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]] **application** *application-name*

- *src-addr* – Specifies the source addresses of the **address entry** type.
- *src-ip* – Specifies the source addresses of the **member IP** type.
- *dst-addr* – Specifies the source addresses of the **address entry** type.
- *dst-ip* – Specifies the source addresses of the **member IP** type.
- **dst-port** *min-port* [*max-port*] – Specify the destination port number of the user-defined application signature. If the destination port number is within a range, StoneOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.
- **src-port** *min-port* [*max-port*] – Specify the source port number of the user-defined application signature. If the source port number is within a range, StoneOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port*as the maximum port number. The range of source port number is 0 to 66535.
- *application-name* – Specifies the application name of the signature rule.

Configuring Rules in Application Signature Rule Configuration Mode

In the user-defined application signature configuration mode, use the following command to create a user-defined application signature rule and enter the application signature rule configuration mode. If the specified ID already exists, the system will enter the application signature rule configuration mode.

signature id *id*

To delete this user-defined application signature rule, use the following command in the user-defined application configuration mode:

no signature id *id*

Configuring the Entry of the User-defined Application Signature Rule

A user-defined application signature rule can contain multiple signature rule entries. The logical relationship between each entry is **AND**. **AND** represents that StoneOS can identify the traffic type when the traffic satisfies all entries in this user-defined application signature rule.

Configuring the entry of the user-defined application signature rule includes the following sections:

- Source security zone
- Source/destination IP address
- Source/destination port number of applications of TCP type or UDP type; The type value and the code value of applications of ICMP type
- Application name

To specify the source security zone of the signature rule, use the following command in the application signature rule configuration mode:

src-zone *zone-name*

- *zone-name* – Specifies the name of the source security zone.

To specify the source address of the **address entry** type, use the following command in the application signature rule configuration mode:

src-addr *src-addr*

- *src-addr* – Specifies the source addresses of the **address entry** type.

To specify the source address of the **member IP** type, use the following command in the application signature rule configuration mode:

src-ip *src-ip*

- *src-ip* – Specifies the source addresses of the **member IP** type.

To specify the destination address of the **address entry** type, use the following command in the application signature rule configuration mode:

dst-addr *dst-addr*

- *dst-addr* – Specifies the source addresses of the **address entry** type.

To specify the destination address of the **member IP** type, use the following command in the application signature rule configuration mode:

dst-ip *dst-ip*

- *dst-ip* – Specifies the source addresses of the **member IP** type.

For the application signature of TCP type or UDP type, specify the type and corresponding parameters using the following command in the application signature rule configuration mode:

protocol {**tcp** | **udp**} **dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]

- **dst-port** *min-port* [*max-port*] – Specify the destination port number of the user-defined application signature. If the destination port number is within a range, StoneOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.
- **src-port** *min-port* [*max-port*] – Specify the source port number of the user-defined application signature. If the source port number is within a range, StoneOS will identify the value of *min-port* as the minimum port number and identify the value of *max-port* as the maximum port number. The range of source port number is 0 to 66535.

For the application signature of ICMP type, specify the type and corresponding parameters using the following command in the application signature rule configuration mode:

protocol icmp type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – Specifies the value of the ICMP type of the application signature. The options are as follows: 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information), and any (any

represents all above values).

- **code** *min-code* [*max-code*] – Specifies the value of the ICMP code of the application signature. The ICMP code is in the range of 0 to 5. The default value is 0-5.

For the application signature of other types, use the following command in the application signature rule configuration mode:

protocol other-protocol *protocol-number*

- *protocol-number* – Specifies the protocol number of the application signature. The protocol number is in the range of 1 to 255.

To specify the application name of the signature rule, use the following command in the application signature rule configuration mode :

application *application-name*

- *application-name* – Specifies the application name of the signature rule.

To delete the signature rule, use the no form of the above commands. For the existing signature rules, you cannot edit them but can delete them.

Configuring the Application Timeout Value

You can configure the application timeout value. If not, StoneOS will use the default value of the protocol. To configure it, use the following command in the application configuration mode:

timeout {**tcp** | **udp** | **icmp** | **other-protocol**} *timeout-value*

- **tcp** | **udp** | **icmp** | **other-protocol** – Specifies the protocol type.
- *tiemout-value* – Specifies the timeout value of the application. The range is 1 to 65535.

To specify the timeout period in days, use the following command in application configuration mode:

timeout-day {tcp | udp | icmp | other-protocol} timeout-value

- **tcp** | **udp** | **icmp** | **other-protocol** – Specifies the protocol type.
- *tiemout-value* – Specifies the timeout value of the application. The range is 1 to 1000.

Modifying the Order of the User-defined Application Signature Rule

Each user-defined application signature rule has a unique ID. When traffic flows into the device, StoneOS will search the user-defined application signature rule in the order of priority to see which signature rule matches the traffic. Once the traffic satisfies a specific application signature rule, StoneOS will process the traffic according to this matched rule. The order of searching signature rule is not related to the order of the signature ID but the order of priority. To view the order of priority, use the **show app-signature static** command. And then StoneOS will list all application signatures according to the priority. The signature rule with the highest priority will be listed at the top and the signature rule with the lowest priority will be listed at the bottom. When you create a signature rule, you can specify its priority. And you can also modify its priority in the user-defined application signature configuration mode. You can adjust the priority of the signature rule to be at the top or at the bottom or between two signature rules. To modify the priority, use the following command in the user-defined application signature configuration mode:

move *id* {**top** | **bottom** | **before** *id* | **after** *id*}

User-defined Application Group

An application group contains multiple applications. You can apply the application group to the policy. An application group has the following features:

- Each application in the application book can be used in one or more application groups.
- Each application group can contain predefined applications and user-defined applications.
- Each application group can contain one or more application groups. StoneOS supports the nested application group. An application group within an application group can continue referencing one or more application groups. StoneOS can support up to 8-level nested application groups.

An application group also has its restrictions:

- The names of an application group and an application cannot be identical.
- The application group referenced by the policy cannot be deleted. To delete an application group, make sure that no module references this application group.
- When you delete an application from the application book, this application will also be deleted from the application groups that contain this application group.

Creating/Deleting an Application Group

To create an application group and add it to the application book, use the following command in the global configuration mode:

application-group *application-group-name*



Notes: Make sure the application group name is unique in StoneOS.

After executing this command, the system enters the application group configuration mode.

To delete an application group, use the following command in the global configuration mode:

no application-group *application-group-name*

Adding/Deleting an Application or Application Group

An application group can contain applications or application groups. To add an application to an application group, use the following command in the application group configuration mode:

application {*application-name* | *application-group-name*}

Note the following matters when adding an application:

- The application in the application group must be unique.
- Each application group can contain up to 2000 applications and support up to 8-level nested application groups.

To delete an application or application group from an application group, use the following command in the application group configuration mode:

no application { *application-name* | *application-group-name*}

Adding/Deleting a Description for an Application or Application Group

In the application configuration mode or the application group configuration mode, you can use the following command to add the description:

description *description*

- *description* – Specify the description for the application or application group. You can enter up to 255 characters.

In the application configuration mode or the application group configuration mode, use the following command to delete the corresponding description:

no description

Application Identification

A number of functional modules in the system process data stream based on the type of application (to view the mapping relationship between Application IDS and Application names, use the command **show application list**), for example, stat-set and QoS. Therefore, system needs to identify the data stream first, and then implements the statistics and management functions based on the identification result (Application ID) and configuration.

Dynamic Identification

Dynamic identification allows the system to identify an application automatically by its signature. The automatic identification of application is based on the security zone. By default, the automatic identification function of all the security zones is disabled. To enable the dynamic identification function of a security zone, in the security zone configuration mode, use the following command:

application-identify

With dynamic identification enabled, the system will identify all the supported dynamically identified application. To view the identified session information, use the command show session. To disable the dynamic identification functions of a security zone, in the security zone configuration mode, use the following command:

no application-identify

Even if the automatic identification function of a security zone is disabled, the system can still identify some specific applications if being configured with appropriate policy rules. For example, to identify QQ, configure the following two rules (take policy rules from the zone untrust to the zone trust as the example):

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any application QQ permit
Rule id 5 is created
hostname(config-policy)# rule from any to any application any permit
Rule id 6 is created
hostname(config-policy)# exit
hostname(config)#
```

SIP Deep Identification

SIP is an application layer protocol that is typically used to set up, connect and disconnect multimedia sessions, such as Internet phone calls. SIP Protocol can deliver multimedia session data, such as voice, video, or text. When the result of application identification is SIP, the system can further identify whether the packets use GB/T 28181 or GB/T 35114.

Enabling/Disabling SIP Deep Identification

To enable/disable SIP Deep Identification, in the global mode, use the following commands:

- To enable: **app deep-identify protocol SIP enable**
- To disable: **no app deep-identify protocol SIP enable**

Viewing the Status of SIP Deep Identification

To view the status of SIP Deep Identification, in the global mode, use the following command:

show app deep-identify status



Notes: Update the application signature DB before enabling this function.

Application Identification Bypass

When a large number of newly created sessions occur in the device, it will consume a large amount of the device CPU to perform application identification for all new sessions. After the application identification bypass function is configured, the device, with a certain probability, only performs service identification and cache table identification for the new sessions but not further identification. Therefore, the CPU usage of the device is controlled, and other functional modules are not influenced. By default, this function is disabled.

You can configure the CPU usage range according to your own needs. According to the configured CPU range and the current CPU usage, the device processes newly created sessions in different ways. If the current CPU usage is lower than the configured minimum CPU usage, the device performs application identification for all newly created sessions. If the current CPU usage is higher than the minimum CPU usage but lower than the configured maximum CPU usage, the device performs application identification for the newly created sessions in a certain probability. The probability is approximately equal to (current CPU usage - minimum CPU usage)/(maximum CPU usage - minimum CPU usage). If the current CPU usage is higher than the maximum CPU usage, the device only performs service identification and cache table identification for all newly created sessions.

Enabling/Disabling Application Identification Bypass

To enable/disable application identification bypass, in the global configuration mode, use the following commands:

app-ident-bypass {**enable** | **disable**}

- **enable** − Enables the application identification bypass.
- **disable** − Disables the application identification bypass.

Configuring CPU Usage Range

To configure the CPU usage range, in the global configuration mode, use the following commands:

app-ident-bypass threshold *start_value end_value*

- *start_value* – Specifies the minimum CPU usage. The value range is 0 to 100. The default value is 60. The unit is %.
- *end_value* – Specifies the maximum CPU usage. The value range is 0 to 100. The default value is 80. The unit is %.

Viewing Information of Application Identification Bypass

To view the status of the application identification bypass and the configured CPU usage range, in the global configuration mode, use the **show app-ident-bypass** command.

Application Identification Cache Table

Application identification cache table can store application information to provide support for application identification and PBR. The system supports dynamic and static application identification cache tables.

- Dynamic application identification cache table: stores application information that is dynamically learned (the result of dynamic application identification).
- Static application identification cache table: stores static application information. This table is included in the application signature database.

You can configure application cache tables as needed for different scenarios.

Enabling/Disabling Application Identification Cache Table

Both the dynamic and static application identification cache tables are enabled by default. If the dynamic application identification cache table is disabled, the system will still write entries to the table, but will not identify any application based on the entries in the table. The static application identification cache table will not take effect unless the dynamic application identification cache table is enabled, i.e., disabling the dynamic application identification cache table will also disable the static application identification cache table.

To disable/enable the dynamic application identification cache table, in the global configuration mode, use the following commands:

- Disable: **app cache disable**
- Enable: **no app cache disable**

To disable/enable the static application identification cache table, in the global configuration mode, use the following commands:

- Disable: **app cache static disable**
- Enable: **no app cache static disable**

Specifying a Working Mode for the Dynamic Application Identification Cache Table

To specify a working mode for the dynamic application identification cache table, in the global configuration mode, use the following command:

app cache {**cache-strict** | **response-check** | **pbr-check-strict**}

- **cache-strict** – Applicable for SNAT scenarios (Intranet users visit Internet via NAT devices). In such a scenario, enabling this option can effectively evade false positive. This option is disabled by default.
- **response-check** – When the system is possibly subjected to single-directional packet attacks, this option is recommended to assure the accuracy of application identification. This option is disabled by default.
- **pbr-check-strict** – Specifies the application identification method for PBR. By default even if the system has already identified the application in PBR based on dynamic application identification cache table, it will still go on with the identification procedure and select a policy-based route based on the final identification result. With this option enabled, the system will not go on with the identification procedure once the application is identified based on the dynamic application identification cache table, and will directly select a policy-based route based on the above identification result.

To cancel the above configuration, in the global configuration mode, use the following command:

no app cache {**cache-strict** | **response-check** | **pbr-check-strict**}

Clearing the Application Identification Cache Table

To clear all the entries in the dynamic application identification cache table, in any mode, use the following command:

clear app cache table

To clear all the entries in the static application identification cache table, in any mode, use the following command:

clear app cache table static

Viewing Application Identification Cache Table Information

To view if the dynamic or static application identification cache table is enabled and related configuration information, in any mode, use the command **show app cache status**.

Updating the Signature Database

Applications are updated frequently. Hillstone devices allow you to update the application signature database to assure the devices can adapt to these changes in time and identify the latest software version. You can download the latest signature file and upload to the device. Hillstone regularly uploads new signature files on the Hillstone website. You need to download the files, and then upload them to the device.

To upload the signature file via CLI, in the execution mode, use the following command:

import application-signature from {ftp server *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} *file-name*

- *ip-address* – Specifies the name of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the signature file that will be uploaded.

After the signature database is updated, the new signature database takes effect immediately without restarting the system.

Configuring an Application Signature Update Mode

System supports both manual and automatic update modes. To configure an application signature update mode, in the global configuration mode, use the following command:

app update mode {**auto** | **manual**}

- **auto** – Specifies the automatic application signature update mode. This is the default mode.
- **manual** – Specifies the manual application signature update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no app update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

app update protocol HTTP

In the global configuration mode, use the command **no app update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest application signature database as needed. To configure the update the server, in the global configuration mode, use the following command:

app update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is

update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter** *vrouter-name* - Specifies the VRouter to which the update server belongs.

In the global configuration mode, use the following command to restore the default settings of the update server.

no app update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the application signature database updating, use the following command in the global configuration mode:

app update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the **main** parameter to specify the main proxy server and use the **backup** parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no app update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the application identification database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

app update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically updated this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the application signature database immediately as needed. To update the application signature database now, in any mode, use the following command:

exec app update [**professional** | **standard**]

- **exec app update** [**professional**] – Compares the version number of the current application signature database with that of the latest professional version released on the update server. If the version number is different, the application signature database of the device is updated to the latest professional version. If the version number is the same, no update operation is performed. If the application signature database type is not specified, the application signature database is Professional by default.
- **standard** – Compares the version number of the current application signature database with that of the latest standard version released on the update server. If the version number is different, the application signature database of the device is updated to the latest standard version. If the version number is the same, no update operation is performed.

Viewing Application Signature Information

You can view the application signature database information of the device as needed, including the application signature database version, and the release date. To view application signature

database information, in any mode, use the following command:

show app info

Example:

```
hostname(config)# show app info
Application identification engine version: 03.88 (Displays the version of the application signature database engine)
Application identification signature version: 3.0.231124(Professional) (Displays the version of the application signature database)
Release time: 2023-11-24 17:57 (Displays the release time of the application signature database version)
```

Viewing Application Signature Update Information

You can view the application signature update information of the device as needed, including the update server information, update mode, update frequency and time. To view the application signature update information, in any mode, use the following command:

show app update

Example:

```
hostname(config)# show app update
APP signature update options:
protocol: HTTP (Displays the transport protocol for updating the application signature database)
server1: update1.hillstonenet.com, 80, trust-vr (Displays the application signature database update server: server1)
server2: update2.hillstonenet.com, 80, trust-vr (Displays the application signature database update server: server2)
server3:(Displays the application signature database update server: server3)
proxy server status: disable( Displays the status of the
```

```
HTTP proxy server)

main proxy server: (Displays the main proxy server)

backup proxy server: (Displays the backup proxy server)

mode: auto(Displays the update mode of the application sig-
nature database)

state report: disable (Displays whether to enable the func-
tion of uploading application signature database version
information and application traffic statistics to the update
server)

schedule: daily 09:21 (Displays the update frequency of the
application signature database)

current status: normal (Displays the update status of the
application signature database)

last update result: latest signature, needn't update (Dis-
plays the result of the last update of the application sig-
nature database)

last update time: Thu Dec 21 09:21:22 2023 (Displays the
time when the application signature database was last
updated)
```

Application Filter Group

Application Filter Group allows you to create a gourp to filter applications according to application category, sub-category, technology, risk, and attributes.

Configure the application filter group as follows:

1. To create a application filter group
2. To specify application category
3. To specify application subcategory

4. To specify application technology
5. To specify risk value for application
6. To specify characteristic for application

Creating Application Filter Group

To create an application filter group, in the global configuration mode, use the following commands:

application-filter *filter-name*

- *filter-name* – Specifies a name for the application filter group.

Use **no application-filter** *filter-name* to delete the application filter group.

Specifying Application Category

To specify application category, in the application-filter-group configuration mode, use the following commands:

category *category-type*

- *category-type* – Specifies the category type for the application filter group.

Use **no category** *category-type* to delete the category type.

Specifying Application Subcategory

To specify application subcategory, in the application-filter-group configuration mode, use the following commands:

subcategory *subcategory-type*

- *subcategory-type* – Specifies the subcategory type for the application filter group.

Use **no subcategory** *subcategory-type* to delete the subcategory type.

Specifying Application Technology

To specify application technology, in the application-filter-group configuration mode, use the following commands:

technology *technology-type*

- *technology-type* – Specifies the technology type for the application filter group.

Use **no technology** *technology-type* to delete the technology type.

Specifying Risk Value for Application

To specify the risk value, in the application-filter-group configuration mode, use the following commands:

risk *risk-value*

- *risk-value* – Specifies the application risk value. The range is from 1 to 5. 5 means the highest risk.

Use **no risk** *risk-value* to delete the risk value.

Specifying Application Characteristics

To specify the application characteristics, in the application-filter-group configuration mode, use the following commands:

- Specifies "evasive" attributes: **evasive** [**yes** | **no**]
- Specifies "excessive bandwidth" attributes: **excessive-bandwidth** [**yes** | **no**]
- Specifies "file transfer" attributes: **file-transfer** [**yes** | **no**]
- Specifies "known vunerabilities" attributes: **known-vunerabilities** [**yes** | **no**]
- Specifies "prone to misuse" attributes: **prone-to-misuse** [**yes** | **no**]
- Specifies "tunnels other apps" attributes: **tunnels-other-apps** [**yes** | **no**]

- Specifies "used by malware" attributes: **used-by-malware** [**yes** | **no**]
- Specifies "widely used" attributes: **widely-used** [**yes** | **no**]

Configuration Example

In the configuration example, you create an application named my-application and configure the following settings for this application:

- Create a user-defined application signature rule for my-application and specify the ID of the signature as 1.
- Configure the entry of the application signature rule as follows:
  - Source zone: untrust
  - Source address: any
  - Destination address: any
  - Application type: TCP type; destination port number: 2121

See the following detailed commands:

```
hostname(config)# app-signature
hostname(config-appsig)# signature id 1
hostname(config-appsig-rule)# application my-application
hostname(config-appsig-rule)# src-zone untrust
hostname(config-appsig-rule)# src-addr any
hostname(config-appsig-rule)# dst-addr any
hostname(config-appsig-rule)# protocol tcp dst-port 2121
hostname(config-appsig-rule)# exit
hostname(config-appsig)# exit
hostname(config)#
```

After completing the configurations, traffic that satisfies the signature rule 1 will be identified as the application of my-application.

DNS

DNS, the abbreviation for Domain Name System, is a computer and network service naming system in form of domain hierarchy. DNS is designed for TCP/IP network to look for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.

Overview

Hillstone devices' DNS provides the following functions:

- Server: Configures DNS servers and default domain names for the Hillstone device.
- Proxy: The Hillstone device acts as a DNS proxy server and provides proxy service for the connected PCs and other clients. Besides, the Hillstone device can also choose different DNS servers according to domain names.
- Resolver: Sets retry times and timeout for Hillstone device's DNS service.
- Cache: Stores DNS mappings to cache to speed up query.

Configuring a DNS Server

The configuration of DNS server includes:

- Configuring a domain name for the device
- Configuring a DNS domain name server for the device

Configuring a Domain Name

You can specify a domain name for the Hillstone device. The StoneOS will append the domain name as a suffix to the incomplete name. For example, if you specify the domain name as yahoo.-com, and ping www on the device, then the StoneOS will append the domain name to look for www.yahoo.com. In addition, the resolution sequence is different when specifying the domain name to yahoo.com and com: if you specify the domain name as yahoo.com and ping www, the

system will first look for www.yahoo.com; if you specify the domain name as com and ping www.yahoo, the system will first look for www.yahoo, and then look for www.yahoo.com.

To specify a domain name, in the global configuration mode, use the following command:

ip domain name *domain-name*

- *domain-name* – Specifies the domain name. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.

To restore to the default domain name, in the global configuration mode, use the command **no ip domain name** .

The following command specifies the default domain name as hillstonenet.com:

```
hostname(config)# ip domain name hillstonenet.com
```

Configuring a DNS Domain Name Server

DNS domain name server is used by the Hillstone device to resolve DNS. To specify a DNS domain name server, in the global configuration mode, use the following command:

ip name-server *server-address1* [*server-address2*] ... [*server-address6*] [**vrouter** *vrouter-name*]

- *server-address1* – Specifies the IP address of the domain name server. You can configure up to 6 domain name servers by one command or multiple commands, i.e., running command **ip name-server 1.1.1.1 2.2.2.2** and running commands **ip name-server 1.1.1.1** and **ip name-server 2.2.2.2** make no difference. You can configure up to 64 domain name servers.
- *vrouter-name* – Specifies a DNS server for the specified VRouter.

To cancel the specified DNS domain name server, in the global configuration mode, use the command **no ip name-server** *server-address1* [*server-address2*] ... [*server-address6*].

Configuring a DNS Proxy

DNS Proxy function take effect by the DNS proxy rules.Generally a proxy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's ingress interface , source address, destination address, and domain name. The action of the DNS

proxy rules includes proxy,bypass and block. When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers, so that the DNS request meeting the filtering condition will be resolved by these DNS proxy servers.

Each proxy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a proxy rule ID at your own choice. All proxy rules in StoneOS are arranged in a specific order. When DNS traffic flows into a Hillstone device, the device will query for proxy rules in the list by turns, and processes the traffic according to the first matched rule.

The configuration of DNS proxy on Hillstone devices includes:

- Configuring a DNS proxy rule
- Moving a DNS Proxy Rule
- Configuring Time Interval of Tracking for DNS Proxy
- Enabling/Disabling Calculating the Checksum of UDP Packet for DNS Proxy
- Specifying the TTL for DNS-proxy Response Packets
- DNS Proxy Hit Analysis

Configuring a DNS Proxy Rule

You can configure a DNS proxy rule via CLI to control the DNS traffic destined to the device. The configuration includes:

- Creating a DNS proxy rule
- Configuring the Filtering Condition of a DNS Proxy rule
- Specifying the Action of a DNS Proxy Rule
- Configuring DNS Proxy Servers
- Enabling/Disabling DNS Proxy Log

- Enabling/Disabling a DNS Proxy Rule
- Modifying/Deleting the Descriptions of a Proxy Rule

Creating a DNS Proxy Rule

To create a DNS proxy rule or enter the DNS Proxy rule configuration mode, in the global configuration mode, use the following command:

dns-proxy rule [**id** *id*]

- **id** *id* – Specifies the ID of the DNS proxy rule. If not specified, the system will automatically assign an ID to the DNS proxy rule. The ID must be unique in the entire system.

To delete the DNS proxy rule, in the global configuration mode, use the command **no dns-proxy rule id** *id*.

Configuring the Filtering Condition of a DNS Proxy rule

The filtering conditions of a DNS Proxy rule include the ingress interface, source address, destination address and DNS domain name of DNS request. You should configure these four conditions simultaneously, and then system will filter the DNS requests after configuration. Only if the DNS request meets the above four conditions can it is considered a successful match.

Specifying Ingress Interface

You can specify the ingress interface of DNS request in the rule to filter the DNS request message. It is permissible to specify numbers of interfaces. To add or delete the ingress interface of request, in DNS proxy rule configuration mode, use the following command:

- Add the ingress interface of DNS traffic: **ingress-interface** *interface-name*
- Delete the ingress interface of DNS traffic: **no ingress-interface** *interface-name*

Specifying Source Address

You can specify the source address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. To add or delete the

source address of DNS request, in DNS proxy rule configuration mode, use the following command:

- Add the source address of the address entry type: **src-addr** { *addr-name* | **any**}
- Delete the source address of the address entry type: **no src-addr** { *addr-name*| **any**}
- Add the source address of the IP member type: **src-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the source address of the IP member type: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Add the source address of the IP range type: **src-range** *min-ip max-ip*
- Delete the source address of the IP range type: **no src-range** *min-ip max-ip*

Specifying Destination Address

You can specify the destination address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple destination address filtering conditions.To add or delete the destination address of request, in DNS proxy rule configuration mode, use the following command:

- Add the destination address of the address entry type: **dst-addr** { *addr-name* | **any**}
- Delete the destination address of the address entry type: **no dst-addr** { *addr-name* | **any**}
- Add the destination address of the IP member type: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destinaion address of the IP member type: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Add the destination address of the IP range type: **dst-range** *min-ip max-ip*
- Delete the destination address of the IP range type: **no dst-range** *min-ip max-ip*

Specifying Domain Name

You can specify the domain name of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple domain name filtering conditions.To add or delete the domain name, in DNS proxy rule configuration mode, use the following command:

domain { **any** | *domain-name* | **host-book** *host-book-entry* }

- *domain-name* - Specifies the domain name that will be matched.
- **any** – Specifies as any domain name that will be matched.
- **host-book** *host-book-entry* – Specifies the name of the host entry that will be matched.

In DNS proxy rule configuration mode ,use the following command to delete the domain name that will be matched:

no domain any | *domain-name* | **host-book** *host-book-entry*.

Specifying the Action of a DNS Proxy Rule

For the DNS request that meets the filtering conditions, system can proxy, bypass and block the traffic.You can specify the action for a DNS proxy rule, in the DNS proxy rule configuration mode, using the following command:

action {**proxy** [**rollback**]| **secure-dns** | **bypass** | **block**}

- **proxy** [**rollback**] – Specifies the action of a DNS proxy rule as proxy. The DNS request will be resolved through the proxy server. You can configure the **rollback** property as needed. After **rollback** is configured, when there is no DNS server or DNS server unable to resolve the DNS address, system will bypass the DNS request and forward it to the DNS server originally requested by the message.
- **secure-dns** – Specifies the action of a DNS proxy rule as secure DNS. That is, the DNS request will be proxied and resolved through the DoH server. When the secure DNS function is not enabled or the connection fails, the default action is "proxy". For more information, see Secure DNS.

- **bypass** – Specifies the action of a DNS proxy rule as bypass. That is, the DNS request will be forwarded to the DNS server originally requested by the message.
- **block** – Specifies the action of a DNS proxy rule as block. That is,the DNS request will be discarded.

Configuring DNS Proxy Servers

When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers. You can specify up to six DNS server and you can configure the interface and preferred properties for the DNS server as needed. When you configure multiple DNS servers, the DNS server with preferred property will be selected for domain name resolution. If no preferred server is specified, the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin; Except for the two DNS servers, which means that you only have a regular DNS server, then select this kind of DNS servers in a round robin. You can also use the DNS server automatically obtained by the system.

To add a DNS proxy server,in the DNS proxy rule configuration mode, use the following command:

name-server *server-ip* [**vrouter** *vrouter-name*| **egress-interface** *interface-name*| **preferred**]
use-system [**vrouter** *vrouter-name*| **interface** *interface-name*

- *server-ip* [**vrouter** *vrouter-name*| **egress-interface** *interface-name*| **preferred** - Specifies the user-defined DNS proxy server.
  - *server-ip* – Specifies the IP address of the user-defined DNS proxy server.
  - *vrouter-name* – Specifies the VRouter where the user-defined DNS proxy belongs.
  - *interface-name* – Bind the egress interface to the DNS proxy server. After binding, the system will forward the DNS request to the DNS proxy server through this interface.
  - **preferred** – Specifies a user-defined DNS proxy server as the preferred server. Only one server can be specified as the preferred server in each DNS proxy rule.

- **use-system** [**vrouter** *vrouter-name*| **interface** *interface-name* − Specifies to use the DNS server configured by the system or learned through DHCP, PPPoE, etc.
    - **vrouter** *vrouter-name* - Specifies the virtual router from which the DNS server is learned and obtained.
    - **interface** *interface-name* - Specifies the interface from which the DNS server is learned and obtained.

Use **no name-server** *server-ip* [**vrouter** *vrouter-name*] to delete user-defined DNS proxy server.

Use **no name-server use-system** to cancel the DNS server automatically obtained by the system.

Modifying/Deleting the Descriptions of a Proxy Rule

In the DNS proxy rule configuration mode, use the following command to modify the description of a rule.

description *description*

- *description* − Specifies the description for the dns proxy rule.

In the DNS Proxy Rule configuration mode, use the command **no description** to delete the description.

Enabling/Disabling DNS Proxy Log

With the DNS Proxy Log function enabled, the system will generate log information when there is DNS request traffic matching a DNS proxy rule. To enable or disable the DNS proxy log function, in the DNS proxy rule configuration mode, use the following command:

log {**enable** | **disable**}

- **enable** | **disable** - Enable (**enable**) or disable (**disable**) the DNS proxy log function.

Enabling/Disabling a DNS Proxy Rule

DNS proxy rule is enabled by default. To disable or enable the function, in the DNS proxy rule configuration mode, use the following command:

- Disable a DNS proxy rule : **disable**
- Enable a DNS proxy rule: **enable**

Moving a DNS Proxy Rule

Each DNS proxy rule is labeled with a unique ID. When traffic flowing into the Hillstone device, the device will query for DNS proxy rules by turns, and then process the DNS request according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dns-proxy is the query sequence for the matching. You can move a DNS proxy rule to modify the matching sequence. To move a DNS proxy rule, in the globle configuration mode, use the following command:

dns-proxy move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id* }

- **move** *rule-id* – Specifies the DNS proxy rule that will be moved.
- **top** – Move the DNS proxy rule to the top of all the rules.
- **bottom** – Moves the DNS proxy rule to the bottom of all the rules.
- **before** *rule-id* – Move the DNS proxy rule before the rule id.
- **after** *rule-id* – Move the DNS proxy rule after the rule id.

Configuring Time Interval of Tracking for DNS Proxy

This function is to track the reachability of the DNS proxy server. System will periodically detect the DNS proxy server at a specific time interval. When the server cannot be tracked, the IP address of server will be removed from the DNS resolution list untill the link is restored. By default, the tracking for DNS proxy server is enabled.To configure the time interval of tracking for DNS proxy server,in the global configuration mode, use the following command:

dns-proxy server-track [**interval** *interval-time*]

- *interval-time* – Specifies the tracking interval time. The value range is 0 to 30 seconds. The default value is 10.

To disable tracking for DNS proxy server, in the global configuration mode, use the following command:

no dns-proxy server-track

Enabling/Disabling Calculating the Checksum of UDP Packet for DNS Proxy

The system will calculate the checksum of UDP packet for DNS proxy when the DNS proxy on interfaces is enabled. If you need to improve the performance of the device,you can disable this function.

To enable/disable calculating the checksum of UDP packet for DNS proxy, in the globle configuration mode, use the following command:

- Enable: **dns-proxy udp-checksum enable**
- Disable: **dns-proxy udp-checksum disable**

Specifying the TTL for DNS-proxy Response Packets

TTL refers to the survival time of the DNS records in DNS-proxy server. To specify the TTL of DNS-proxy response packets, in the global configuration mode, use the following command:

dns-proxy ttl *ttl-time*

- *ttl-time* – Specifies the TTL for DNS-proxy's response packets. If the DNS-proxy requests are not responded after the TTL, the DNS client will clear all DNS records. The value range is 30 to 600 seconds. The default value is 60.

To disable this function, in the global configuration mode, use the command **dns-proxy ttl disable**.

DNS Proxy Hit Analysis

DNS Proxy Hit Analysis is a process to check the DNS proxy rule hit counts, that is, when DNS request traffic matches a certain DNS proxy rule, the hit count will increase by 1 automatically, and the ratio of the hit number of each DNS proxy rule to all the DNS requests of the system is counted, which directly shows the efficiency of the use of DNS proxy rules in the user network.

Viewing DNS Proxy Statistical Information

To view the DNS proxy statistical information, in any mode, use the following command:

show dns-proxy statistics [**history** {**day** | **hour** | **month** | **week**}]

- **history** {**day** | **hour** | **month** | **week**} – View the statistical information within the latest 1 hour (**hour**), the latest 1 day (**day**), the latest 1 week (**week**) or the latest 1 month (**month**). If it's not specified, all DNS proxy statistics will be displayed.

Clearing DNS Proxy Statistical Information

To clear all the DNS proxy statistical information, in any mode, use the following command:

clear dns-proxy statistics

Viewing the DNS Proxy Rule

To view the DNS proxy rule in details, in any mode, use the following command:

show dns-proxy [**rule id** *rule-id*]

- *rule-id* – Shows the details of the specified DNS proxy rule. If it's not specified, all DNS proxy rules will be displayed.

Resolution

Users can specify the retry times and timeout of DNS requests for the DNS function of Hillstone devices, TTL for the DNS-proxy response packets and DNS load balancing.

Specifying the Timeout of DNS Requests

StoneOS will wait for DNS server's response after sending the DNS request, and will send the request again if no response returns after a specified time. The period of waiting for response is known as timeout. To specify the timeout of DNS requests, in the global configuration mode, use the following command:

ip domain timeout *timeout-value*

- *timeout-value* – Specifies the timeout value. The value range is 1 to 3 seconds. The default value is 2.

To restore to the default timeout, in the global configuration mode, use the command **no ip domain timeout**.

Specifying the Retry Times of DNS Requests

If the DNS request is not responded after timeout, StoneOS will send the request again; if still not responded after the specified retry times (i.e., the repetition times of the DNS request), StoneOS will send the request to the next DNS server. To specify the retry times, in the global configuration mode, use the following command:

ip domain retry *times*

- *times* – Specifies the retry times. The value range is 1 to 3 times. The default value is 2.

To restore to the default retry times, in the global configuration mode, use the command **no ip domain retry**.

Specifying the Maximum Request Interval for DNS Resolution

The system supports to specify the maximum time interval time for the device to send DNS requests to the DNS server. If not specified, the device will send DNS requests to the DNS server after the domain name resolution cache has expired. To specify the maximum request interval time for DNS resolution, in the global configuration mode, use the following command:

ip domain interval-time*value*

- *value* – Specifies the maximum time interval time for the device to send DNS requests to the DNS server. The range of values is 60 to 3600 seconds.



Notes: This command takes effect only for registered domain names.

Specifying the TTL for DNS Resolution Cache

TTL refers to the survival time of the DNS domain name resolution cache (including dynamic DNS cache and register DNS cache). To specify the TTL of DNS resolution cache, in the global configuration mode, use the following command:

ip domain ttl *ttl-time*

- *ttl-time* – Specifies the TTL for DNS resolution cache. If the DNS resolution cache are not responded after the TTL, the system will clear all domain name records. The value range is 60 to 86400 seconds.

In the global configuration mode, use **no ip domain ttl** command to restore to the default value which is a value returned by DNS server.

Configuring Host TTL

Host TTL refers to the survival time of the DNS domain name resolution cache. You can configure the TTL for the specified domain name resolution cache.

To configure host TTL, you need to enter the DNS Cache mode first. To enter the DNS Cache mode, in the global mode, use the following command:

dns-cache

To configure host TTL, in the DNS Cache mode, use the following command:

host*host-name***ttl***ttl-time* [**vrouter***vr-name*]

- *host-name* – Specifies the domain name. The length is 1 to 255 characters.
- *ttl-time* – Specify the survival time of the DNS domain name resolution cache. When the TTL value exceeds the specified value, the system sends a DNS request to the DNS server again. If the request receives a response, the cache is updated. If no response is received, the cache is cleared from the device. The value range is 60 to 86400 seconds.
- *vr-name* – Specifies the VRouter.

In the global configuration mode, use **no host***host-name* [**vrouter***vr-name*] command to delete the specifies host TTL entries.



Notes:

- This function takes effect only for register domain names.
- Host TTL has a higher priority than TTL which configured by using ip domain ttl command.

Viewing the Configuration Information of Host TTL

To view the configuration information of host TTL, in any mode, use the following command:

show dns-cache

Below is a return example:

```
hostname# show dns-cache
Total:2
=============================================================
======
Host TTL(sec) VR NAME
-------------------------------------------------------------
www.test1.com 300 trust-vr
www.test2.com 200 mgt-vr
=============================================================
======
```

Enabling the DNS Resolution Log

You can enable the DNS resolution log function to record the result of DNS resolution, and generate the log information, the log content including the domain name, IP address of the DNS and

generation time. By default, the function is closed.To enable the DNS resolution log function, in the global configuration mode, use the following command:

ip domain response-log

To disable the DNS resolution log function, in the global configuration mode, use the command **no ip domain response-log**.

DNS Cache

When using DNS, a system might store the DNS mappings to its cache to speed up the query. There are 3 ways to obtain DNS mappings:

- Dynamic: Obtains from DNS response.
- Static: Adds DNS mappings to cache manually.
- Register: DNS hosts specified by some modules of Hillstone devices, such as NTP, AAA, address book, etc.

You can add static DNS mappings to cache, view DNS mappings and delete dynamic mappings.

Adding a Static DNS Mapping

To manually add a DNS mapping to the cache, in the global configuration mode, use the following command:

ip host*host-name* {*address1* [*address2*] ... [*address8*]} [**ttl***ttl-time*] [**vrouter***vrouter-name*]

- *host-name* – Specifies the host name. The length is 1 to 255 characters.
- {*address1* [*address2*] ... [*address8*]} – Specifies the IP Address of the host. You can specify up to 8 IP addresses.
- *ttl-time* – Specifies the TTL value, which is the survival time of the DNS mapping entry cache on the device. When the device has enabled the DNS proxy function and the DNS request initiated by the client matches the DNS proxy rule, if the DNS request hits the local

cache, the TTL value set in the local cache will be returned to the client, and the cache will be deleted from the client if the TTL value is exceeded. The range is 60 to 86400 seconds.

- *vrouter-name* – Specifies the VRouter for the host.

To delete the specified DNS mapping, in the global configuration mode, use the command **no ip host** *host-name*.

Viewing a DNS Mapping

To view a DNS mapping, in any mode, use the following command:

show ip hosts [*host-name*] [**vrouter** *vrouter-name*]

- *host-name* – Shows the DNS mapping of the specified host.
- *vrouter-name* - Shows the DNS mapping of the specified VRouter.

Deleting a Dynamic DNS Mapping

To manually remove a dynamic DNS mapping, in the execution mode, use the following command:

clear host [*host-name* [**vrouter** *vrouter-name*]]

- *host-name* – Deletes the DNS mapping of the specified host.
- *vrouter-name* – Deletes the host DNS mapping of the specified VRouter.

This command is used to delete the specified or all the dynamic DNS mappings. To delete the static DNS mappings that are manually added, use the command **no ip host**.

Secure DNS

The Secure DNS function is a cloud-network collaborative security solution that allows real-time security detection of DNS traffic and blocks malicious domain access when DNS proxy requests are initiated by intranet devices. In this solution, the firewall forwards DNS traffic proxies passing through the firewall to the cloud-based Secure DNS SaaS service by using the DNS proxy

function and DoH encrypted transmission protocol, where the threat is sensed, identified, and blocked. In addition, basic DNS resolution is implemented.

When configuring the Secure DNS function, you do not need to modify the DNS configuration of intranet devices, so it is completely transparent to the intranet devices. In addition, compared with traditional DNS service, Secure DNS SaaS service provides DNS service as well as the ability of security protection.



Notes: The device supports integration with 360 Secure DNS SaaS service. Before you enable this function, go to sdns.360.cn to apply for 360 Secure DNS SaaS service.

The configuration of the Secure DNS function includes:

- Enabling/Disabling the Secure DNS Function
- Entering the Secure-DNS Profile Configuration Mode of a Specified Provider
- Configuring the DoH Server
- Enabling/Disabling the Function of Sending the Client Address
- Configuring the Health Check Interval
- Enabling/Disabling the Function of Generating Logs
- Viewing Information about Secure DNS Configuration

Enabling/Disabling the Secure DNS Function

By default, the Secure DNS function is disabled. To enable this function and specify the DoH server provider, in global configuration mode, use the following command:

secure-dns enable service-provider *provider-name*

- *provider-name* – Specifies the provider name of the DoH server. Only 360 is supported.

To disable the Secure DNS function, in global configuration mode, use the following command:

secure-dns disable

Entering the Secure-DNS Profile Configuration Mode of a Specified Provider

To configure the Secure DNS function, you need to enter the Secure-DNS Profile configuration mode of a specified provider. To do this, in global configuration mode, use the following command:

secure-dns profile service-provider *provider-name*

- *provider-name* – Specifies the provider name of the DoH server. Only 360 is supported.

Configuring the DoH Server

To configure the domain name or IP address of the DoH server and the corresponding virtual router, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

doh-server {*domain* | *ip-address*} [**vrouter** *vr-name*]

- *domain* | *ip-address* – Specifies the domain name or IP address of the DoH server. By default, doh.360.cn is used.
- *vr-name* – Specifies the virtual router to which the DoH server belongs. By default, trust-vr is used.

In Secure-DNS Profile configuration mode, use the **no doh-server** command to restore to the default configuration.

Enabling/Disabling the Function of Sending the Client Address

After enabling this function, when you request domain resolution by using DNS proxy, the system uploads the IP address of the client to 360 cloud for O&M.

To enable/disable the function of sending the client address, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

- Enable: **send-client-ip enable**
- Disable: **send-client-ip disable**

Configuring the Health Check Interval

To avoid the failure of domain name resolution by using the DoH protocol due to an abnormal DoH server, the system can periodically send DNS health check messages to the DoH server. When two consecutive health checks fail, the system switches the Secure DNS function to Inactive. While in the Inactive status, the system cannot use the DoH protocol through the Secure DNS function to resolve domain names , but it continues to send health check messages. Once a successful check is detected, the Secure DNS function will be immediately switched to Active.

To configure a health check interval, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

track-interval *time-value*

- *time-value* – Specifies the interval at which a DNS health check message is sent to the DoH server. Valid values: 3 to 60 seconds. Default value: 10 seconds.

In Secure-DNS Profile configuration mode, use the **no track-interval** command to restore to the default configuration.

Enabling/Disabling the Function of Generating Logs

After enabling this function, when you request the resolution of malicious domain names by using DNS proxy, corresponding threat logs are generated. By default, this function is disabled.

To enable/disable the function of generating logs, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

- Enable: **threat-log enable**
- Disable: **threat-log disable**

Viewing Information about Secure DNS Configuration

To view information about Secure DNS configuration, in any mode, use the following command:

show secure-dns

The following result is returned:

```
hostname(config)# show secure-dns
==========================================================-
=============
Secure DNS: Enable (The status of the Secure DNS function)
Service provider: 360 (The provider that provides the Secure DNS function)
Service status: Active (The availability status of the Secure DNS function)
----------------------------------------------------------------------------------------------------------
----------------------
Profile 360:
Bootstrap server: 101.198.198.198 101.198.199.200 (The built-in 360 public DoH server,
which is used to resolve the DoH server domain name)
DoH server domain: hxr5.n.360.net (The specified DoH server domain name)
DoH server IP: 36.110.234.252, TTL 241 s (The IP address of the DoH server that is
resolved by Bootstrap)
DoH server vrouter: trust-vr (The VRouter to which the DoH server belongs)
Send-client-addr: Enable (The status of the function of sending the client address)
Threat-log: Enable (The status of the function of generating logs)
Track interval: 10 s (The health check interval)
==========================================================-
=============
```

DNS Snooping

The DNS Snooping function creates and maintains a mapping table for domain names and corresponding IPv4/IPv6 addresses through domain name resolution. Meanwhile the system returns the IP address in the mapping table to the function modules that refer to the domain name (such as the address book, PBR, policy, etc.), so as to realize the access control based on the domain name.

DNS Snooping supports obtaining domain name and IP address mapping through the following two methods of domain name resolution:

- Active mode: System periodically initiates DNS queries to the configured DNS domain name server to obtain the mapping information between the domain name and the IP address.
- Passive mode: System monitors the DNS response packets which flow through the device to obtain the mapping information between the domain name and the IP address.

The configurations include:

- Specifying the Domain Name Resolution Mode
- Specifying the Maximum Mapping IP Addresses for a Specific Domain Name
- Specifying the Maximum Wildcard Domain Names
- Specifying the TTL for DNS Snooping Mapping Cache
- Viewing the Configuration Information of DNS Snooping
- Viewing the Mapping information of DNS Snooping

Specifying the Domain Name Resolution Mode

To specifying the mode of the domain name resolution, in the global configuration mode, use the following command:

dns snooping mode {**active** | **passive** | **all**}

- **active** - Specifies the domain name resolution mode as the active mode. In this mode, system periodically initiates DNS queries to the configured DNS domain name server to obtain the mapping information between the domain name and the IP address, meanwhile returns the IP address to the function modules that refer to the domain name. This is the default value.
- **passive** - Specifies the domain name resolution mode as the passive mode. In this mode, system monitors the DNS response packets which flow through the device to obtain the mapping information between the domain name and the IP address, meanwhile returns the IP address to the function modules that refer to the domain name.
- **all** - Specifies the domain name resolution mode as both active mode and passive mode. The IP address will be the union of the IP address resolved by active mode and passive mode.

In the global configuration mode, use the command **no dns snooping mode** to restore the default value.

Specifying the Maximum Mapping IP Addresses for a Specific Domain Name

When the domain name resolution mode is passive mode, users can specify the maximum number of mapping IP addresses for each specific domain name. To specify the maximum number of mapping IP addresses for each specific domain name, in the global configuration mode, use the following command:

dns snooping host-ip-num *number*

- *number* - Specifies the maximum number of mapping IP addresses for each specific domain name. The range is 32 to 256. The default value is 64.

In the global configuration mode, use the command **no dns snooping host-ip-num** to restore the default value.

Specifying the Forward Delay of DNS Response Packets

When DNS Snooping receives DNS response packets and the mapping information between the domain name and the IP address needs to be updated, DNS Snooping supports forwarding the

DNS response packets to client in a delay time, so that client obtains IP address delay. To specify the forward delay time, in the global configuration mode, use the following command:

dns snooping pak-delay *time*

- *time* - Specifies the forward delay time. The range is 0 to 2000 milliseconds. The default value is 5 milliseconds.

In the global configuration mode, use the command **no dns snooping pak-delay** to restore the default value..

Specifying the Maximum Wildcard Domain Names

System supports the function of wildcard domain name (e.g., *.test.com) resolution. To specify the maximum number of wildcard domain names supported by the system, in the global configuration mode, use the following command:

dns snooping wildcard-num *number*

- *number* - Specifies the maximum number of wildcard domain names supported by the system. The range is 128 to 512. The default value is 128.

In the global configuration mode, use the command **no dns snooping wildcard-num** to restore the default value.



Notes: System only supports to resolve wildcard domain names through passive mode.

Specifying the TTL for DNS Snooping Mapping Cache

TTL (Time-to-live) refers to the storage time of the domain name and IP address mapping cache. To specify the TTL for DNS snooping mapping cache, in the global configuration mode, use the following command:

dns snooping ttl *ttl-value*

- *ttl-value* - Specifies the TTL for DNS snooping mapping cache. The range is 60 to 3600 seconds. The default value is 3600 seconds.

In the global configuration mode, use the command **no dns snooping ttl** to restore the default value.



Notes: System will periodically clear the domain name and IP address mapping cache that reaches the timeout value:

- In the passive mode, timeout value of the domain name and IP address mapping cache = TTL for the DNS response packets + TTL for DNS snooping mapping cache.
- For StoneOS 5.5R8P17 and later P versions, StoneOS 5.5R9P8 and later P versions, StoneOS 5.5R10P4 and later P versions, StoneOS 5.5R10F4 and later F versions, StoneOS 5.5R11 and later versions, in active mode, timeout value of the domain name and IP address mapping cache = TTL for DNS Resolution Dynamic Cache. For other versions, in active mode, timeout value of the domain name and IP address mapping cache = TTL for DNS snooping mapping cache. For more information about TTL for DNS Resolution Dynamic Cache, see Specifying the TTL for DNS Resolution Dynamic Cache.

Configuring the UDP Packet Length That Can Be Parsed by DNS Snooping in the Active Mode

By default, the UDP packet length that can be parsed by DNS Snooping in the active mode is up to 512 bytes. You can make configurations to enable DNS snooping parse UDP packet longer than 512 bytes in the active mode. To configure the UDP packet length that can be parsed by DNS Snooping in the active mode, use the following command in the global configuration mode:

dns udp-max-size*value*

- *value* - Specifies the UDP packet length that can be parsed by DNS Snooping in the active mode. This value ranges from 512 to 1536 bytes. The default value is 512 bytes.

In the global configuration mode, use command **no dns udp-max-size** to restore to the default value.

To view the UDP packet length that can be parsed by DNS Snooping in the active mode, use the following command in any mode:

show dns udp-max-size

Viewing the Configuration Information of DNS Snooping

To view the configuration information of DNS snooping, in any mode, use the following command:

show dns snooping configuration

Viewing the Mapping information of DNS Snooping

To view the mapping information of DNS snooping, in any mode, use the following command:

show dns snooping domain {**active** | **passive**} [*domain-name*]

- **active** | **passive** - View the domain name and IP address mapping information obtained by the active mode or the passive mode.
- *domain-name* - View the domain name and IP address mapping information for a specified domain name.

Enabling/Disabling DNS

By default, DNS is disabled on Hillstone devices. To enable/disable the DNS function, in the global configuration mode, use the following commands:

- Enable: **ip domain lookup**
- Disable: **no ip domain lookup**

Viewing DNS configuration information

To view DNS configuration information, in any mode, use the following command:

show dns

DNS Configuration Example

This section describes a typical DNS configuration example.

Requirement

The Hillstone device allows PC1 within the trust zone to access Internet via DNS proxy. The IP address of DNS server in the public network is 202.106.0.20; the IP address of the device's ethernet0/0 interface is 192.168.10.1/24; the IP address of PC1 in the trust zone, which is connected to the above interface, is 192.168.10.3/24; the IP address of ethernet0/1 interface, which is connected to the public network in the untrust zone, is 10.160.65.31/24.

Configuration Steps

Step 1: Bind security zones and configure IP addresses for Hillstone device's interfaces

```
hostname# configure
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.160.65.31/24
hostname(config-if-eth0/1)# exit
```

Step 2: Configure DNS proxy rule on the Hillstone device

```
hostname(config)# dns-proxy rule
```

```
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/0
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.0.20
hostname(config-dns-proxy-rule)# exit
```

Step 3: ping www.sina.com.cn. This address can be resolved on PC1

DDNS

DDNS, the abbreviation for Dynamic Domain Name Server, is designed to resolve fixed domain names to dynamic IP addresses. Generally you will be allocated with a dynamic IP address from ISP each time you connect to the Internet, i.e., the allocated IP addresses for different Internet connections will vary. DDNS can bind the domain name to your dynamic IP address, and the binding between them will be updated automatically each time you connect to Internet.

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. Hillstone devices support the following 5 DDNS providers:

- 3322.org: http://www.3322.org
- Huagai.net: http://www.ddns.com.cn
- ZoneEdit.com: http://www.zoneedit.com
- no-ip.com： http://www. no-ip.com
- dyndns.org： http://www.dyndns.org

Visit one of the above websites to complete registration.

Configuring DDNS

When the IP address of the interface connecting to the external network changes, the Hillstone device will send an update request to the DDNS server (over HTTP) to update the IP address and the binding domain. You can configure different DDNS names, then configure DDNS parameters for the DDNS names (such as the update method, DDNS server and update interval), and finally bind the configured DDNS names to interfaces to enable the DDNS function.

This section describes the following configurations:

- Configuring a DDNS name
- Binding the DDNS name to an interface

Configuring a DDNS Name

The DDNS service parameters need to be configured in the DDNS name configuration mode. To create a DDNS name, specify the type of update and enter the specified DDNS service configuration mode, in the global configuration mode, use the following command:

ddns name *ddns-name* **type http**

- *ddns-name* – Specifies the DDNS name.
- **type http** – Specifies how to update the DDNS service, i.e., sending the DDNS update requests over HTTP.

The command leads you into the configuration mode of the specified DDNS name. You can configure DDNS parameters for the DDNS service, including the DDNS provider, DDNS server name and port number, the minimum and maximum update interval, as well as the username and password of the DDNS provider.

To delete the specified DDNS name, in the global configuration mode, use the command **no ddns name** *ddns-name* **type http**.

Specifying the DDNS Provider

Hillstone devices support 5 DDNS servers: 3322.org, Huagai.net, ZoneEdit.com, no-ip.com and dyndns.org. To specify the DDNS provider, in the DDNS name configuration mode, use the following command:

type {**dyndns** | **huagai** | **no-ip** | **qdns** | **zoneedit**}

- **dyndns** - Use dyndns.org as the DDNS provider.
- **huagai** - Use Huagai.net as the DDNS provider.
- **no-ip** - Use no-ip.com as the DDNS provider.
- **qdns** - Use 3322.org as the DDNS provider.
- **zoneedit** - Use ZoneEdit.com as the DDNS provider.

To cancel the specified DDNS provider, in the DDNS name configuration mode, use the command **no type**.

Specifying the DDNS Server Name and Port

Different DDNS servers are configured with different server names and port numbers. To specify the DDNS server name and port number, in the DDNS name configuration mode, use the following command:

server name *server-name* **port** *port-number*

- *server-name* – Specifies the server name for the configured DDNS.
- *port-number* – Specifies the server port number for the configured DDNS. The value range is 1 to 65535.

To cancel the specified DDNS server name and port number, in the DDNS name configuration mode, use the command **no server**.



Notes: The DNS server name and port number must be the corresponding name and port of the DDNS server. Do not configure these options if the exact information is unknown. The server will return the name and port information automatically after connection to the DDNS server has been established successfully.

Specifying the Minimum Update Interval

When the IP address of the interface with DDNS enabled changes, StoneOS will send an update request to the DDNS server. If the request is not responded, StoneOS will send the request again according to the configured minimum update interval. For example, if the minimum update interval is set to 5 minutes, then StoneOS will send the second request 5 minutes after the first request failure; if it fails again, StoneOS will send the request again 10 (5x2) minutes later; and 20 (10x2) minutes later, so and forth. The value will not increase anymore when reaching 120, i.e., StoneOS will send the request at a fixed interval of 120 minutes. To configure the minimum update interval, in DDNS name configuration mode, use the following command:

minupdate interval *time-value*

- *time-value* – Specifies the minimum update interval. The value range is 1 to 120 minutes. The default value is 5.

To restore to the default minimum update interval, in DDNS name configuration mode, use the command **no minupdate**.

Specifying the Maximum Update Interval

On the condition that IP address has not changed, StoneOS will send an update request to the DDNS server at the maximum update interval. To configure the maximum update interval, in the DDNS name configuration mode, use the following command:

maxupdate interval *time-value*

- *time-value* – Specifies the maximum update interval. The value range is 24 to 8760 hours. The default value is 24.

To restore to the default maximum update interval, in DDNS name configuration mode, use the command **no maxupdate**.

Specifying the DDNS Username/Password

This command is to specify the user information registered in the DDNS provider. To configure the user information, in the DDNS name configuration mode, use the following command:

user *user-name* **password** *user-password*

- *user-name* - Specifies the username registered in the DDNS provider.
- *user-password* - Specifies the corresponding password.

To cancel the specified user information, in the DDNS name configuration mode, use the command **no user**.

Binding a DDNS Name to an Interface

The domain names will not be updated according to the configured DDNS parameters upon any interface IP address changes unless the DDNS name is bound to an interface. To bind the DDNS

name to an interface, in the global configuration mode, use the following command:

ddns enable *ddns-name* **interface** *interface-name* **hostname** *host-name*

- *ddns-name* – Specifies the DDNS name.
- *interface-name* – Specifies the name of the binding interface.
- *host-name* – Specifies the domain name obtained from the corresponding DDNS provider.

To cancel the specified binding, in the global configuration mode, use the command **no ddns enable** *ddns-name* **interface** *interface-name*.

Viewing DDNS Information

To view the DDNS information, in any mode, use the following command:

- Show the DDNS configuration information: **show ddns config** *ddns-name*
- Show the DDNS state: **show ddns state** *ddns-name*

Example of Configuring DDNS

This section describes a typical DDNS configuration example.

Requirement

The interface ethernet0/1 of the Hillstone device locates at the untrust zone, and the interface obtains IP address by PPPoE. If the IP address changes during PPPoE connection, the interface will send an update request to the DDNS server.

Configuration Steps

Step 1: Create a PPPoE instance named pppoe1

```
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
hostname(config-pppoe-group)# idle-interval 5
```

```
hostname(config-pppoe-group)# route distance 2
hostname(config-pppoe-group)# route weight 10
hostname(config-pppoe-group)# authentication any
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

Step 2: Configure ethernet0/1

```
hostname# configure
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address pppoe setroute
hostname(config-if-eth0/1)# pppoe enable group pppoe1
hostname(config-if-eth0/1)# exit
```

Step 3: Configure DDNS on the device

```
hostname(config)# ddns name 3322 type http
hostname(config-ddns)# type qdns
hostname(config-ddns)# user test password 123456
hostname(config-ddns)# exit
```

Step 4: Bind ethernet0/1 to the DDNS named 3322 (the domain name obtained from 3322.org is hillstonenet.3322.org)

```
hostname(config)# ddns enable 3322 interface ethernet0/1 hostname hillstonenet.3322.org
```

Step 5: Configure DNS on the device in order to parse domain names

```
hostname(config)# ip name-server 202.106.0.20
```

Step 6: Launch a PPPoE connection to trigger DDNS when the IP address of the interface changes

```
hostname(config)# pppoe-client group pppoe1 connect
```

DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for subnets automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

DHCP on Hillstone Devices

Hillstone devices support DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: A Hillstone device's interface can be configured as a DHCP client and obtain IP addresses from the DHCP server.
- DHCP server: A Hillstone device's interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: A Hillstone device's interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

Hillstone devices are designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Client

You can configure an interface of the Hillstone device as the DHCP client that obtains IP address from the DHCP server. The DHCP client should be configured in the interface configuration mode. The configuration includes:

- Obtaining an IP address via DHCP
- Releasing and renewing the IP address
- Configuring the route priority (administration distance) and route weight

- Obtaining the Server MTU
- Configuring the DNS Management Priority

Obtaining an IP Address via DHCP

To enable the interface to obtain an IP address via DHCP, in the interface configuration mode, use the following command:

ip address dhcp [**setroute**]

- **setroute** – Uses the gateway specified by the DHCP server as the default route gateway.

To cancel the configuration, in the interface configuration mode, use the command **no ip address dhcp**.

For example, to enable etherenet0/1 to obtain the IP address dynamically via DHCP, and set the default gateway route, use the following commands:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address dhcp setroute
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Releasing and Renewing the IP Address

The interface that has obtained a dynamic IP address via DHCP can release and renew its IP address. To release and renew the IP address, in the interface configuration mode, use the following commands:

- Release: **dhcp-client ip release**
- Renew: **dhcp-client ip renew**

To view the DHCP IP address information allocated to an interface, in the interface configuration mode, use the following command:

dhcp-client ip show

Configuring the Route Priority (Administration distance) and Route Weight

After the DHCP interface is configured with the default route (**ip address dhcp setroute**), to configure the route priority (administration distance) and route weight, in the interface configuration mode, use the following command:

dhcp-client route {**distance** *value*| **weight** *value*}

- **distance** *value* – Specifies the route priority. The value range is 1 to 255. The default value is 1.
- **weight** *value* – Specifies the route weight. The value range is 1 to 255. The default value is 1.

To restore to the default route priory and weight, in the interface configuration mode, use the command **no dhcp-client route** {**distance** | **weight**}.

Enable/ Disable Classless Static Routing Options

After the DHCP interface is configured with the default gateway route (**ip address dhcp setroute**), you can enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. To enable the classless static routing function via DHCP, in the interface configuration mode, use the following command:

dhcp-client classless-static-route

To disable the function of obtaining classless static route via DHCP, in the interface configuration mode, use the following command:

no dhcp-client classless-static-route

Notes:

- The priority of classless static route is higher than the default gateway route, i.e. when the device receives classless static routing options and default gateway routing options at the same time, the device will only add classless static routing information to the routing table.
- By default, it is enabled on interface eth0/0, while it is disabled on other interfaces. You can enable or disable the function on all interfaces.

Viewing DHCP Client Configuration Information

To view the DHCP Client configuration information, in any mode, use the following command:

show dhcp-client interface {*interface-name*}

- *interface-name* – Specifies the name of interface.

Obtaining the Server MTU

You can enable the function of obtaining the server MTU for interface whose IP address is obtained dynamically by using DHCP. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

dhcp-client mtu

In interface configuration mode, use the **no dhcp-client mtu** command to disable the function of obtaining the server MTU.

Notes:

- For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure



the interface MTU, specify the MTU parameter in the interface field section.)

- By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.

Configuring the DNS Management Priority

Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. A larger number indicates a higher priority.

To configure the DNS management priority, in interface configuration mode, use the following command:

dhcp-client dnsadmin-preference *value*

- **admin-preference** *value* – Specifies the DNS management priority. Valid values: 1 to 255. Default value: 20.

Use the **no dhcp-client dnsadmin-preference** command to restore the default value of the DNS management priority.

Configuring a DHCP Server

The Hillstone devices can act as a DHCP server to allocate IP addresses for the DHCP clients in the subnets. The DHCP server should to be configured in the DHCP server configuration mode. To enter the DHCP server configuration mode, in the global configuration mode, use the following command:

dhcp-server pool *pool-name*

- *pool-name* – Specifies the name of the DHCP address pool.

After executing the above command, the system will create a new DHCP address pool and enter the DHCP server configuration mode of the address pool; if the specified address pool exists, the system will directly go to the DHCP server configuration mode:

To delete the specified address pool, in the global configuration mode, use the command **no dhcp-server pool** *pool-name*.

The DHCP server functions you can configure in the DHCP server configuration mode are:

- Basic configuration of the DHCP address pool
- Configuring auto-config
- Configuring DNS/WINS servers and domain name for the DHCP client
- Configuring SMTP/ POP3/news servers for the DHCP client
- Configure the IP address of the relay agent
- IP-MAC Binding
- Configuring option 49

After configuring the DHCP server address pool, you need to bind the DHCP address pool to an interface in order to enable the DHCP server on the interface. For more specific commands, see Binding the Address Pool to an Interface.

In addition, you can view the DHCP configuration of the system anytime by the command **show**.

Basic Configuration of the DHCP Address Pool

This section describes how to configure DHCP address pool.

Configuring an IP Range

You need to specify the IP range used for external allocation. To specify the IP range of the address pool, in the DHCP server configuration mode, use the following command:

address *start-ip-address* [*end-ip-address*]

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no address** *start-ip-address*.

Configuring a Reserved Address

IP addresses in the reserved address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated. To configure the reserved address, in the DHCP server configuration mode, use the following command:

exclude address *start-ip-address* [*end-ip-address*]

- *start-ip-address* – Specifies the start IP address of the reserved address.
- *end-ip-address* – Specifies the end IP address of the reserved address.

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no exclude address** *start-ip-address*.

Configuring a Gateway

To configure the IP address of the gateway for the client, in the DHCP server configuration mode, use the following command:

gateway *ip-address*

- *ip-address* – Specifies the IP address of the gateway.

To cancel the specified IP address of the gateway, in the DHCP server configuration mode, use the command **no gateway**.

Configuring a Netmask

To configure the netmask for the client, in the DHCP server configuration mode, use the following command:

netmask *netmask*

- *netmask* – Specifies the netmask, such as 255.255.255.0.

To cancel the specified netmask, in the DHCP server configuration mode, use the command **no netmask**.

Configuring a DHCP Lease Time

Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is allocated. After the lease expired, the client will have to request an IP address again from the DHCP server. To configure the lease of DHCP server, in the DHCP server configuration mode, use the following command:

lease *lease-time*

- *lease-time* – Specifies the lease time. The value range is 300 to 1048575 seconds. The default value is 3600.

To restore to the default lease time, in the DHCP server configuration mode, use the command **no lease**.

Configuring Auto-config

Auto-config is able to function when an interface in a DHCP server configured gateway has been enabled as DHCP client. When auto-config is enabled, if the DHCP server (Hillstone) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will distribute the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server (Hillstone). However, the DNS, WINS and domain name that are configured manually still have the priority. To configure auto-config, in the DHCP server configuration mode, use the following command:

auto-config interface *interface-name*

- *interface-name* – Specifies the interface with the DHCP client enabled on the same device.

To disable the function, in the DHCP server configuration mode, use the command **no auto-config**.

Configuring DNS/WINS Servers and Domain Name for the DHCP Client

To configure DNS, WINS servers and domain name for the DHCP client, in the DHCP server configuration mode, use the following commands:

dns {**use-system** | *ip-address1* [*ip-address2*]}

- **use-system** - Use the DNS server configured in the system as the DNS server of the client. If the system has configured more than two DNS servers, you can use the first two DNS servers as the DNS servers of the client.
- *ip-address1* – Specifies the IP address of the primary DNS server.
- *ip-address2* – Specifies the IP address of the alternative DNS server.

wins *ip-address1* [*ip-address2*]

- *ip-address1* – Specifies the IP address of the primary WINS server.
- *ip-address2* – Specifies the IP address of the alternative WINS server.

domain *domain-name*

- *domain-name* – Specifies the domain name.

To cancel the configured DNS, WINS server and domain name, in the DHCP server configuration mode, use the following commands:

- **no dns**
- **no wins**
- **no domain**

Configuring SMTP/ POP3/news Servers for the DHCP Client

To configure the SMTP, POP3 and news servers for the DHCP client, in the DHCP server configuration mode, use the following commands:

- **smtp** *ip-address*
- **pop3** *ip-address*
- **news** *ip-address*

To cancel the configured SMTP, POP3 and news servers, in the DHCP server configuration mode, use the following commands:

- **no smtp**
- **no pop3**
- **no news**

Configure the IP Address of the Relay Agent

When the device (Hillstone1) with DHCP server enabled is connected to another deivce(Hillstone2) with DHCP relay enabled, and the PC obtains Hillstone1's DHCP information from Hillstone2, then only when the relay agent's IP address and netmask are configured on Hillstone1 can the DHCP information be transmitted to the PC successfully. To configure a relay agent, in the DHCP server configuration mode, use the following command:

relay-agent *ip-address netmask*

- *ip-address netmask* – Specifies the IP address and netmask of the relay agent, i.e., the IP address and netmask for the interface with relay agent enabled on Hillstone2.

To cancel the specified relay agent, in the DHCP server configuration mode, use the command **no relay-agent** *ip-address netmask*.

IP-MAC Binding

You can manually bind IP and MAC addresses to establish a corresponding relationship between IP and MAC address on the device. In this way, the specified MAC address can only obtain the corresponding bound IP address. To configure an IP-MAC binding, in the DHCP server configuration mode, use the following command:

ipmac-bind *ip-address* **mac** [**description** *description*]

- *ip-address* – Specifies the IP address. The IP address must be the address defined in the address pool.
- *mac* – Specifies the binding MAC address.

- **description** *description* – Specifies a description for this IP-MAC binding entry. You can specify up to 63 characters.

To cancel the specified IP-MAC binding, in the DHCP server configuration mode, use the command **no ipmac-bind** *ip-address*.

Binding the Address Pool to an Interface

If the address pool is bound to an interface, the interface will run DHCP server based on the configuration parameters of the address pool. To bind the address pool to an interface, in the interface configuration mode, use the following command:

dhcp-server enable pool *pool-name*

- *pool-name* – Specifies the address pool defined in the system.

To disable the DHCP server on the interface, in the interface configuration mode, use the command **no dhcp-server enable**.

Configuring DHCP Options

When the interface acts as the DHCP server, the system supports the option 43, option 49, option 60, option 66, option 67, option 138, option 150 and option 242.

Configuring Option 43

Option 43 is used to exchange specific vendor specific information (VSI) between DHCP client and DHCP server. The DHCP server uses option 43 to assign Access Controller (AC) addresses to wireless Access Point (AP), and the wireless AP use DHCP to discover the AC to which it is to connect.

Configuring the VSI Carried by Option 43 for DHCP Server

To configure the VSI carried by option 43 for DHCP server, use the following command in the DHCP server configuration mode:

option 43 {**ascii** *value*| **hex** *value*}

- **ascii** *value* – Specify the VSI in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* – Specify the VSI in hex.

To cancel the option 43 settings, use the **no option 43** command.



Notes:

- If the VCI matching string has been configured, first of all, you need to verify the VCI carried by the option 60 field in client's DHCP packets. When the VCI matches the configured one, the IP address, option 43 and corresponding information will be offered. If not, DHCP server will drop client's DHCP packets and will not reply to the client.
- For verifying VCI carried by option 60, see Verifying VCI Carried by Option 60 section.

Configuring Option 49

To make the DHCP client obtain the list of the IP addresses of systems that are running the X window System Display Manager, configure the option 49 settings. Use the following command to configure the option 49 settings in the DHCP server configuration mode:

option 49 ip *ip-address*

- *ip-address* – Specifies the IP address of the server that is running the X window System Display Manager.

To cancel the option 49 configurations, in the DHCP server configuration mode, use the command **no option 49 ip** *ip-address*.

Configuring Option 60

Option 60 is used by DHCP clients to optionally identify the type and configuration of a DHCP client. The information is a string of n octets, interpreted by servers. Vendors and sites may

choose to define specific vendor class identifiers (VCI) to convey particular configuration or other identification information about a client.

You can configure the following functions:

- Verify the VCI carried by the option 60 field in client's DHCP packets. When the VCI matches the configured one, the IP address and corresponding information will be offered.
- Set the VCI carried by the option 60 for the DHCP server.

Verifying VCI Carried by Option 60

The DHCP server can verify the VCI carried by option 60 in the client's DHCP packets. When the VCI in client's DHCP packet matches the VCI matching string you configured in the DHCP server, DHCP server will offer the IP address and other corresponding information. If not, DHCP server will drop client's DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60. To configure the VCI matching string, use the following command in the DHCP server configuration mode:

vci-match-string {**ascii** *value*| **hex** *value*}

- **ascii** *value* – Specify the VCI matching string in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* – Specify the VCI matching string in hex.

In each specified DHCP server configuration mode, you can only set one VCI matching string. The newly configured VCI matching string will replace the previous one.

To cancel the VCI matching string settings, use the **no vci-match-string** command.

Configuring the VCI Carried by Option 60 for DHCP Server

After configuring the VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI. To configure the VCI carried by option 60 for DHCP server, use the following command in the DHCP server configuration mode:

option 60 {**ascii** *value*| **hex** *value*}

- **ascii** *value* – Specify the VCI in ASCII. If the string contains spaces, it must be enclosed in quotes.
- **hex** *value* – Specify the VCI in hex.

To cancel the option 60 settings, use the **no option 60** command.

Configuring Option 66

The option 66 is used to configure the TFTP server name option. By configuring Option 66, the DHCP client get the domain name or the IP address of the TFTP server. You can download the startup file specified in the Option 67 from the TFTP server.

To configure option 66, in the DHCP server configuration mode, use the following command:

option 66 {**ascii** *string* | **hex** *value*}

- **ascii** *string* – Specify the domain name or the IP address of the TFTP server in ASCII. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.
- **hex** *value* – Specify the domain name or the IP address of the TFTP server in hex.

To cancel the option 66 configurations, in the DHCP server configuration mode, use the command **no option 66**.



Notes: The TFTP server name must start with a letter or number, and cannot end with ” .” (dot). The "-" (hyphen) and"." (dot) cannot appeare continuously.

Configuring Option 67

The option 67 is used to configure the startup file name option for the TFTP server. By configuring option 67, the DHCP client can get the name of the startup file.

To configure option 67, in the DHCP server configuration mode, use the following command:

option 67 {**ascii** *string* | **hex** *value*}

- **ascii** *string* – Specify the startup file name in ASCII. The length is 1 to 255 characters.
- **hex** *value* – Specify the startup file name in hex.

To cancel the option 67 configurations, in the DHCP server configuration mode, use the command **no option 67**.

Configuring Option 138

The Control And Provisioning of Wireless Access Points Protocol (CAPWAP) allows a Wireless Termination Point (WTP) to use DHCP to discover the Access Controllers (AC) to which it is to connect.

The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list.

If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will not offer the option 138 settings.

To add an AC IP address into the list carried by option 138, use the following command in the DHCP server configuration mode:

option 138 ip *A.B.C.D*

- *A.B.C.D* – Specify the IP address of the AC.

Repeat this command to add multiple ACs. Each DHCP server supports up to 4 ACs.

To cancel the specified AC, use the **no optioin 138 ip** *A.B.C.D* command.

Configuring Option 150

The option 150 is used to configure the address options for the TFTP server. By configuring option 150, the DHCP client can get the address of the TFTP server.

To configure option 150, in the DHCP server configuration mode, use the following command:

option 150 ip *ip-address*

- *ip-address* – Specify the IP address of the TFTP server. You can configure up to 8 TFTP servers.

To cancel the option 150 configurations, in the DHCP server configuration mode, use the command **no option 150 ip** *ip-address*.

Configuring Option 242

The option 242 is a private DHCP private option for IP phones. By configuring option 242, the specific parameters information of IP phone can be exchanged between DHCP server and DHCP client, such as call server address (MCIPADD), call the server port (MCPORT), the address of the TLS server (TLSSRVR), HTTP (HTTPSRVR) HTTP server address and server port (HTTPPORT) etc.

To configure option 242, in the DHCP server configuration mode, use the following command:

option 242 {**ascii** *string* | **hex** *value*}

- **ascii** *string* – Specify the specific parameters of the IP phone in ASCII. The length is 1 to 255 characters.
- **hex** *value* – Specify the specific parameters of the IP phone in hex.

To cancel the option 242 configurations, in the DHCP server configuration mode, use the command **no option 242**.

Viewing DHCP Configuration Information

To view the DHCP address pool binding information or statistics, use one of the following commands:

show dhcp-server {**binding** | **pool** | **statistics**} *pool-name*

- **binding** *pool-name* – Shows the binding information of the specified address pool.
- **statistics** *pool-name* – Shows the statistics of the specified address pool.
- **pool** *pool-name* – Shows the information of the specified address pool.

Configuring a DHCP Relay Proxy

The Hillstone device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client. The DHCP relay proxy should be configured in the interface configuration mode. The configurations include:

- Specifying the IP address of the DHCP server
- Enabling DHCP relay proxy on an interface



Notes: To ensure that clients can successfully obtain IP addresses, the administrator needs to configure DHCP relay permit policies in the direction from the DHCP server to clients.

Specifying the IP Address of the DHCP Server

To specify the IP address of the DHCP server, in the interface configuration mode, use the following command:

dhcp-relay server *ip-address*

- *ip-address* – Specifies the IP address of the DHCP server.

To cancel the specified IP address, in the interface configuration mode, use the command **no dhcp-relay server** *ip-address*.

Enabling DHCP Relay Proxy on an Interface

To enable DHCP relay proxy on an interface, in the interface configuration mode, use the following command:

dhcp-relay enable

To disable the specified DHCP relay proxy, in the interface configuration mode, use the command **no dhcp-relay enable**.

Enabling the Function of Replacing the Source IP of the DHCP Relay Packets

In the scenario where the device acts as a DHCP relay proxy, when the device forwards requests to the DHCP server, by default, it uses the IP address of the egress interface as the source IP of the DHCP relay packets, whose source port is 68. However, in specific configurations where strict security policies are applied, packets returned by the DHCP server may be dropped by the device. To avoid this type of packet loss, you can enable this function. This way, the source IP of the DHCP relay packets is replaced with the IP address of the interface on which the DHCP relay proxy is enabled. The source port of the packets is changed to 67.

To enable the function of replacing the source IP address of the DHCP relay packets, in the global configuration mode, use the following command:

dhcp-relay source-ip agent-ip

To restore to the default configuration, use the following command:

no dhcp-relay source-ip agent-ip

PPPoE

PPPoE, the abbreviation for Point-to-Point Protocol over Ethernet, combines PPP protocol and Ethernet to implement access control, authentication and accounting on clients during IP address allocation.

The implementation of PPPoE protocol consists of two stages: discovery stage and PPP session stage.

- Discovery stage: The client discovers the access concentrator by identifying the Ethernet MAC address of the access concentrator and establishing a PPPoE session ID.
- PPP session stage: The client and the access concentrator negotiate over PPP. The negotiation procedure is the same with that of a standard PPP negotiation.

Hillstone devices' interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

Hillstone devices allow you to configure multiple PPPoE instances, and then bind the configured PPPoE instances to interfaces. If an interface is configured to obtain its IP address via PPPoE, the interface will launch a PPPoE connection based on the parameters configured in PPPoE instances. The PPPoE configurations include:

- Configuring a PPPoE instance
- Binding the PPPoE instance to an interface
- Obtaining an IP address via PPPoE
- Manually Connecting or Disconnecting PPPoE
- Viewing PPPoE configuration

Configuring a PPPoE Instance

You can configure various PPPoE parameters in the PPPoE instance, including access concentrator, authentication method, PPPoE connection method, netmask, route distance and weight, service, static IP, PPPoE user information, schedule and DNS preference. The PPPoE instances must be configured in the PPPoE instance configuration mode. To enter the PPPoE instance configuration mode, in the global configuration mode, use the following command:

pppoe-client group *group-name*

- *group-name* – Specifies the name of the PPPoE instance. After executing the command, the system will create a new PPPoE instance, and enter the instance configuration mode; if the specified name exists, the system will enter the instance configuration mode directly.

To delete the specified PPPoE instance, in the global configuration mode, use the command **no pppoe-client group** *group-name*.

Specifying the Access Concentrator

To use PPPoE connections, you need to specify the access concentrator first. To specify the access concentrator, in the instance configuration mode, use the following command:

ac *ac-name*

- *ac-name* - Specifies the name of the concentrator.

To cancel the specified access concentrator, in the instance configuration mode, use the command **no ac**.

Specifying the Authentication Method

Hillstone devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and any. The configured authentication must be the same with that configured in the PPPoE server. To specify the authentication method, in the instance configuration mode, use the following command:

authentication {**chap** | **pap** | **any**}

- **chap** - Specifies the authentication as CHAP.
- **pap** - Specifies the authentication as PAP.
- **any** - Specifies the authentication as either CHAP or PAP. This is the default option.

To restore to the default authentication method, in the instance configuration mode, use the command **no authentication**.

Configuring a PPPoE Connection Method

PPPoE supports two connection methods:

- Automatic connection: If the PPPoE connection has been disconnected due to any reasons for a certain period, i.e., the specified re-connect interval, StoneOS will try to re-connect automatically.
- On-demand dial-up: If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, StoneOS will disconnect the Internet connection; if the interface requires Internet access, StoneOS will connect to Internet automatically.

The above two methods are mutually exclusive, you are not recommended to use these two methods at the same time. When the schedule is not configured, the system will select the automatic connection by default.

To specify the re-connect interval, in the instance configuration mode, use the following command:

auto-connect *time-value*

- *time-value* - Specifies the re-connect interval. The value range is 0 to 10000 seconds. The default value is 10, which means the function is disabled.

To restore to the default re-connect interval, in the instance configuration mode, use the command **no auto-connect**.

To specify the idle interval, in the instance configuration mode, use the following command:

idle-interval *time-value*

- *time-value* - Specifies the idle interval. The value range is 0 to 10000 minutes. The default value is 0.

To restore to the default idle interval, in the instance configuration mode, use the command **no idle-interval**.

Specifying the Netmask

You can specify the netmask for the IP address obtained via PPPoE. To specify the netmask, in the instance configuration mode, use the following command:

netmask *netmask*

- *netmask* - Specifies the network mask, such as 255.255.255.0.

To cancel the specified netmask, in the instance configuration mode, use the command **no net-mask**. After that the system will used the default netmask 255.255.255.255.

Specifying the Route Distance/Weight

To specify the route distance and weight, in the instance configuration mode, use the following command:

route {**distance** *value*| **weight** *value*}

- **distance** *value* – Specifies the route distance. The value range is 1 to 255. The default value is 1.
- **weight** *value* – Specifies the route weight. The value range is 1 to 255. The default value is 1.

To restore to the default route distance and weight, in the instance configuration mode, use the command **no route** {**distance** | **weight**}.

Specifying the Service

To specify the allowed service, in the instance configuration mode, use the following command:

service *service-name*

- *service-name* – Specifies the allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone devices will accept any service returned from the server automatically.

To cancel the specified service, in the instance configuration mode, use the command **no service**.

Specifying the Static IP

You can specify a static IP address and negotiate to use this address to avoid IP change. To specify the static IP address, in the instance configuration mode, use the following command:

static-ip *ip-address*

- *ip-address* – Specifies the static IP address.

To cancel the specified static IP address, in the instance configuration mode, use the command **no static-ip**.

Specifying the PPPoE User Information

To specify the PPPoE user information, in the instance configuration mode, use the following command:

user *user-name* **password** *password*

- *user-name* – Specifies the PPPoE username.
- *password* – Specifies the corresponding password.

To cancel the specified PPPoE user information, in the instance configuration mode, use the command **no user**.

Configuring the Schedule

Hillstone devices support schedules. You can specify a schedule for the PPPoE instance to make the PPPoE interface maintain the Internet connection or disconnect from the Internet during the specified period. To configure the schedule, in the instance configuration mode, use the following command:

schedule *schedule-name* [**disconnect** | **sch-auto-connection** *time-value* | **sch-idle-timeout** *time-value*]

- *schedule-name* – Specifies the name of the schedule.
- **disconnect** – If this keyword is selected, the system will disconnect PPPoE connection during the specified period.
- **sch-auto-connection** *time-value* – If this keyword is selected, the system will connect to the Internet during the specified period automatically. *time-value* is used to specify the re-connect interval. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
- **sch-idle-timeout** *time-value* – If this keyword is selected, the system will dial up to the Internet on demand during the specified period. *time-value* is used to specify the idle interval. The value range is 0 to 10000 minutes. The default value is 30.

To cancel the specified schedule, in the instance configuration mode, use the command **no schedule**.



Tip: For more information about how to create a schedule, see Creating a Schedule of System Management.

Specifying the MAC Address of the PPPoE Server

If the MAC address of the PPPoE server is known, you can specify the MAC address of the PPPoE server so that the Hillstone device can quickly connect to the PPPoE server. To specify the MAC address of the PPPoE server, in the instance configuration mode, use the following command:

mac *mac-address*

- *mac-address* – Specifies the MAC address of the PPPoE server.

To cancel the specified MAC address, in the instance configuration mode, use the command **no mac**.

Configuring Connection Status Detection

To detect the status of the PPPoE connection, you can enable the device to send a LCP Echo request to the PPPoE server. If the device has not yet received response to the request from the PPPoE server after timeout, it will send the request once again; if the retry times reach the specified number, and the device still did not receive any response, then the system will determine the PPPoE server is disconnected, and identify the status of the PPPoE interface as disconnected.

To configure the timeout, in the instance configuration mode, use the following command:

ppp lcp-echo-timeout *timeout-value*

- *timeout-value* – Specifies the timeout value. The value range is 1 to 1000 seconds. The default value is 180.

To restore to the default timeout, in the instance configuration mode, use the following command:

no ppp lcp-echo-timeout

To configure the retry times, in the instance configuration mode, use the following command:

ppp lcp-echo-retries *times*

- *times* – Specifies the retry times. The value range is 1 to 30. The default value is 10.

To restore to the default retry times, in the instance configuration mode, use the following command:

no ppp lcp-echo-retries

Obtaining an IP Address via PPPoE

To enable the interface to obtain an IP address via PPPoE, in the interface configuration mode, use the following command:

ip address pppoe [**setroute**]

- **setroute** – Uses the gateway specified by the PPPoE server as the default route gateway.

To cancel the configuration, in the interface configuration mode, use the command **no ip address pppoe**.

Binding a PPPoE Instance to an Interface

After binding the configured PPPoE instance to an interface, the interface will adopt the parameters of the instance to establish PPPoE connections. To bind the PPPoE instance to an interface, in the interface configuration mode, use the following command:

pppoe enable group *group-name*

- *group-name* – Specifies the name of the PPPoE instance.

To cancel the specified binding, in the interface configuration mode, use the command **no pppoe enable group**.

Manually Connecting or Disconnecting PPPoE

To connect to or disconnect from the PPPoE, in the global configuration mode, use the following command:

pppoe-client group *group-name* {**connect** | **disconnect**}

- *group-name* – Specifies the name of the PPPoE instance.
- **connect** – Connects to PPPoE.
- **disconnect** – Disconnects from PPPoE.

Viewing PPPoE Configuration Information

To view the PPPoE instance parameter information and the connection status, in any mode, use the following command:

show pppoe-client {**all** | **group** *group-name*}

- **all** – Shows the information of all the PPPoE instances.
- **group** *group-name* – Shows the information of the specified PPPoE instance.

Example of Configuring PPPoE

This section describes a typical PPPoE configuration example.

Requirement

The Hillstone device acts as the PPPoE and sends requests to the PPPoE server; the PPPoE server returns response to the client.

Configuration Steps

Step 1: Create a PPPoE instance named pppoe1 and specify the parameters

```
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
hostname(config-pppoe-group)# idle-interval 5
hostname(config-pppoe-group)# route distance 2
hostname(config-pppoe-group)# route weight 10
hostname(config-pppoe-group)# authentication any
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

Step 2: Enable ethernet0/3 to obtain its IP address via PPPoE, and bind the PPPoE instance to ethernet0/3

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address pppoe setroute
hostname(config-if-eth0/3)# pppoe enable group pppoe1
```

```
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Create a schedule named schedule1, and enable ethernet0/3 to launch PPPoE connections via on-demand dial-up from 9:00 to 15:30 everyday. The idle time of the on-demand dial-up is 20 minutes

```
hostname(config)# schedule schedule1
hostname(config-schedule)# absolute start 10/15/2007 09:30 end 11/05/2007 15:00
hostname(config-schedule)# periodic daily 09:00 to 15:30
hostname(config-schedule)# exit
hostname(config)# pppoe-client group pppoe1
hostname (config-pppoe-group)# schedule schedule1 sch-idle-timeout 20
hostname (config-pppoe-group)# exit
hostname(config)#
```

NAT

Overview

NAT (Network Address Translation) is a protocol for IP address translation in an IP packet header. When the IP packets pass through a firewall or router, the device or router will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, or vice versa. NAT has the following advantages:

- Helps to solve the problem of IP address resources exhaustion by using a small number of public IP addresses to represent the majority of the private IP addresses.
- Hides the private network from external networks, for the purpose of protecting private networks.

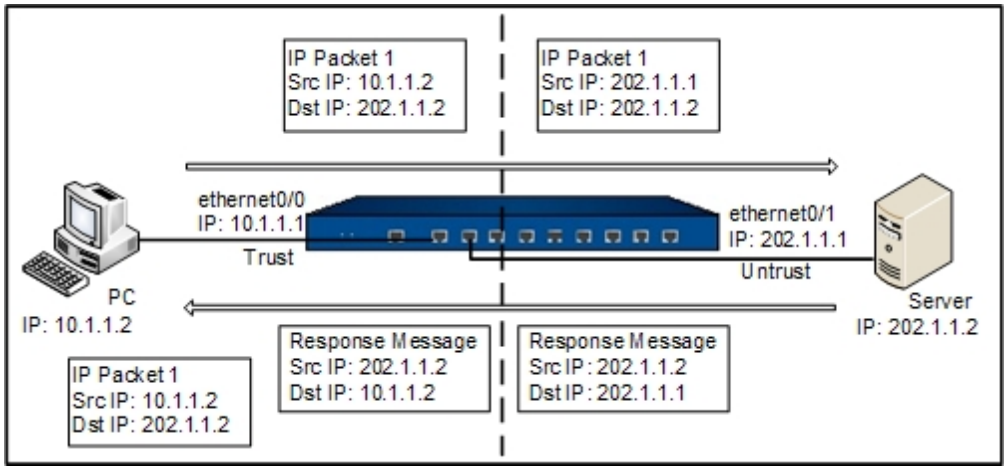
Typically private networks use private IP addresses. RFC1918 defines three types of private IP addresses as follows:

- Class A: 10.0.0.0 - 10.255.255.255 (10.0.0.0 / 8)
- Class B: 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
- Class C: 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

IP addresses in the above three ranges will not be allocated on the Internet. You can use those IP addresses in an enterprise network freely without requesting them from an ISP (Internet Service Provider) or registration center.

Basic Translation Process

When a firewall is implementing the NAT function, it locates between the public network and the private network. Figure below illustrates the basic translation process of NAT.



As shown above, the firewall lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the firewall, the appliance checks the packet header. Finding that the IP packet is destined to the public network, the appliance translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the appliance also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the firewall, the appliance checks the packet header again and finds the mapping records in its NAT table, then replaces the destination address with the private address 10.1.1.2. In this process, the firewall is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is 202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

NAT of Hillstone Devices

The NAT function of the Hillstone devices translates the IP address and port number of the internal network host to the external network address and port number of the device, and vice versa. That is translation between the "private IP address + port number" and the "public IP address + port number".

The Hillstone devices achieve the NAT function through the creation and implementation of NAT rules. There are two types of NAT rules, which are source NAT rules (SNAT rules) and destination NAT rules (DNAT rules). SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses; DNAT translates destination IP

addresses, usually translating IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device to public IP addresses.

Limits on Configuring NAT in HA Scenario

When you use the NAT function in HA scenario, take note of the following limits:

- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the same dynamic port (**dynamicport**) SNAT rule, you need to enable the SNAT port distribution function by using the **split-port-pool by ha-node** command. This ensures that ports assigned for the two devices in the HA group are not duplicate.
- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the same dynamic IP (**dynamicip**) SNAT rule, the SNATed IP address may be reused because IP occupation is not synchronized between the devices in the HA group.
- The source or destination address in the NAT rule cannot contain the IP address of the HA link interface (heartbeat interface). This avoids abnormal heartbeat link communication when heartbeat packets are NATed.
- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the SNAT rule that translates the source IP address to Egress IF IP (**eif-ip** or **eif-ipv6**), the two devices in the HA group may behave inconsistently after an HA switchover because their NATed IP addresses may be different.

Configuring a NAT Rule

NAT rules are created based on VRouters. You can create, move and delete SNAT/DNAT rules in the VRouter configuration mode, or configure NAT rules for the default VR trust-vr in the NAT configuration mode (to enter the NAT configuration mode, in global configuration mode, use the command nat).

To enter the VRouter configuration mode, in the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of VRouter.

Creating a BNAT Rule

BNAT can be seen as a combination of DNAT and SNAT, which uses just one rule to achieve both source and destination translation.

In the packet processing flow, BNAT has precedence over DNAT. When a packet matches a BNAT rule, it follows the destination translation and source translation defined in that BNAT rule. It will not check for other regular NAT rules. After it finishes BNAT mapping, it will start to match policy.

To create a BNAT rule, under VRouter configuration mode, use the command below:

bnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] [**interface** *interface-name*] [**zone** *zone-name*] **virtual** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } **real** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } [**group** *group-id*] [**description** *description*][**schedule***schedule-name*]

- **id** *id* – Specifies an ID for this BNAT rule. Each BNAT has its unique ID. If you skip entering ID for it, the system will assign an ID number automatically. If you specify an existing ID, the new rule will replace the existing rule.
- **before***id* | **after***id* | **top** – Specifies the position of the rule. The position can be top, before id or after id. If the position is not specified, the rule would be located at the end of all the BNAT rules. By default, the newly-created BNAT rule is located at the end of all the rules.
- **interface***interface-name* – Specifies the external interface for Internet users to visit.
- **zone***zone-name* – Specifies the security zone to which the interface provided for Internet user access is bound. After the configuration is completed, only the traffic that flows through the interface bound to this security zone can continue to match the BNAT rule. By default, the parameter is set to **Any**.

  Note:

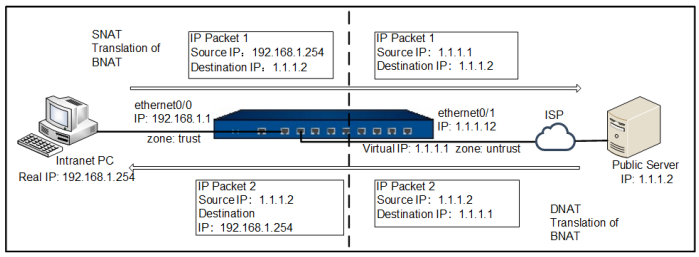
- The security zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
- Only one security zone can be configured for a BNAT rule.

- **virtual** {**ip** { *A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } – Specifies the external IP address for Internet users to visit. This is normmaly 1-to-1 mapping. If the address is an address book or range, you should make sure the virtual address has the same the number of the real addresses. The mapping order is from top to bottom.
  Note: Netmask must be specified. An IP address without netmask is not supported. If an IPv4 address is specified, the range of the netmask is from 0 to 32. If an IPv6 address is specified, the range of the IPv6 prefix is from 48 to 128. If an address book is specified, the number of IPv4 virtual addresses cannot exceed 2^{32} while the number of IPv6 virtual addresses cannot exceed 2^{80}.
- **real** {**ip** {*A.B.C.D/M* | *X:X:X:X:X::X/M*} | **address-book** *address-name* } - Specifies the real internal address. This address is invisible to Internet users, and it is the real Intranet address of the server.
  Note: Netmask must be specified. An IP address without netmask is not supported. If an IPv4 address is specified, the range of the netmask is from 0 to 32. If an IPv6 address is specified, the range of the IPv6 prefix is from 48 to 128. If an address book is specified, the number of IPv4 virtual addresses cannot exceed 2^{32} while the number of IPv6 virtual addresses cannot exceed 2^{80}.
- **group** *group-id* - Specifies the HA group the BNAT rule belongs to. If the parameter is not specified, the BNAT rule being created will belong to HA group0.
- **description** *description* – Specifies the description for this BNAT rule. You can specify at most 63 characters.
- **schedule***schedule-name* – Specifies the schedule for the BNAT rule.

To delete a BNAT rule, use the following command:

no bnatrule id *id*

For example, you can use the following command to implement BNAT translation. If Internet traffic accesses the internal network, when the traffic matches the BNAT rule based on the security zone to which the interface provided for Internet user access is bound, the traffic will be DNATed. If traffic over the internal network accesses the Internet, when the traffic matches the BNAT rule based on the security zone to which the interface provided for Internet user access is bound, the traffic will be SNATed.



hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **bnatrule interface ethernet0/1 zone untrust virtual ip 1.1.1.1/32 real ip 192.168.1.254/32**

(ethernet0/1 is the interface provided for Internet user access, untrust is the security zone to which the preceding interface is bound, 1.1.1.1/32 is the public IP address provided for Internet user access, and 192.168.1.254/32 is the real internal address of the intranet PC.

(DNAT translation of BNAT: If Internet traffic accesses the internal network from 1.1.1.2 to 1.1.1.1, when the traffic matches the BNAT rule, the traffic will be DNATed. To be specific, the destination address is converted to 192.168.1.254 and the source address remains unchanged.)

(SNAT translation of BNAT: If traffic over the internal network accesses the Internet from 192.168.1.254 to 1.1.1.2, when the traffic matches the BNAT rule, the traffic will be SNATed. To be specific, the source address is converted to 1.1.1.1 and the destination address remains unchanged.

```
rule ID=1
```

Moving an BNAT Rule

You can move an BNAT rule to modify the matching sequence. To move an BNAT rule, in the VRouter configuration mode, use the following command:

bnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the BNAT rule that will be moved.
- **before** *id* – Moves the BNAT rule before the specified ID.
- **after** *id* – Moves the BNAT rule after the specified ID.
- **top** – Moves the BNAT rule to the top of the BNAT rule list.
- **bottom** – Moves the BNAT rule to the bottom of the BNAT rule list.

Specifying a Schedule for a BNAT Rule

You can associate an existing BNAT rule with a schedule or modify the schedule for a BNAT rule. To specify a schedule for a BNAT rule, use the following command in VRouter configuration mode/NAT configuration mode:

bnatrule id*id***schedule***schedule-name*

- *id* – Specifies the ID of the BNAT rule that needs to reference a schedule.
- *schedule-name* – Specifies the schedule for the BNAT rule.

In VRouter configuration mode/NAT configuration mode, use the **no bnatrule id***id***schedule** command to delete the schedule from a specified BNAT rule.

Viewing BNAT Configuration Information

After BNAT is configured, to view BNAT configuration information in the system, in any mode, use the following command:

show bnat [**id***id* | **vrouter***vrouter-name*]

- **id** *id* – Shows the BNAT rule information of a specified ID.
- **vrouter** *vrouter-name* – Shows the BNAT rule information of a specified VRouter. If not specified, the system displays the BNAT rule of the default VRouter (trust-vr).

Example:

```
hostname(config)# show bnat
------------------------------------------------------------
--------------
vr name:trust-vr
bnat rules total number is :1 (shows the total number of
BNAT rules within the VRouter trust-vr)
============================================================
==============
id interface virtual-address real-address(shows the con-
figuration information of the BNAT rule)
------------------------------------------------------------
--------------
123 ethernet0/1 1.1.1.1/32 192.168.1.254/32
zone: untrust
============================================================
==============
```

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT on the source IP address of the matched traffic. If NAT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before***id* | **after***id* | **top**] [**ingress-interface** *interface-name*] [**from-zone** zone-name] [**to-zone** zone-name] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-*

interface | **evr** *vrouter-name*] **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**] | **nptv6**} [**log**] [**group** *group-id*] [**disable**] [**track** *track-name*] [**description** *description*][**schedule***schedule-name*]

- **id** *id* – Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be top, before id or after id. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.
- **ingress-interface** *interface-name* – Specifies the ingress interface of the SNAT rule. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, and traffic from other interfaces will not.
- **from-zone***zone-name* – Specifies the security zone to which the ingress interface of traffic that matches the SNAT rule is bound. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the SNAT rule. By default, the parameter is set to **Any**.

  Note:

  - The source zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
  - Only one source zone can be configured for an SNAT rule.
- **to-zone***zone-name* – Specifies the security zone to which the egress interface of traffic that matches the SNAT rule is bound. After the configuration is completed, only the traffic that flows through the interface bound to this security zone can continue to match the SNAT rule. By default, the parameter is set to **Any**.

  Note:

- The destination zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
- Only one destination zone can be configured for an SNAT rule.

- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions include:
  - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book(IPv4 type or IPv6 type).
  - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book (IPv4 type or IPv6 type).
  - **service** *service-name* – Specifies the service type of the traffic. *service-name* should be a service defined in the service book.
  - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.
- **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip** | **eif-ipv6**} – Specifies the translated IP address. It can be an ipv4 address, IPv6 address, an address entry in the address book or the address of the egress interface (**eif-ip** or **eif-ipv6**).
- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** |**round-robin**] | **nptv6**} – Specifies the translation mode. StoneOS supports four translation modes: static, dynamicip, dynamicport, and nptv6. For more details, see the table below:

Mode	Description
static	Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same num-

Mode	Description
	ber of IP addresses as that of the source address entry (*src-address*). **Notes:** When configuring a static source NAT66 rule, the minimum subnet mask must be 48 bits.
dynamicip	Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
dynamicport	Namely PAT. Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. If Round-robin, all sessions from an IP address will be polled to map the IP address. If Sticky and Round-robin are not enabled, the system will select an IP address in the address entry, when port resources of the first address are exhausted, the second address will be used. **Note**: Sticky function and Round-robin function are mutually exclusive and cannot be configured at the same time.
nptv6	NPTv6 (IPv6-to-IPv6 Network Prefix Translation) is described in RFC 6296 and used to implement NAT66. When this mode is selected, NPTv6 can translate an inside IPv6 source address prefix to outside IPv6 source prefix in IPv6 packet header. The translation is based on the algorithm described in RFC 6296, which serves as a useful mechanism for implementing address independence. This mode supports a larger number of address translation and reduces resource consumption by using quick

Mode	Description

	address mapping.
	 Notes:
	• The NPTv6 mode is available only when the Type parameter is set to IPv6 and the Translated parameter is set to Specified IP.
	• The NPTv6 mode requires that both the source address of the traffic and the translated address are either "IPv6/prefix" or address from address book.
	  • If the source address of the traffic and the translated address are "IPv6/prefix", the IPv6 prefix needs to be 8 to 64 in length.
	  • If the source address of the traffic and the translated address are address from address book, you can only configure one IPv6 subnet mask member whose subnet mask is 8 to 64 in length.

- **log** – Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule). **Note**: If the translated NAT IP address is an egress interface IP address (**`eif-ip`** or **eif-ipv6**), it is necessary to specify the egress interface of the traffic (**eif** *egress-interface*) at the same time in order to generate logging information.

- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.
- **disable** – Enter this command to disable the SNAT rule.
- **track** *track-name* – Specifies a track object name that is configured in the system. After configuring this option, the system will track whether the translated public address is valid. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see Configuring a Track Object of System Management. This function only supports dynamicport mode, and the translated address should be an IP address or an address in address book (i.e., **trans-to address book** *trans-to-address*). The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log.
- **description** *description* – Specifies the description for this SNAT rule. You can specify at most 63 characters.
- **schedule***schedule-name* – Specifies the schedule for the SNAT rule.

For example, you can use the following command to implement SNAT translation. If traffic over the internal network accesses the Internet, the traffic will be SNATed based on the security zone to which the ingress interface of the traffic is bound and the security zone to which the egress interface of the traffic is bound.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from-zone trust to-zone untrust from ip
192.168.2.23 to 1.1.12.3 trans-to ip 1.1.10.6 mode static
 (trust is the security zone to which the ingress interface of traffic that
```

```
matches the SNAT rule is bound, untrust is the security zone to which the egress interface of traffic that matches the SNAT rule is bound, 192.168.2.23 is the source IP address, 1.1.12.3 is the destination IP address, and 1.1.10.6 is the SNATed source IP address.)
 (SNAT translation: If traffic over the internal network accesses the Internet from 192.168.2.23 to 1.1.12.3, when the traffic matches the SNAT rule, the source address is converted to 1.1.10.6 and the destination address remains unchanged.)
snat service not set, set to default Any
rule ID=1
```

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT, in the NAT configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*] [**description** *description*]

Enabling/Disabling SNAT Rule

To enable or disable an SNAT rule, under NAT configuration mode, use the following command:

snatrule id *id* [**enable** | **disable**]

- **enable** – Enable an SNAT rule of the specified ID.
- **disable** – Disable an SNAT rule of the specified ID.

Moving an SNAT Rule

Each SNAT rule is labeled with a unique ID. When traffic flows into the Hillstone device, the device will query for SNAT rules in the list by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command **show snat** is the query sequence for the matching. You can move an SNAT rule to modify the matching sequence. To move an SNAT rule, in the NAT configuration mode, use the following command:

snatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the SNAT rule that will be moved.
- **before** *id* – Moves the SNAT rule before the specified ID.
- **after** *id* – Moves the SNAT rule after the specified ID.
- **top** – Moves the SNAT rule to the top of the SNAT rule list.
- **bottom** – Moves the SNAT rule to the bottom of the SNAT rule list.

Enabling/Disabling Expanded PAT Port Pool

When the translation mode of SNAT is set to dynamicport, you can enable or disable the expanded PAT port pool to expand the network address port resources after NAT. This function is disabled by default. To enable the function, in the global configuration mode, use the following command:

expanded-port-pool

To disable the function, in the global configuration mode, use the following command:

no expanded-port-pool



Notes:

- Only some of Hillstone models support the expanded PAT port pool, and the supported port resources also vary from different platforms.



- The function is only applicable to the SNAT rules that have not been enabled yet; if the SNAT rule is already enabled, reboot the system to make the function take effect.

The function is only applicable to the SNAT rules that have not been enabled yet; if the SNAT rule is already enabled, reboot the system to make the function take effect.

Enabling/Disabling the Function of Expanding Translated IP Address Range

When SNAT/BNAT (DNAT with the source address translation function enabled) is in dynamic port mode, you can enable the function of expanding the range of translated IP addresses. After this function is enabled, when you configure an SNAT/BNAT rule, the system no longer restricts the number of translated IP addresses. The number of translated IP addresses that are actually effective is determined by the device capacity. By default, this function is disabled. To enable/disable this function, use the following command:

snat-trans-expension {**enable** | **disable**}

- **enable** – Enable the function of expanding translated IP address range.
- **disable** – Disable the function of expanding translated IP address range.



Notes:

- You cannot configure this function and the NAT444 function at the same time.
- Before you disable this function, make sure that all SNAT/BNAT rules whose number of translated IP addresses exceeds the device capacity are deleted.

Checking Whether the Function of Expanding Translated IP Address Range is Enabled

To check whether the function of expanding translated IP address range is enabled, in global configuration mode, use the following command:

show snat-trans-expension

Deleting an SNAT Rule

To delete the SNAT rule with the specified ID, in the NAT configuration mode, use the following command:

no snatrule id *id*

Modifying/Deleting the Descriptions of a SNAT Rule

In the NAT configuration mode, use the following command to modify the description of a specific SNAT rule:

snatrule id *id* **description** *description*

- *id* – Specifies the ID of the SNAT rule whose description you want to modify.
- **description** *description* – Specifies the new description. You can enter at most 64 characters.

In the NAT configuration mode, use the following command to delete the description of a specific SNAT rule:

no snatrule id *id* **description**

Specifying a Schedule for an SNAT Rule

You can associate an existing SNAT rule with a schedule or modify the schedule for an SNAT rule. To specify a schedule for an SNAT rule, use the following command in VRouter configuration mode/NAT configuration mode:

snatrule id*id***schedule***schedule-name*

- *id* – Specifies the ID of the SNAT rule that needs to reference a schedule.
- *schedule-name* – Specifies the schedule for the SNAT rule.

In VRouter configuration mode/NAT configuration mode, use the **no snatrule id***id***schedule** command to delete the schedule from a specified SNAT rule.

Configuring the SNAT Rule Port Resource Monitor Function

The system can monitor the usage of a SNAT rule IP address's port resource usage and record logs based on the configuration. This function is disabled by default.

To enable the monitor of SNAT rules' port resource usage, in the global configuration mode, use the following command:

monitor-snat-port-resource rising-threshold *threshold-value* **sample-period** *period-value*

- **rising-threshold** *threshold-value* - Specifies the rising threshold. When the current port resource usage exceeds the percentage threshold specified by this parameter, the system will record a warning log. The value range is 1 to 99.
- **sample-period** *period-value* - Specifies the report period. The value range is 900 to 3600 seconds.

To disable the monitor of SNAT rules' port resource usage, in the global configuration mode, use the following command:

no monitor-snat-port-resource

Viewing the SNAT Rule Port Usage Monitor Function Configuration

To view the SNAT rule port usage monitor function configuration, in the global configuration mode, use the following command:

show monitor-snat-port-resource

Viewing SNAT Configuration Information

To view the SNAT configuration information, in any mode, use the following command:

show snat [**id** *id* | **vrouter** *vrouter-name*]

show snat [**vrouter** *vrouter-name*] [**src** *src-address*] [**dst** *dst-address*] [**service** *service-name*] [**trans-to** *trans-to-address*] [**description** *description*]

- *id* – Shows the SNAT rule information of the specified ID.
- **vrouter** *vrouter-name* – Shows the SNAT configuration information of the specified VRouter. If this parameter is not specified, the system will show the SNAT rule information of the default VRouter (trust-vr).
- **src** *src-address* – Shows the SNAT configuration information of the specified source address.
- **dst** *dst-address* - Shows the SNAT configuration information of the specified destination address.
- **service** *service-name* – Shows the SNAT configuration information of the specified service.
- **trans-to** *trans-to-address* - Shows the SNAT configuration information of the specified translated IP.
- **description** *description* – Shows the SNAT configuration information of the specified description.

Viewing SNAT Source Utilization

To view the source utilization information, in any mode, use the following command:

show snat id *id* **resource** [**ip** *A.B.C.D*] [**detail**]

show snat resource [**vrouter** *vrouter-name*] [**ip** *A.B.C.D*] [**detail**]

- **resource** – When the translation mode of SNAT is set to dynamicport, this parameter is used to show the source utilization of the source port address pool.
    - **ip** – Shows the port resource ultilization of the specified IP in the translation address pool.

- **detail** - Shows the detail information of port resource ultilization of the translation address pool. Such as the allocated state, translation mode and port range.

Viewing Tracked Failed Information of SNAT Translated Address

To view the tracked failed information of SNAT translated address, in any mode, use the following command:

show snat track-failedslot*slot-number* [**vrouter***vrouter-name*][**ip** *A.B.C.D* [**detail**] | **detail**]

show snattrack-failed [**vrouter***vrouter-name*]

show snattrack-failedcpu*cpu-numb*

- **track-failed** – Displays the tracked failed information of SNAT translated address.
- **vrouter** *vrouter-name* – Dispalys the tracked failed SNAT translated address of the specified VRouter. If this parameter is not specified, the system will display the information of the default VRouter (trust-vr).
- **slot** *slot-number* – Dispalys the tracked failed SNAT translated address of the specified slot.
- **cpu** *cpu-number* – Dispalys the tracked failed SNAT translated address of the specified CPU.

Viewing SNAT Rule Hit Counts

To facilitate users' management and maintenance of SNAT rules, the system supports statistics on SNAT rule hit counts. This feature counts how many times the traffic matches a SNAT rule. Every time the inbound traffic matches a specific SNAT rule, the hit count of that SNAT rule automatically increases by 1. You can view statistics on SNAT rule hit counts with the following command in any mode:

show snat hit-count vrouter *vr-name* {**id** *id* | **top** {10 | 20 | 50 | **all**}}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **id** *id* - Shows the hit counts statistics of the SNAT rule whose ID is the specified ID.

- **top** {**10** | **20** | **50** | **all**} - Shows the hit count statistics of the top 10, 20, 50 matched SNAT rules , or shows the hit count statistics of all SNAT rules (**all**).

Viewing Statistics on SNAT Rule Hits

In any mode, you can use the corresponding show commands to view statistics on SNAT rule hits, including SNAT rule ID, hit counts, first-hit time, last-hit time, days since last-hit time, SNAT rule created time, and SNAT rule status (enabled/disabled).

To view hit statistics of the SNAT rule that belongs to the specified VRouter:

show snat hit-info vrouter*vr-name*

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.

To view hit statistics of the SNAT rule whose ID is the specified ID:

show snat hit-info vrouter *vr-name* **id** *id*

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **id** *id* - Specifies SNAT rule ID.

To view SNAT rules that are never hit by traffic:

show snat hit-info vrouter never-hitted

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.

To view hit statistics of the SNAT rule whose days since created are longer than the specified days:

show snat hit-info vrouter *vr-name* **days-since-created** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the SNAT rule whose days since first hit are longer than the specified days:

show snat hit-info vrouter *vr-name* **days-since-first-hitted** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the SNAT rule whose days since last hit are longer than the specified days:

show snat hit-info vrouter *vr-name* **days-since-last-hitted** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

Use the following command to view hit statistics of the combinedly filtered SNAT rules. The filters include that SNAT rules' days since last hit are longer than the specified days, SNAT rules' days since first hit are longer than the specified days, and SNAT rules' days since created are longer than the specified days.

show snat hit-info vrouter *vr-name* [**days-since-last-hitted** *value*] [**days-since-first-hitted** *value*] [**days-since-created** *value*]

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the SNAT rule whose days since last hit are longer than the specified days.
- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the SNAT rule whose days since first hit are longer than the specified days.
- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the SNAT rule whose days since created are longer than the specified days.

To view hit statistics of all SNAT rules in ascending or descending order of SNAT rule ID:

show snat hit-info vrouter *vr-name* **sorted-by id** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **id** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of SNAT rule ID.

To view hit statistics of all SNAT rules in ascending or descending order of hit counts:

show snat hit-info vrouter *vr-name* **sorted-by hit-count** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **hit-count** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of hit counts.

To view hit statistics of all SNAT rules in ascending or descending order of SNAT rule created time:

show snat hit-info vrouter *vr-name* **sorted-by created-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **created-time** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of SNAT rule created time.

To view hit statistics of all SNAT rules in ascending or descending order of SNAT rule first hit time:

show snat hit-info vrouter *vr-name* **sorted-by first-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **first-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of SNAT rule first hit time.

To view hit statistics of all SNAT rules in ascending or descending order of days since SNAT rule last hit:

show snat hit-info vrouter *vr-name* **sorted-by days-since-last-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **days-since-last-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of days since SNAT rule last hit.

To view hit statistics of all SNAT rules in ascending or descending order of SNAT rule last hit time:

show snat hit-info vrouter *vr-name* **sorted-by last-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **last-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all SNAT rules are displayed in ascending or descending order of SNAT rule last hit time.

Clearing Statistics on SNAT Rule Hits

In any mode, use the following command to clear statistics on SNAT rule hits:

clear snat hit-info vrouter *vr-name* [**id** *id*]

- **vrouter** *vr-name* - Specifies the VRouter to which the SNAT rule belongs.
- **id** *id* - Clear hit statistics of the SNAT rule in specified ID. If no ID is specified, clear hit statistics of all SNAT rules.

Creating a DNAT Rule

DNAT rules are used to specify whether to implement NAT on the destination IP address of the matched traffic. To configure a DNAT rule for NAT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] [**ingress-interface** *interface*] [**from-zone** zone-name] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**port** *port*] [{**redirect** | **load-balance**} [**track-tcp** *port*] [**track-ping**] | **source-trans-to** *source-trans-to-address* **mode** {**dynamicport** | **static**}] [**log**] [**group** *group-id*] [**disable**] [**description** *description*]

- **id** *id* – Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules.
- **ingress-interface** *interface* – Specifies the ingress interface whose traffic will match this dnat rule. When this interface is designated, only the traffic from this interface will continue to match this DNAT rule. Traffic from other interfaces will not.
- **from-zone***zone-name* – Specifies the security zone to which the ingress interface of traffic that matches the DNAT rule is bound. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the DNAT rule. By default, the parameter is set to **Any**.
  Note:
  - The source zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
  - Only one source zone can be configured for a DNAT rule.
- **from** *src-address* **to** *dst-address* [**service** *service-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* – Specifies the source IP address /netmask of the traffic. *src-address* should be an IP address /netmask or an address entry in the address book.
  - **to** *dst-address* – Specifies the destination IP address/netmask of the traffic. *dst-address* should be an IP address /netmask or an address entry in the address book.

- **service** *service-name* – Specifies the service type of the traffic. If the port number needs to be translated together (specified by port port), the specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.

- **trans-to** *trans-to-address* – Specifies the translated IP address. *trans-to-address* is an IP address/netmask or an address entry in the address book. When the number of this translated IP address be different from the destination IP address of the traffic (specified by **to** *dst-address*) or the destination IP address is **any**, you must enable the redirect function for this DNAT rule (specified by **redirect**). If the DNAT rule is enabled with**load-balance**, the number of translated IP addresses can be allowed different from the destination IP address of the traffic, but the destination IP address cannot be **any**.If this translated IP address is an address book entry containing a DNS domain name, you need to enable load-balance for the DNAT rule (specified by load-balance).

- **port** *port* – Specifies port number of the internal network server.

- **redirect** - Enables **redirect** for this DNAT rule, allows the destination IP address of the traffic to be **any**.

- **load-balance** – Enables **load-balance** for this DNAT rule. The system will adopt persistent algorithm to distribute traffic and balance the traffic to different servers in the internal network based on the hash of user IP.

- **track-tcp** *port* – If this parameter is configured and the port number of the internal network server is specified, the system will send TCP packets to the internal network server every 3 seconds to monitor if the specified port is reachable. If no response is returned for 3 packets in succession, the system will conclude the server fails.

- **track-ping** – If this parameter is configured, the system will send Ping packets to the internal network server every 3 seconds to monitor if the server is reachable. If no response is returned for 3 packets in succession, the system will conclude the server fails.
- **source-trans-to** *source-trans-to-address* - Enables the source address translation function (bi-irectional NAT) and specifies the IP address after translation, which can be an address entry in the address book or an IPv4 or IPv6 address/mask.
- **mode** {**dynamicport** | **static**} - Specifies the source address translation mode. The **dynam-icport** mode will translate the multiple source IP and port number to the same NAT address and different port number. If translation fails, the system will select one randomly. The **static** mode means one-to-one translation. This mode requires the number of source IP addresses be the same as that of translated IP addresses.
- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this NAT rule).
- [**group** *group-id*] - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.
- **disable** – Enter this command to disable the DNAT rule.
- **description** *description* – Specifies the description for this DNAT rule. You can specify at most 63 characters.
- **schedule***schedule-name* – Specifies the schedule for the DNAT rule.

For example, you can use the following command to implement DNAT translation. If Internet traffic accesses the internal network, the traffic will be DNATed based on the security zone to which the ingress interface of the traffic is bound.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# dnatrule from-zone untrust from ip 1.1.2.2 to ip 2.2.2.56 trans-to ip 192.168.4.56
```

(untrust is the security zone to which the ingress interface of traffic that matches the DNAT rule is bound, 1.1.2.2 is the source IP address, 2.2.2.56 is the destination IP address, 192.168.4.56 is the DNATed destination IP address.)

(DNAT translation: If Internet traffic accesses the internal network from 1.1.2.2 to 2.2.2.56, when the traffic matches the DNAT rule, the destination address is converted to 192.168.4.56 and the source address remains unchanged.)

dnat service not set, set to default Any

rule ID=2

For example, the following command will translate the IP address of the request from addr1 to the IP address of addr2, but will not translate the port number:

```
hostname(config-vrouter)# dnatrule from any to addr1 service any trans-to addr2
rule id=1
```

To configure a DNAT rule that disables NAT, in the NAT configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*] [**description** *description*]

Enableing/Disabling DNAT Rule

To enable or disable a DNAT rule, under NAT configuration mode, use the following command:

dnatrule id *id* [**enable** | **disable**]

- **enable** – Enable the DNAT rule of the specified ID.
- **disable** – Disable the DNAT rule of the specified ID.

Moving a DNAT Rule

Each DNAT rule is labeled with a unique ID. When traffic flowing into the Hillstone device, the device will query for DNAT rules by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dnat is the query

sequence for the matching. You can move a DNAT rule to modify the matching sequence. To move a DNAT rule, in the NAT configuration mode, use the following command:

dnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the DNAT rule that will be moved.
- **before** *id* – Moves the DNAT rule before the specified ID.
- **after** *id* – Moves the DNAT rule after the specified ID.
- **top** – Moves the DNAT rule to the top of the DNAT rule list.
- **bottom** – Moves the DNAT rule to the bottom of the DNAT rule list.

Modifying/Deleting the Descriptions of a DNAT Rule

In the NAT configuration mode, use the following command to modify the description of a specific DNAT rule:

dnatrule id *id* **description** *description*

- *id* – Specifies the ID of the DNAT rule whose description you want to modify.
- **description** *description* – Specifies the new description. You can enter at most 64 characters.

In the NAT configuration mode, use the following command to delete the description of a specific DNAT rule:

no dnatrule id *id* **description**

Deleting a DNAT Rule

To delete the DNAT rule with the specified ID, in the NAT configuration mode, use the following command:

no dnatrule id *id*

Specifying a Schedule for a DNAT Rule

You can associate an existing DNAT rule with a schedule or modify the schedule for a DNAT rule. To specify a schedule for a DNAT rule, use the following command in VRouter

configuration mode/NAT configuration mode:

dnatrule id*id***schedule***schedule-name*

- *id* − Specifies the ID of the DNAT rule that needs to reference a schedule.
- *schedule-name* − Specifies the schedule for the DNAT rule.

In VRouter configuration mode/NAT configuration mode, use the **no dnatrule id***id***schedule** command to delete the schedule from a specified DNAT rule.

Viewing DNAT Configuration Information

To view the DNAT configuration information, in any mode, use the following command:

show dnat [**id** *id* | **vrouter** *vrouter-name*][**src** *src-address*] [**dst** *dst-address*] [**service** *service-name*] [**trans-to** *trans-to-address*] [**source-trans-to** *source-trans-to-address*] [**trans-port** *port-number*] [**description** *description*]]

- **id** *id* − Shows the DNAT rule information of the specified ID.
- **vrouter** *vrouter-name* − Shows the DNAT configuration information of the specified VRouter. If this parameter is not specified, the system will show the DNAT rule information of the default VRouter (trust-vr).
- **src** *src-address* − Shows the DNAT configuration information of the specified source address.
- **dst** *dst-address* - Shows the DNAT configuration information of the specified destination address.
- **service** *service-name* − Shows the DNAT configuration information of the specified service.
- **trans-to** *trans-to-address* - Shows the DNAT configuration information of the specified translated IP.
- **source-trans-to** *source-trans-to-address* - Shows the DNAT configuration information of the specified source IP address after translation.

- **trans-port** *port-number* - Shows the DNAT configuration information of the specified translated port.
- **description** *description* – Shows the DNAT configuration information of the specified description.

To show the information of the DNAT rule with load balancing configured, in any mode, use the following command:

show load-balance rule [*id*]

- *id* – Shows the DNAT rule information (with load balancing) of the specified ID.

To view the status of the load-balancing server, in any mode, use the following command:

show load-balance server [*ip-address*] [**vrouter** *vrouter-name*]

- *ip-address* – Shows status of the load-balancing server of the specified IP address.
- **vrouter** *vrouter-name* – Shows status of the load-balancing server of the specified VRouter. If this parameter is not specified, the system will show status of the load-balancing server of the default VRouter (trust-vr).

To view the status of the internal network server, in any mode, use the following command:

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – Shows status of the internal network server of the specified IP address.
- **vrouter** *vrouter-name* – Shows status of the internal network server of the specified VRouter. If this parameter is not specified, the system will show status of the internal network server of the default VRouter (trust-vr).
- **tcp-port** *port* – Shows status of the internal network server of the specified port number.
- **ping** – Shows Ping monitor status of the internal network server.

Viewing DNAT Rule Hit Counts

To facilitate users' management and maintenance of DNAT rules, the system supports statistics on DNAT rule hit counts. This feature counts how many times the traffic matches a DNAT rule. Every time the inbound traffic matches a specific DNAT rule, the hit count of that DNAT rule automatically increases by 1. You can view statistics on DNAT rule hit counts with the following command in any mode:

show dnat hit-count vrouter *vr-name* {**id** *id* | **top** {10 | 20 | 50 | **all**}}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **id** *id* - Shows the hit counts statistics of the DNAT rule whose ID is the specified ID.
- **top** {10 | 20 | 50 | **all**} - Shows the hit count statistics of the top 10, 20, 50 matched DNAT rules , or shows the hit count statistics of all DNAT rules (**all**).

Viewing Statistics on DNAT Rule Hits

In any mode, you can use the corresponding show commands to view statistics on DNAT rule hits, including DNAT rule ID, hit counts, first-hit time, last-hit time, days since last-hit time, DNAT rule created time, and DNAT rule status (enabled/disabled).

To view hit statistics of the DNAT rule that belongs to the specified VRouter:

show dnat hit-info vrouter *vr-name*

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.

To view hit statistics of the DNAT rule whose ID is the specified ID:

show dnat hit-info vrouter *vr-name* **id** *id*

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **id** *id* - Specifies DNAT rule ID.

To view DNAT rules that are never hit by traffic:

show dnat hit-info vrouter never-hitted

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.

To view hit statistics of the DNAT rule whose days since created are longer than the specified days:

show dnat hit-info vrouter *vr-name* **days-since-created** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the DNAT rule whose days since first hit are longer than the specified days:

show dnat hit-info vrouter *vr-name* **days-since-first-hitted** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the DNAT rule whose days since last hit are longer than the specified days:

show dnat hit-info vrouter *vr-name* **days-since-last-hitted** *value*

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

Use the following command to view hit statistics of the combinedly filtered DNAT rules. The filters include that DNAT rules' days since last hit are longer than the specified days, DNAT rules' days since first hit are longer than the specified days, and DNAT rules' days since created are longer than the specified days.

show dnat hit-info vrouter *vr-name* [**days-since-last-hitted** *value*] [**days-since-first-hitted** *value*] [**days-since-created** *value*]

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the DNAT rule whose days since last hit are longer than the specified days.
- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the DNAT rule whose days since first hit are longer than the specified days.
- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the DNAT rule whose days since created are longer than the specified days.

To view hit statistics of all DNAT rules in ascending or descending order of SNAT rule ID:

show dnat hit-info vrouter *vr-name* **sorted-by id** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **id** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of DNAT rule ID.

To view hit statistics of all DNAT rules in ascending or descending order of hit counts:

show dnat hit-info vrouter *vr-name* **sorted-by hit-count** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **hit-count** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of hit counts.

To view hit statistics of all DNAT rules in ascending or descending order of DNAT rule created time:

show dnat hit-info vrouter *vr-name* **sorted-by created-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **created-time** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of DNAT rule created time.

To view hit statistics of all DNAT rules in ascending or descending order of DNAT rule first hit time:

show dnat hit-info vrouter *vr-name* **sorted-by first-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **first-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of DNAT rule first hit time.

To view hit statistics of all DNAT rules in ascending or descending order of days since DNAT rule last hit:

show dnat hit-info vrouter *vr-name* **sorted-by days-since-last-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **days-since-last-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of days since DNAT rule last hit.

To view hit statistics of all DNAT rules in ascending or descending order of DNAT rule last hit time:

show dnat hit-info vrouter *vr-name* **sorted-by last-hit-time** {**ascending** | **descending**}

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **last-hit-time** {**ascending** | **descending**} - Specifies that hit statistics of all DNAT rules are displayed in ascending or descending order of DNAT rule last hit time.

Clearing Statistics on DNAT Rule Hits

In any mode, use the following command to clear statistics on DNAT rule hits:

clear dnat hit-info vrouter *vr-name* [**id** *id*]

- **vrouter** *vr-name* - Specifies the VRouter to which the DNAT rule belongs.
- **id** *id* - Clear hit statistics of the DNAT rule in specified ID. If no ID is specified, clear hit statistics of all DNAT rules.

Configuring an Excluding Port Rule

By configuring the excluded port rules, you can rule out port or port range. The system will not convert the specified port when the source address is translated.

To configure the excluding port function, take the following steps:

1. Create a SNAT port group.
2. Configure the SNAT port group, and specify the description excluded port number.
3. Bind the SNAT port group to the specified VRouter to make the function take effect.

Creating a SNAT Port Group

To create a SNAT port group, in the global configuration mode, use the following command:

snat-port-group *snat-port-group-name*

- *snat-port-group-name* - Specifies the SNAT port group name and enters the SNAT port group configuration mode. If the specified name exists, then the system will directly enter the SNAT port group configuration mode. The name range is 1 to 95 characters.



Notes: System supports at most 8 SNAT port groups.

To delete a SNAT port group, in the global configuration mode, use the following command:

no snat-port-group *snat-port-group-name*

Specifying the Description of SNAT Port Group

To specify the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

description *description*

- *description* – Specifies the description of SNAT port group, the range is 0 to 256 characters.

To delete the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

no description

Specifying the Excluding Port Number

To specify the port range that needs to be excluded, in the SNAT port group configuration mode, use the following command:

port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

- **TCP** | **UDP** – Specifies the protocol type of excluded ports.
- **min-port** *min-port* [**max-port** *max-port*]- Specifies the excluded port number. If the port number is a number range, then *min-port* is the minimum port number, and *max-port*is the maximum port number.

To cancel the above configuration, in the SNAT port group configuration mode, use the following command:

no port {**TCP** | **UDP**} **min-port** *min-port* [**max-port** *max-port*]

Binding the SNAT Port Group to VRouter

After binding the SNAT port group to the specified VRouter, the SNAT rule of all dynamic ports of the VRouter excludes the port number specified in the SNAT port group, in the VRouter configuration mode, use the following command:

snat-exclude-port *snat-port-group-name*

To cancel the binding, in the VRouter configuration mode, use the following command:

no snat-exclude-port

Viewing the SNAT Port Group Information

To view the configuration information of SNAT port group, in any mode, use the following command:

show snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – Display the SNAT port group configuration information of the specified name.

Viewing the SNAT Port Group References

To view the SNAT port group references, in any mode, use the following command:

show reference snat-port-group [*snat-port-group-name*]

- *snat-port-group-name* – Display the SNAT port group references of the specified name.

Redundancy Check

If a large amount of NAT rules pile up in the device and you are not sure whether to delete them, this makes it more difficult to maintain these rules. To ensure the validity of NAT rules, the system performs redundancy check on the NAT rules. In other words, the system checks the coverage scope of NAT rules to solve the problem that certain NAT rules are overwritten and thus cannot be hit.

To start/stop/clear redundancy check, use the following command in any mode:

exec {snat | dnat | bnat} redundancy-checkvrouter*vrouter-name* **{start | stop | clear}**

- **snat** | **dnat** | **bnat** – Specifies the type of rules on which you want to perform redundancy check.
- **vrouter***vrouter-name* – Specifies the virtual router to which SNAT rules, DNAT rules, or BNAT rules belong.
- **start** – Specifies to start redundancy check on SNAT rules, DNAT rules, or BNAT rules.
- **stop** – Specifies to stop redundancy check on SNAT rules, DNAT rules, or BNAT rules.

- **clear** – Specifies to clear the results of redundancy check performed on SNAT rules, DNAT rules, or BNAT rules.

In any mode, use the **show** {**snat** | **dnat** | **bnat**} **redundancy-checkvrouter***vrouter-name* command to view the redundancy check results of SNAT rules, DNAT rules, or BNAT rules.

- **vrouter***vrouter-name* – Specifies the virtual router to which NAT rules whose redundancy check results you want to view belong.

Example:

```
hostname(config)# show snat redundancy-check vrouter trust-vr
Total count: 1  (Displays the total number of redundant SNAT rules that belong to the virtual router trust-vr)
VR name: trust-vr
=================================================
SNAT ID covered by (Displays that the SNAT rule whose ID is 4 is overwritten by the SNAT rule whose ID is 3)
-------------------------------------------------
4 3;
=================================================
```

DNS Rewrite

When the client initiates a DNS request, DNS server in Internet will return DNS response to the client. The security device can rewrite the IP address/host name in DNS response packet to private IP in order to protect the private network configurations.

Each DNS rewrite rule has a unique ID. By specifying or adjusting the position of a rule ID, the administrator can adjust the rule priority. When receiving a DNS response, the device will try to match all rules from top to bottom and rewrite the response according to the rule that is matched firstly.



Notes: After enabling the DNS ALG function, the DNS rewrite function will take effect. To enable the DNS ALG function, in the global configuration mode, use the command **alg dns**. For detailed information on ALG, please refer to "Application Layer Identification and Control" on Page 307.

Configuring DNS Rewrite Rules

In NAT configuration mode, type the following command:

dns-rewrite-rule [**id** *id*] [**after** *id* | **before** *id* | **top**] **dns-response** {**ip** *ip-address* | **address-book** *address-name* | **host-book** *host-book-name*} **rewrite-to** {**ip** *ip-address* | **address-book** *address-name*} **dynamic-mapping** [**description** *description*]

- **id** *id* – Specifies the rule ID. Each rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified ID exists, the original rule will be overwritten.
- **after** *id* | **before***id* | **top** - Specifies the position of the rule. The rule can be placed before or after a specific ID, or placed on the top of all rules. By default, the rule is placed at the end of all rules.
- **dns-response** {**ip** *ip-address* | **address-book** *address-name* | **host-book** *host-book-name*} - Specifies public IP, address book or host name book in DNS response.
- **rewrite-to** {**ip** *ip-address* | **address-book** *address-name*} – Specifies private IP or address book which the security device rewrites.
- **description** *description* - Specifies the description of the DNS rewrite rule.

In NAT configuration mode, use the following command to delete a DNS rewrite rule:

no dns-rewrite-rule [**id***id*]

Modifying/Deleting DNS Rewrite Rule Description

In NAT configuration mode, use the following command to modify the description of a DNS rewrite rule:

dns-rewrite-rule [**id** *id*] **description** *description*

Use the following command to delete the description of a DNS rewrite rule:

no dns-rewrite-rule [**id** *id*] **description**

Viewing DNS Rewrite Rules

In any mode, use the following command to view DNS rewrite rules:

show dns-rewrite-rule [**id** *id* | **vrouter** *vr-name*]

- [**id** *id* | **vrouter** *vr-name*] − View the DNS rewrite rules of the specified ID or VRouter. If not specified, view all DNS rewrite rules in the default VR.

Viewing Dynamic Mapping Entries of DNS Rewrite

The dynamic mapping table of DNS rewrite stores the mappings between the response address and the rewrite address. In any mode, use the following command to view dynamic mapping entries of NDS rewrite:

show dns-rewrite-rule [**id** *id* | **vrouter** *vr-name*] **dynamic-mapping** [**detail**]

- [**id** *id* | **vrouter** *vr-name*] - View dynamic mapping entries of the DNS rewrite rules with specified ID or VRouter. If not specified, view dynamic mapping entries of all DNS rewrite rules in the default VR.
- **detail** - View the details of dynamic mapping entries of the DNS rewrite rules.

Example:

```
hostname(config)# show dns-rewrite-rule vrouter trust-vr dynamic-mapping
Total 1 entries.
vr name:trust-vr
==================================================
id DNS-response Rewrite-to Life-time
--------------------------------------------------
3 192.168.1.88 192.168.1.77 3134
```

```
=================================================

hostname(config)# show dns-rewrite-rule vrouter trust-vr dynamic-mapping detail

Total 1 entries.

vr name:trust-vr

=================================================

id DNS-response Rewrite-to Life-time Timeout TTL

-------------------------------------------------

3 192.168.1.88 192.168.1.77 3124 3780 60

=================================================

( id refers to the rule ID; DNS-response refers to the pub-
lic IP, address book or host name book in DNS response;
Rewrite-to refers to the private IP or address book which
the security device rewrites; Life-time is the lifespan of
the mapping entry; Timeout is the expiration time of the map-
ping entry; TTL is the validity time of the DNS record in
the cache)
```

Adjusting the Priority of DNS Rewrite Rule

To adjust the priority of a DNS rewrite rule, in the NAT configuration mode, use the following command:

dns-rewrite-rule move *id* {**after** *id* | **before** *id* | **top** | **bottom**}

- *id* - Specifies the ID of the DNS rewrite rule to be moved.
- **after** *id* - Moves the DNS rewrite rule after the specified ID.
- **before** *id* - Moves the DNS rewrite rule before the specified ID.
- **top** - Moves the DNS rewrite rule to the top of the DNS rewrite rule list.
- **bottom** - Moves the DNS rewrite rule to the bottom of the DNAT rule list.

Enabling/Disabling DNS Rewrite Rule Rematch

When a DNS response hits a DNS Rewrite rule, the device will rewrite the response based on the DNS Rewrite rule and establish an entry to record the mapping relationships between the response IP and the rewrite IP. Subsequent service requests will be translated based on the mapping relationships recorded. When the user adds, modifies or deletes a DNS Rewrite rule, rule priorities might change. When an entry established by a previously hit rule matches a new rule:

- If DNS Rewrite rematch is enabled, the device will directly delete the previous entry.
- If DNS Rewrite rematch is disabled, the device will not delete the previous entry and subsequent service requests might still hit the entry.

The DNS Rewrite rematch function is disabled by default. To enable this function, in the global configuration mode, use the following command:

dns-rewrite-rule rematch

Use the following command to disable this function:

no dns-rewrite-rule rematch

NAT444

Hillstone devices support NAT444. NAT444 is carrier-grade NAT that is designed to extend the service life of IPv4 during the transition from IPv4 to IPv6 and win some time for the deployment of IPv6.

With NAT444 configured, the system will create a mapping table according to user's address pool (source IP), public address pool (translated IP), available port range and port block size, and implement NAT for the source IPs and ports of matched traffic based on the mapping table.

Configuring NAT444

NAT444 on Hillstone devices is implemented by creating and executing SNAT rules. Compared with traditional SNAT rules, NAT444 SNAT rules are featured with some new parameters. This section mainly describes these new parameters. To configure an SNAT rule for NAT444, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to addressbook** *trans-to-address* **mode dynamicport** [**fixed-block** | **random-block**] **start** *start-port* **end** *end-port* **size** *port-block-size* [**max-block-per-user** *blocks*] [**log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} [**group** *group-id*] [**description** *description*]

- - **mode dynamicport** [**fixed-block** | **random-block**] **start** *start-port* **end** *end-port* **size** *port-block-size* [**max-block-per-user** *blocks*] – All the sessions originating from one source IP will be mapped to one specified IP address in an address entry. The source IP corresponds to one or more port blocks of the mapped IP. If the port resources in the block are exhausted, the translation will fail. For detailed mapping relationship, see the NAT444 SNAT example below.
    - **fixed-block** – Uses the static port block mapping mode . Each source IP address corresponds to a fixed port block of the mapped IP.
    - **random-block** – Uses the dynamic port block mapping mode. Each source IP address can correspond to one or more port blocks and the parameter **max-block-per-user** *blocks* determines how many port blocks that each source IP address can correspond to.
    - **start** *start-port* **end** *end-port* – Specifies the start port and end port of the available port range. The value range is 1024 to 65535.
    - **size** *port-block-size* – Specifies the size of the port block. The value range is 64 to 64512, and the value must be the integer multiple of 64.
    - **max-block-per-user** *blocks* – Specifies the maximum number of port blocks that each user in the intranet can occupy. When using the dynamic port block mapping mode, you can set this parameter. The default value is 1.

- **log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} – Configures log for NAT444 (generates logs for matched traffic):
  - **port-block** {**allocate** | **release** | **all**} – Generates logs when the system is allocating (**allocate**) or releasing (**release**) port block. **all** indicates generating logs for both of the above events.
  - **session** {**allocate** | **release** | **all**} – Generates logs when the system is creating (**allocate**) or disconnecting (**release**) a NAT session. **all** indicates generating logs for both of the above events.
  - **all** – Generates log when the system is either allocating/releasing a port block or creating/disconnecting a NAT session.

  group*group-id* | **both** - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0. In the static port block mapping mode (**fixed-block**), the both parameter can be specified. System will divide the port range of the device under the HA Peer mode according to the HA Node ID. That is, the device of each HA Node ID uses half the port range. For example, the device of HA Node ID is 0 uses the first half of the port range, and the device of HA Node ID is 1 uses the second half of the port range.

The following is a NAT444 SNAT example:

Suppose the source IP is src_addr: 192.168.1.0/24, and the translated IP is global_addr: `200.1.2.10~200.1.2.100`

hostname(config-vrouter)# **snatrule id 1 from src_addr to any trans-to address-book global_addr mode dynamicport fixed-block start 1024 end 65000 size 4096**

rule id=1

`The mapping relationship is shown as below:`

hostname(config-vrouter)# **show snat id 1 ports-map**

```
-------------------------------------------------------------
=============================================================
====================
from translate to start port end port
-------------------------------------------------------------
192.168.1.0 200.1.2.10 1024 5119
192.168.1.1 200.1.2.10 5120 9215
192.168.1.2 200.1.2.10 9216 13311
……
192.168.1.14 200.1.2.10 58368 62463
192.168.1.15 200.1.2.11 1024 5119
192.168.1.16 200.1.2.11 5120 9215
192.168.1.17 200.1.2.11 9216 13311
……
```

To configure an SNAT rule that disables NAT444, in the NAT configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

Monitoring the Port Utilization and Port Block Utilization

The system can monitor the port utilization and port block utilization. When the real utilization is higher than the specified threshold, the system will send the corresponding alarms. This monitor function is available to all NAT444 rules.

To configure the port utilization or port block utilization monitor, in the global configuration mode, use the following command:

nat444-resource monitor {**port-utilization threshold** *value* | **port-block-utilization threshold** *value*} **log**

- **port-utilization threshold** *value* – Specifies the threshold of the port utilization. When the actual value is higher than the threshold specified here, the system will send the corresponding alarm. The value range is from 1 to 99.
- **port-block-utilization threshold** *value* – Specifies the threshold of the port block utilization. When the actual value is higher than the threshold specified here, the system will send the corresponding alarm. The value range is from 1 to 99.

In the global configuration mode, use the command to cancel the monitor configuration.

no nat444-resource monitor {**port-utilization** | **port-block-utilization**}

Viewing NAT444 Configuration Information

To view SNAT rule information of NAT444, in any mode, use the following command:

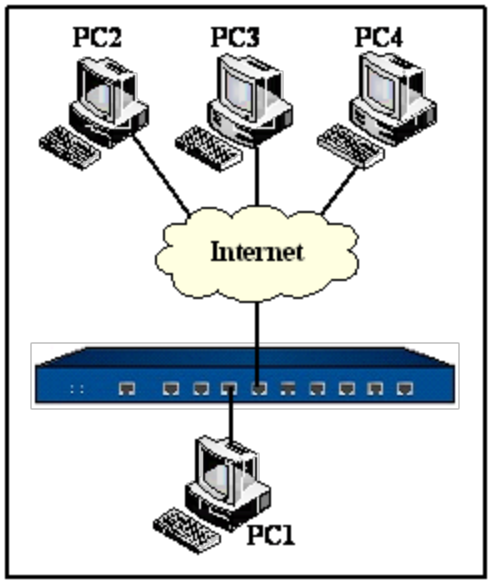
show snat [**id** *id*] **ports-map** {**slot** *slot_number* **src** *src-address* [**detail**] | **trans-to** *trans-to-address* | **vrouter** *vrouter-name* {**src** *src-address* [**detail**] | **trans-to** *trans-to-address*}}

- **id** *id* – Shows the mapping information of the SNAT rule with the specified ID.
- **slot** *slot_number* – Shows the mapping information of the SNAT rule with the specified slot. This parameter only support for X series devices.
- **src** *src-address* – Shows the mapping information of the specified source IP.
- **detail** – Shows the mapping information of the specified source IP and port block utilization.
- **trans-to** *trans-to-address* – Shows the mapping information of the translated IP address.
- **vrouter** *vrouter-name* - Shows the SNAT rule mapping information of the specified VRouter.

Full-cone NAT

Full-cone NAT, also known as one-to-one NAT, will map all the requests from one IP/port in the private network to one IP/port in the public network, and thereafter all the hosts in the public network will be able to communicate with the host that initiated the request by making use of the mapping relationship.

As shown below, suppose PC1 in the Intranet has already established a connection with PC2 in the Internet after NAT translation, and the device translates the IP/port of PC1 (Private IP:Private port) to a public IP/port (Public IP:Public port). Since there exists a session, PC2 can connect to PC1 reversely by matching the session. However, due to no session matching information, by default PC3 and PC4 cannot communicate with PC1 even if the translated public IP/port (Public IP:Public port) is routable. With Full-cone NAT enabled, the device will create and maintain a Full-cone NAT entry and advertise the mapping between the public and private IPs/ports (Local IP:Local port <==> Public IP:Public port) by the entry. In such a condition, if only PC3 and PC4 can reach the public IP/port of PC1 (Public IP:Public port), they can tranverse the NAT device and connect to PC1 proactively by making use of the mapping information.



To enable Full-cone NAT, in the global configuration mode, use the following command:

nat type full-cone

To disable Full-cone NAT, in the global configuration mode, use the following command:

no nat type full-cone

To specify the protocol that is enabled with Full-cone NAT, in the global configuration mode, use the following command:

nat protocol {tcp | udp}

- **tcp**- Enables Full-cone NAT on TCP.
- **udp** - Enables Full-cone NAT on UDP.

To cancel the configuration, in the global configuration mode, use the following command:

no nat protocol {**tcp** | **udp**}

Viewing Full-cone NAT Configuration Information

To view the configuration information of Full-cone NAT, in any mode, use the following command:

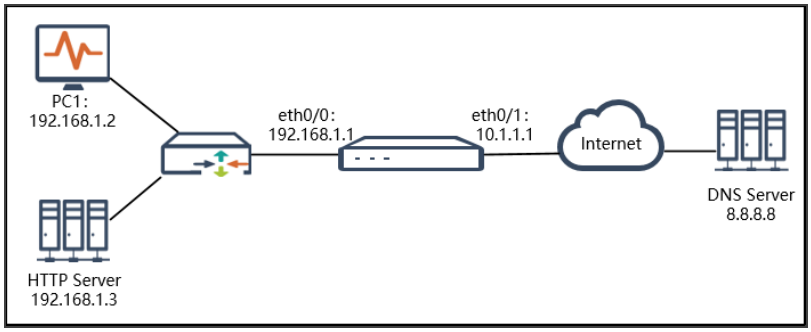
show nat {**configuration** | **generic** | **entry** [**all** | **src-ip** *ip-address* [**src-port** *port-number* **protocol** {**tcp** | **udp**} *snat-id*[**interface** *interface-name*]] | **vr** *vrouter-name*] | **control** [**vrouter** *vrouter-name*]}

- **configuration** - Shows the configuration of Full-cone NAT.
- **generic** - Shows the general information of Full-cone NAT entry.
- **entry** [**all** | **src-ip** *ip-address* [**src-port** *port-number* **protocol** {**tcp** | **udp**} *snat-id* [**interface***interface-name*]] | **vr** *vrouter-name*]
  - **entry** - Shows the detailed information of Full-cone NAT entry.
  - **all** - Shows the detailed information of Full-cone NAT entry in VSYS.
  - **src-ip** *ip-address* [**src-port** *port-number* **protocol** {**tcp** | **udp**} *snat-id* [**interface***interface-name*]] - Shows the detailed information of Full-cone NAT entry of the specified source IP address (**src-ip** *ip-address*), source port (**src-port** *port-number*), protocol type (**protocol** {**tcp** | **udp**}) and SNAT rule ID (*snat-id*) and interface (*interface-name*).
  - **vr** *vrouter-name* - Shows the detailed information of Full-cone NAT entry of the specified VRouter. If not specified, the system will show the Full-cone NAT entry information of trust-vr by default.

- **control** [**vrouter** *vrouter-name*]
  - **control** - Shows the status of the following functions: full-cone NAT, expanded PAT port pool, SNAT port split under HA peer mode and "Bounce NAT" on Page 301.
  - **vrouter** *vrouter-name* - Shows the status of Bounce NAT of the specified VRouter. If not specified, the system will show the status of Bounce NAT of trust-vr by default.

Bounce NAT

Suppose the HTTP server is deployed in the intranet and users from the internet try to access the server via the configured DNAT rules as shown in the following picture. When the intranet PC1 (192.168.1.2) visits the HTTP server (192.168.1.3), it will send the domain name to the internet DNS server for analyzing and obtain the public IP (10.1.1.2) of the HTTP server. Therefore, the PC1 will send HTTP request to 10.1.1.2. After the request is received, the destination IP will be translated to 192.168.1.3 and forwarded to the HTTP server in the intranet. When the HTTP server receives the request, it will send response packets to PC1. At this moment, the source IP of the response packet is 192.168.1.3, which is not consistent with the destination IP (10.1.1.2) in the request packet sent by PC1. Then PC1 will drop the response packets and the PC1 in the intranet will fail to visit the intranet server in the same segment.



With the Bounce NAT function, the above problem can be solved. Only the request matches the following conditions can the function be triggered. With the function, the source IP address in the request packet will be modified as the IP address of egress interface (such as eth0/0: 192.168.1.1 in the above picture), and then the PC in the intranet will access the intranet server normally. The conditions are as follows:

- Match DNAT rules.
- Do not match all the SNAT rules.
- The egress and ingress interfaces are the same.

By default, the Bounce Nat function is enabled. To disable the function, in the VRouter configuration mode, use the following command:

bounce-snat-disable

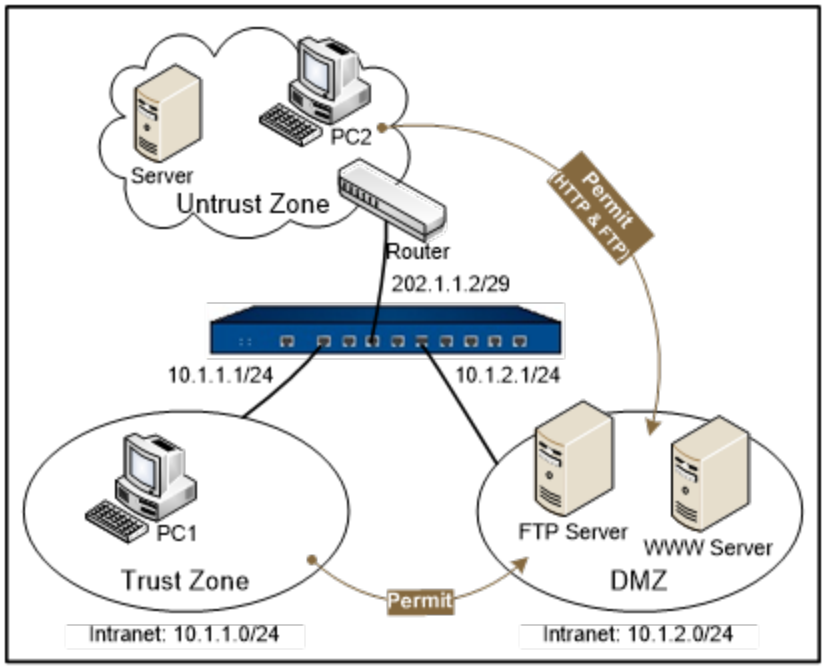
Use the command **no bounce-snat-disable** to enable the Bounce NAT function.

Example of Configuring NAT

This section describes a typical NAT configuration example.

Requirement

The company network is divided into three zones by a Hillstone device: Trust Zone, DMZ Zone and Untrust Zone. Employees work in the Trust zone, they are allocated with the private network segment of 10.1.1.0/24 and get the highest security priority; WWW server and FTP server are in the DMZ zone, they are allocated with the private network segment of 10.1.2.0/24 and can be accessed by internal employees and external users; external networks are in the Untrust zone. The network topology is shown in Figure below:



There are three requirements:

- Requirement 1: Employees in segment 10.1.1.0/24 in the trust zone are able to access the Internet, while PCs in other segments of the zone cannot access the Internet. The legitimate IP address range provided to access the external network is 202.1.1.3 to 202.1.1.5. Because there are not enough public network addresses, NAT address multiplexing function is needed.
- Requirement 2: Two internal servers are provided for users and can be accessed from the external networks, including an FTP server (the internal IP address is 10.1.2.2, port number is 21) and a WWW server (the internal IP address is 10.1.2.3, port number is 80); external mapping IP address is 202.1.1.6.
- Requirement 3: After any PC in the Trust zone has gained access to the host in the Untrust zone, all the hosts in the Untrust zone can connect to the PC in the Trust zone reversely by making use of Full-cone NAT.

Configuration Steps

Step 1: Configure security zones and IP addresses

```
hostname# configure
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 10.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.1.2/29
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure address entries

```
hostname(config)# address addr1
hostname(config-addr)# ip 10.1.1.1/24
hostname(config-addr)# exit
hostname(config)# address addr2
hostname(config-addr)# range 202.1.1.3 202.1.1.5
hostname(config-addr)# exit
hostname(config)# address test1
hostname(config-addr)# ip 202.1.1.6/32
hostname(config-addr)# exit
hostname(config)# address test2
hostname(config-addr)# ip 10.1.2.2/32
```

```
hostname(config-addr)# exit
hostname(config)# address test3
hostname(config-addr)# ip 10.1.2.3/32
hostname(config-addr)# exit
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr addr1
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
```

```
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 4: Configure NAT rules

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from addr1 to any eif ehternet0/2 trans-to address-book addr2 mode dynamicport sticky
rule id=1
hostname(config-vrouter)# dnatrule id 2 from any to test1 service ftp trans-to test2 port 21
rule id=2
hostname(config-vrouter)# dnatrule id 3 from any to test1 service http trans-to test3 port 80
rule id=3
hostname(config-vrouter)# exit
hostname(config)# nat type full-cone
hostname(config)# nat protocol tcp
```

Application Layer Identification and Control

Overview

Hillstone devices provide a wide range of application layer monitoring, statistics and filtering functions. These functions can identify applications such as FTP, HTTP, P2P, IM tools and VoIP, and based on the security policy rules configured, ensure the proper communication of the applications or perform the specified operations on the traffic, such as monitoring, statistics, traffic control and blocking. By making use of the fragment reassembling and transport layer proxy technique, the Hillstone devices can adapt to the complex network environment, reassemble the packets, and identify the applications effectively even when the complete application layer data is fragmented and disordered during the transmission, thus ensuring the effective implementation of security policies.

Fragment Reassembly

Typically the intermediate network device such as a router or switch does not reassemble the fragmented packets it receives. The destination host reassembles the fragmented packets after all the fragments have arrived. Due to the complexity of the network environment, fragmented packets may be dropped or disordered during the transmission, while the reassembling needs to receive and sort all the fragments, which will consume certain system resources. From the aspect of the main function and forwarding efficiency, the network devices usually only forward the fragments and will not reassemble them. However, for security devices, the application of security policies requires an analysis of application layer information, in order to filter the malicious messages that contain potential security risks, or block any attempt of intrusions and attacks. All the operation will only be finally determined after the device receives the complete information of the application layer. Powered by the transport layer proxy function, StoneOS can buffer, sort and reassemble the fragmented packets first, and then re-encapsulate and forward the normal data after a complete analysis and identification.

Application Layer Gateway (ALG)

Some applications use multi-channels for data transmission, such as the widely used FTP. In such a condition the control channel and data channel are separated. Hillstone devices under strict

security policy control set strict limits on each data channel, for example, only allow FTP data from internal network to external network to transfer on the well-known port TCP 21. Once in the FTP active mode, if an FTP server in the public network tries to initiate a connection to a random port of the host in the internal network, Hillstone devices will reject the connection and the FTP server will not work properly in such a condition. This requires Hillstone devices to be intelligent enough to properly handle the randomness of legitimate applications under strict security policies. In FTP instances, by analyzing the transmission information of the FTP control channel, Hillstone devices will be aware that the server and the client reached an agreement, and open up a temporary communication channel when the server takes the initiative to connect to a port of the client, thus assuring the proper operation of FTP.

StoneOS adopts the strictest NAT mode. Some VoIP applications may work improperly after NAT due to the change of IP address and port number. The ALG mechanism can ensure the normal communication of VoIP applications after the NAT. Therefore, the ALG supports the following functions:

- Under strict security policy rules, ensures the normal communication of multi-channel applications, such as FTP, TFTP, PPTP, RTSP, RSH, MSRPC, SUNRPC and SQLNET.
- Ensures the proper operation of VoIP applications such as SIP and H.323 in NAT mode, and performs monitoring and filtering according to the policies.

HTTP, P2P and IM

Powered by the fragment reassembly and transport layer proxy functions, StoneOS supports the identification and control of 3 main types of applications: HTTP applications, P2P applications and IM applications. The Hillstone devices can perform various operations like monitoring, restricting and blocking traffic on each application by creating Profiles. For example:

- Filtering HTTP Java Applets to ensure users are protected from harmful Java Applets.
- Filtering HTTP ActiveX to prevent malicious ActiveX programs from damaging the user's system.
- Identifying, monitoring and blocking P2P applications, like BT, eMule, Thunder, etc.

- Operations on IM tools, such as identifying and controlling IM chatting and file transfer. The supported IM clients include MSN Messenger, QQ, Yahoo

Configuring ALG

StoneOS allows you to enable or disable ALG for different applications. Hillstone devices support ALG for the following applications: FTP, HTTP, MSRPC, PPTP, Q.931, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, TFTP, DNS, H323 and XDMCP. You can not only enable or disable ALG for applications, but also specify H323's session timeout.

To enable or disable the ALG control function for applications, in the global configuration mode, use the following command:

Enable: **alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** |…}

Disable: **no alg** {**all** | **auto** | **TFTP** | **FTP** | **RSH** | …}

- **all** – Enables or disables the ALG control function for all the applications.
- **auto** – Enables or disables the ALG control function based on the result of application identification.
- **TFTP | FTP | RSH |** … - Enables or disables the ALG control function for the specific application.



Notes: If ALG for HTTP is disabled, the Web content filter function on the device will be void.

ALG supports strict mode and non-strict mode. In the strict mode, the newly-created pinhole has the SNAT port which is the same as the SNAT port of the control session. By default, the strict mode is enabled. To enable the ALG strict mode, use the following command in the global configuration mode:

alg strict-mode

Use the **no alg strict-mode** command to enable the non-strict mode. In the scenario below, Hillstone recommends the users to enable the non-strict mode:

- The third-party pinhole exists.
- SNAT is configured and port expansion is enabled.
- The IP address and port number in the payload for negotiating the data session is the same as the IP address and port number of the control session.

To specify the timeout value for the H323 protocol, in global configuration mode, use the following command:

alg h323 session-time *time-value*

- *time-value* - Specifies the timeout value for H323. The value range is 60 to 1800 seconds. The default value is 60.

To cancel the specified timeout value, in global configuration mode, use the following command:

no alg h323 sesstion-time

To limit the number of the SIP messages that can be processed per second, use the following command in the global configuration mode:

Enable: **alg sip-message-rate** *number*

- *number* - Specifies the maximum number of the SIP messages that can be processed per second. The value is in the range of 1 to 65535.

Disable: **no alg sip-message-rate**

To enable or disable the anomaly detection of FTP PORT, in global configuration mode, use the following command:

Enable: **alg ftp anomaly-detection**

Disable: **no alg ftp anomaly-detection**

To enable or disable the ALG FTPS funtion, in global configuration mode, use the following command:

Enable: **alg ftp ftps-extension**

Disable: **no alg ftp ftps-extension**

To enable or diable the logging function for the HTTP persistent connection requests, in global configuration mode, use the following command:

Enable: **alg http persistent connection**

Disable: **no alg http persistent connection**

To view the status and configuration of ALG, in any mode, use the following commands:

- To view if ALG is enabled: **show alg**
- To view the ALG configuration and status of SIP gateway: **show alg sip-capacity**

Enabling/Disabling DNS Rewrite by DNAT

After the device is enabled with the DNS ALG function, if the client initiates a DNS request, the DNS response message returned by the DNS server will prioritize matching DNAT rules, and will match DNS rewrite rules only if DNAT rule matching fails. In this case, the DNS response message may mistakenly match DNAT rules when it only needs to match DNS rewrite rules, resulting in abnormal service access.

To avoid abnormal service access, the system supports to enable/disable the DNS Rewrite by DNAT function. By default, this function is enabled. In other words, DNS response messages prioritize matching DNAT rules, and DNS rewrite rules will be matched only if DNAT rule matching fails. If this function is disabled, DNS response messages will only match DNS rewrite rules.

To enable/disable the DNS Rewrite by DNAT function, in global configuration mode, use the following command:

- Enable: **alg dns dns-rewrite-by-dnat**
- Disable: **no alg dns dns-rewrite-by-dnat**



Notes: The configurations above take effect only after the DNS ALG function is enabled. To enable the DNS ALG function, in global configuration mode, use the **alg dns** command. For more information, refer to the **Firewall > Application Layer Identification and Control** chapter.

Specifying SIP Proxy Server Mode

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls. Multimedia transitted by SIP usually are voice, video and text.

SIP proxy server acts as an intermediary entity when the SIP user agent clients are making requests. When SIP user agent clients exchange media data packets, they can transfer data with or without a SIP proxy server. To avoid communication error, the firewall should select a mode that complies with the actural data transmission mode.

Under global configuration mode, use the command below to inform the firewall that SIP user agent clients are communicating media data directly without SIP proxy server. This is the default setting on the firwall. This command ensures normal communication among SIP user agents.

no alg sip media-proxied-by-server

Under global configuration mode, use the command below to inform the firewall that SIP user agent clients are exchanging media data packets through SIP proxy server.

alg sip media-proxied-by-server

Showing ALG SIP

To show ALG SIP information, including if the firewall has enabled SIP server proxy, SIP message rate maximum, registered client number and busy client number, under any mode, use the following command:

show alg sip

Examples of Configuring Application Layer Identification and Control

This section describes two application layer identification and control examples:

- Example 1: The goal is to strictly restrict internal users' access to TFTP, FTP and RTSP services running on the external network only on the well-known ports, while also ensuring the normal communication of these applications on multiple channels.
- Example 2: The goal is to block ActiveX controls and Java applets from the external network.

Configuration Steps for Example 1

Step 1: Restrict service types in security policy rules

```
The address entry "internal" includes all the IPs of internal clients
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service tftp
hostname(config-policy-rule)# service ftp
hostname(config-policy-rule)# service rtsp
hostname(config-policy-rule)# application tftp
hostname(config-policy-rule)# application ftp
hostname(config-policy-rule)# application rtsp
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Enable ALG for these applications

```
hostname(config)# alg tftp
hostname(config)# alg ftp
hostname(config)# alg rtsp
```

Configuration Steps for Example 2

Step 1: Enable ALG for the HTTP application

```
hostname(config)# alg http
```

Step 2: Configure a Profile to control Java applets and ActiveX

```
hostname(config)# behavior-profile test
hostname(config-bhv-profile)# object active-x deny
hostname(config-bhv-profile)# object java-applet deny
hostname(config-bhv-profile)# exit
hostname(config)#
```

Step 3: Bind the profile to policy rules

```
The address entry "internal" includes all the IPs of
internal clients
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr internal
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# application http
hostname(config-policy-rule)# behavior test
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

RSTP

RSTP, the abbreviation for Rapid Spanning Tree Protocol defined by IEEE 802.1D-2004, is the enhancement and supplement to STP (8021.D). The protocol can provide faster spanning tree convergence after a topology changes.

RSTP is a loop network solution that is designed to block the redundant links to avoid broadcast storms. When a link fails in the network, the redundant link will quickly switch to the forwarding state, and ensure that the traffic will not be interrupted. The root of the Rapid Spanning Tree is known as a root bridge in the RSTP protocol. The root bridge is autonomously selected among the network device by comparing the bridge priorities (the smaller the value is, the higher the priority will be). The farthest port to the root bridge on the other device (the largest cost) will be blocked, and the link corresponding to the blocked port will become a redundant link.

Configuring RSTP

The configurations of RSTP include:

- Creating RSTP
- Enabling RSTP
- Configuring the bridge priority
- Configuring the Hello interval
- Configuring the Forward Delay time
- Configuring the maximum age of BPDU message
- Enabling RSTP on an interface
- Configuring the RSTP priority on an interface
- Configuring the RSTP cost on an interface

Creating RSTP

To create RSTP and enter the RSTP configuration mode, in the global configuration mode, use the following command:

stp

The command creates RSTP and leads you to the RSTP configuration mode; if the RSTP is existing, the system will directly enter the RSTP configuration mode.

To delete RSTP, in the global configuration mode, use the command **no stp**.

Enabling RSTP on the Device

The RSTP function is a global switch. You need to enable both the global function switch and the interface RSTP switch to control RSTP function jointly. By default, RSTP is disabled on the device. To enable RSTP, in the RSTP configuration mode, use the following command:

enable

To disable RSTP, in the RSTP configuration mode, use the command **no enable**.

Enabling RSTP on an Interface

By default, RSTP on an interface is disabled. To enable RSTP on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

stp enable

To disable RSTP on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

no stp enable

Configuring the Bridge Priority

To configure the bridge priority, in the RSTP configuration mode, use the following command:

bridge priority *value*

- *value* – Specifies the bridge priority. The value must be the integer multiples of 4096. The value range is 0 to 61440. The default value is 32768.

To restore to the default bridge priority, in the RSTP configuration mode, use the following command:

no bridge priority

Configuring the Hello Interval

Hello packets are used to confirm whether the link between devices is normal. The Hello interval is used to specify how often the device sends a Hello packet. To configure the Hello interval, in the RSTP configuration mode, use the following command:

hello *seconds*

- *seconds* – Specifies the Hello interval. The value range is 1 to 10 seconds. The default value is 2.

To restore to the default Hello interval, in the RSTP configuration mode, use the following command:

no hello

Configuring the Forward Delay Time

When any link fails, the system will re-calculate the spanning tree network. It's impossible for the system to spread the new BPDU (Bridge Protocol Data Unit, used for data exchanging between bridges) configuration information throughout the network immediately, so if the data transmission starts too early, it may cause a temporary loop. To avoid such a problem, RSTP defines a forwarding delay timer, i.e., the forward delay time.

To configure the forward delay time, in the RSTP configuration mode, use the following command:

forward-delay *value*

- *value* – Specifies the forward delay time. The value range is 4 to 30 seconds. The default value is 15.

To restore to the default forward delay time, in the RSTP configuration mode, use the following command:

no forward-delay

Configuring the Maximum Age of BPDU Message

The maximum age of BPDU messages indicates the lifetime of a BPDU message on the device. When the lifetime runs out, the BPDU message will be deleted.

To configure the maximum age of BPDU message, in the RSTP configuration mode, use the following command:

maximum-age *value*

- *value* – Specifies the maximum age of BPDU message. The value range is 6 to 40 seconds. The default value is 20.

To restore to the default maximum age, in the RSTP configuration mode, use the following command:

no maximum-age

Configuring the RSTP Priority on an Interface

To configure the RSTP priority on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

stp priority *value*

- *value* – Specifies the RSTP priority of the current interface. The value must be the integer multiples of 16. The value range is 0 to 240. The default value is 128.

To restore to the default RSTP priority, in the Ethernet interface or aggregate interface configuration mode, use the following command:

no stp priority

Configuring the RSTP Cost on an Interface

To configure the RSTP cost on an interface, in the Ethernet interface or aggregate interface configuration mode, use the following command:

stp cost *value*

- *value* – Specifies the RSTP cost value on the interface. The value range is 1 to 200000000. If this parameter is not specified, the system will calculate a value based on the interface type (a single interface or aggregate interface), speed (10Mbps, 100Mbps or 1000Mbps) and duplex status (full-duplex or half-duplex).

To restore to the default RSTP cost (calculated based on the above factors), in the Ethernet interface or aggregate interface configuration mode, use the following command:

no stp cost

Viewing RSTP Configuration

To view the RSTP configuration information, in any mode, use the following command:

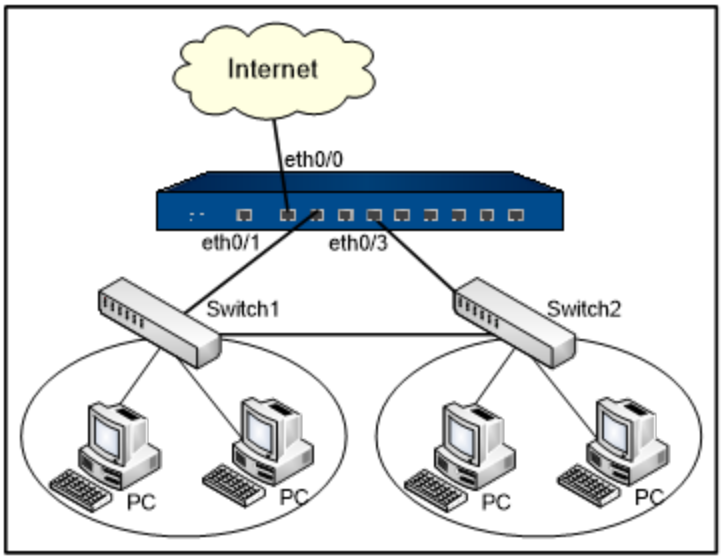
show stp [**port** *interface-name*]

Configuration Example

The section describes a RSTP example.

Requirement

As shown below, the Hillstone device acts as gateway and is connected to Internet. The requirement is: when the link between Switch1 (or Switch2) and the Hillstone device fails, enable STP on the switches and device to implement the Layer 2 link redundancy, and ensure the PC in the LAN is still able to access the Internet.



Configuration Steps

First, ensure that STP on Switch1 and Switch2 can function properly, and then take the following steps:

Step 1: Create a VLAN named VLAN1, and add ethernet0/1 and ethernet0/3 to VLAN1

```
hostname(config)# vlan 1
hostname(config-vlan)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# switchmode access vlan 1
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# switchmode access vlan 1
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Create a VLAN interface named vlan1, bind it to the zone trust and configure the IP address

```
hostname(config)# interface vlan1
```

```
hostname(config-if-vla1)# zone trust
hostname(config-if-vla1)# ip address 192.168.1.1 255.255.255.0
hostname(config-if-vla1)# exit
hostname(config)#
```

Step 3: Ethernet0/0 belongs to the zone untrust. Configure the policy rule from trust to untrust

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 4: Create RSTP, configure necessary parameters, and enable RSTP

```
hostname(config)# stp
```

```
hostname(config-stp)# bridge priority 0
hostname(config-stp)# enable
hostname(config-stp)# exit
hostname(config)#
```

Wireless Access Mode

Introduction

SG-6000-A200W (WLAN version) and SG-6000-A200G4B (4G version) support the wireless access mode. You can use the wireless mode to access the network. This chapter introduces the following functions:

- "WLAN" on Page 324
- "3G/4G" on Page 343

WLAN

WLAN (Wireless Local Area Network) represents the local area network that uses the wireless channel as the medial. WLAN is important supplements and extensions of the wired LAN. By configuring the WLAN function, you can establish the wireless local area network and allow the users to access LAN through wireless mode.

Configuring WLAN Settings

WLAN Profile is the combination of the WLAN settings. To implement the WLAN function, configure the WLAN Profile and then apply the configure WLAN Profile to the WLAN interface. One WLAN Profile can only be applied to one WLAN interface. The WLAN settings contain the following sections:

- Enabling the WLAN function.
- Creating and configuring the WLAN Profile. The WLAN Profile contains the corresponding attributes of wireless service, including SSID, enabling/disabling SSID broadcast, security mode, authentication encryption method, user isolation, maximum user numbers, and authentication server.

- Binding the WLAN Profile to the WLAN interface. After binding the WLAN Profile to the WLAN interface successfully, the WLAN function can take effect.
- Configuring the global parameters of WLAN function, such as country/region code, wireless mode, channel, maximum transmission power, wireless multimedia.

Enabling WLAN Function

By default, the WLAN function is enabled. Use wlan to enter the WLAN configuration mode. To enable the WLAN function, use the following command in the WLAN configuration mode:

wlan enable

To disable the WLAN function, use the following command:

no wlan enable

Creating WLAN Profile

To create the WLAN Profile, use the following command in the global configuration mode:

wlan profile *number*

- *number*- Specifies the number of the WLAN Profile. After executing this command, the system will create the WLAN Profile of the specified number and enter the WLAN Profile configuration mode. If the specified number already exists, the system will enter the WLAN Profile configuration mode directly. The value ranges from 0 to 3, thus allowing up to 4 WLAN Profiles.

To delete the specified WLAN Profile, use the following command in the global configuration mode:

no wlan profile *number*

Configuring SSID

SSID (Service Set Identifier) is the name of the WLAN, which is used to distinguish among different networks.

To configure SSID, use the following command in the WLAN Profile configuration mode:

ssid *ssid-name*

- *ssid-name* – Specifies the name of the WLAN.

To delete the SSID in the WLAN Profile, use the following command in the WLAN Profile configuration mode:

no ssid

Enabling/Disabling SSID Broadcast

After enabling SSID broadcast, any user can search it. After disabling the SSID broadcast, users cannot discover it. By default, the system enables the SSID broadcast.

To enable the SSID broadcast, use the following command in the WLAN configuration mode:

broadcast enable

To disable the SSID broadcast, use the following command in the WLAN Profile configuration mode:

no broadcast enable

Configuring Security Mode and Authentication Encryption Method

To configure the security mode and authentication encryption method, use the following command:

security {**none** | **wep authentication** {**open-system** | **shared-key**} {**wep40**|**wep104**}{**pass-phrase** | **raw-key**} *key* | {**wpa** | **wpa2** |**wpa-wpa2** | **wpa-psk** | **wpa2-psk** | **wpa-wpa2-psk** | **mac-psk**} **encryption** {**tkip** | **ccmp** | **tkip-ccmp**}[**pre-shared-key** { **pass-phrase** | **raw-key**} **psk**]}

- **none** – Do not perform the encryption.
- **wep authentication** {**open-system** | **shared-key**} {**wep40** | **wep104**} {**pass-phrase** | **raw-key**} *key* – Specifies the security mode as WEP (Wired Equivalent Privacy).
    - **open-system** | **shared-key** – Specifies the authentication mode, including the open system authentication (**open-system**) and shared key authentication (**shared-key**).

- wep40 | wep104 – Specifies the encryption method for the key.
- {pass-phrase | raw-key} *key* – Specifies the key form and the key value. **pass-phrase** represents to use character string as the key and **raw-key** represents to use hexadecimal number as the key. The key length of different configuration combinations is as follows: **wep40 pass-phrase** (5 characters), **wep40 raw-key** (10 hexadecimal numbers), **wep104 pass-phrase** (13 characters), **wep104 raw-key** (26 hexadecimal numbers).

- {wpa | wpa2 | wpa-wpa2 | wpa-psk | wpa2-psk | wpa-wpa2-psk | mac-psk } encryption {tkip | ccmp | tkip-ccmp} – Specifies the security mode, including WPA, WPA2, WPA-WPA2, WPA-PSK, WPA2-PSK, WPA-WPA2-PSK, and MAC-PSK.
  - wpa | wpa2 | wpa-wpa2 – WPA, WPA, and WPA-WPA2 are used for 802.1X authentication. WPA-WPS2-PSK is compatible with WPA and WPA-2.
  - wpa-psk | wpa2-psk | wpa-wpa2-psk – WPA-PSK, WPA2-PSK, and WPA-WPA2-PSK use the pre-shared key authentication. WPA-WPA-PSK is compatible with WPA-PSK and WPA2-PSK.
  - mac-psk – MAC-PSK integrates MAC authentication with WPA-WPA2-PSK authentication.
  - tkip | ccmp | tkip-ccmp – Specifies the data encryption method. **ccmp** has higher security, while **tkip-ccmp** has higher compatibility. Hillstone recommend you to use the **ccmp** method.
- pre-shared-key { pass-phrase | raw-key} psk – Specifies the form and the value of the pre-defined key. The pre-defined key length of different types is as follows: **pass-phrase** (8-63 characters), **raw-key** (64 hexadecimal numbers).



Notes: When using the WPA, WPA2, WPA-WPA2, or MAC-PSK method, you must specify the authentication server for the authentication task.

Enabling/Disabling User Isolation

After enabling the user isolation, users within one WLAN cannot access each other. User isolation enhances the security for different users. By default, the user isolation function is disabled. To enable the use isolation function, use the following command in the WLAN Profile Configuration mode:

station-isolation enable

To disable this function, use the following command in the WLAN Profile configuration mode:

no station-isolation enable

Configuring Maximum User Numbers

To specify the allowed maximum number of users that can access this WLAN, use the following command in the WLAN Profile configuration mode:

station-max-number *number*

- *number* – Specifies the allowed maximum number of users. The value ranges from 1 to 128, and the default value is 64.

To restore the setting to the default value, use the following command:

no station-max-number

Specifying the Authentication Server

When specifying the security mode as WPA, WPA2, WPA-WPA2, or MAC-PSK, you must select a configured AAA server as the authentication server for user identification. Use the following command in the WLAN Profile mode to select the AAA server:

radius-server *server-name*

- *server-name* - Specifies the name of the configured AAA server. When the security mode is WPA, WPA2, or WPA-WPA2, the system only support the RADIUS server. When the security mode is MAC-PSK, the system supports the local authentication server and RADIUS server and the username and password must be MAC address.

To delete the specified authentication server, use the following command in the WLAN Profile configuration mode:

no radius-server *server-name*

Binding the WLAN Profile to a WLAN Interface

The WLAN function can take effect after you bind the WLAN Profile to a WLAN interface. To bind the WLAN Profile to a WLAN interface, take the following steps in the interface configuration mode:

wlan profile *number*

- *number* - Specifies the number of the WLAN Profile that is bound to the current WLAN interface. After executing this command, the system binds the WLAN Profile of the specified number to the WLAN interface.

To cancel the binding, use the following command in the interface configuration mode:

no wlan profile



Notes: Since the A200W device has only two WLAN interfaces, a maximum of two WLAN profiles can be bound to the WLAN interface and cannot be bound repeatedly.

Configuring Global Parameters

The following sections introduce the global parameters of WLAN.

Configuring the Country/Region Code

Different countries or regions have different management and limitations on RF use. The country/region code determines the available frequency range, channel, and legal level of transmit power. To configure the country/region code, use the following command in the WLAN configuration mode:

country-zone-code *code*

- **code** - Specifies the country/region code. There are 133 country/region codes.The default value is US. For more information, see the table below:

Country/Region Code	Country/Region
AL	Albania
DZ	Algeria
AR	Argentina
AM	Armenia
AU	Aruba
AT	Australian
AZ	Austria
BS	Azerbaijan
BH	Bahrain
BD	Bangladesh
BB	Barbados
BY	Belarus
BE	Belgium
BZ	Belize

Country/Region Code	Country/Region
BM	Bermuda
BO	Bolivia
BA	Bosnia and Herzegovina
BR	Brazil
BN	Brunei
BG	Bulgaria
KH	Cambodia
CA	Canada
CL	Chile
CN	China
CO	Columbia
CR	Costa Rica
HR	Croatia
CY	Cyprus
CZ	Czechoslovakia
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EG	Egypt
SV	Salvador
EE	Estonia

Country/Region Code	Country/Region
FI	Finland
FR	France
GF	French Guiana
PF	French Polynesia
GE	Georgia
DE	Germany
GR	Greece
GL	Greenland
GD	Grenada
GP	Guadalupian
GU	Guam
GT	Guatemala
HT	Haiti
HN	Honduras
HK	Hong Kong
HU	Hungary
IS	Iceland
IN	India
ID	Indonesia
IR	Iran
IE	Ireland

Country/Region Code	Country/Region
IL	Israel
IT	Italy
JM	Jamaica
JP	Japan
JO	Jordan
KZ	Kazakhstan
KE	Kenya
KP	North Korea
KR	South Korea
KW	Kuwait
LV	Latvia
LB	Lebanon
LI	Liechtenstein
LT	Lithuania
LU	Luxembourg
MO	Macao
MK	Macedonia
MW	Malawi
MY	Malaysia
MT	Malta
MQ	Martinique

Country/Region Code	Country/Region
MU	Mauritius
YT	Mayotte
MX	Mexico
MC	Monaco
MA	Morocco
NP	Nepal
NL	Netherlands
AN	Netherlands Antilles
NZ	New Zealand
NI	Nicaragua
NO	Norway
OM	Oman
PK	Pakistan
PA	Panama
PG	Papua New Guinea
PY	Paraguay
PE	Peru
PH	Philippines
PL	Poland
PT	Portugal
PR	Puerto Rico

Country/Region Code	Country/Region
QA	Qatar
RE	Reunion
RO	Rumania
RU	Russia
RW	Rwanda
SA	Saudi Arabia
RS	Serbia
ME	Montenegro
SG	Singapore
SK	Slovakia
SI	Slovenia
ZA	South Africa
ES	Spain
LK	Sri Lanka
SE	Sweden
CH	Switzerland
SY	Syria
TW	Taiwan
TZ	Tanzania
TH	Thailand
TT	Trinidad and Tobago

Country/Region Code	Country/Region
TN	Tunisia
TR	Turkey
UG	Uganda
UA	Ukraine
AE	The United Arab Emirates
GB	United Kingdom
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZW	Zimbabwe

To restore the setting to the default value, use the following command in the WLAN Profile configuration mode:

no country-zone-code

Configuring the Operation Mode

To configure the operation mode, use the following command in the WLAN configuration mode:

radio-type {dot11a | dot11an | dot11b | dot11bgn | dot11g}

- **dot11a** – Specifies the operation mode as dot11a, which represents that the interface works in the 802.11a mode.

- **dot11an** – Specifies the operation mode as dot11an, which represents that the interface works in the 802.11n mode of 5GHz.
- **dot11b** – Specifies the operation mode as dot11b, which represents that the interface works in the 802.11b mode.
- **dot11bgn** – Specifies the operation mode as dot11bgn, which represents that the interface works in the 802.11n mode of 2.4GHz.
- **dot11g** – Specifies the operation mode as dot11g, which represents that the interface works in the 802.11g mode.
- **dot11ac** - Specifies the operation mode as dot11ac, which indicates that the wireless interface works in 5GHz 802.11AC mode (Only supported by SG-6000-A200W).

Configuring the Channel

The available channels you can select vary with the country/region code and RF type. When configuring the channels, use the following command in the WLAN configuration mode:

channel {**auto** | **channel-number**}

- **auto** – Asks the system to select the channel automatically. After the country/region code or the operation mode is changed, the system will select the channel automatically.
- **channel-number** – Specifies the channel number.

Specifying the Maximum Transmit Power

Sg-6000-A200W doesn't support to configure maximum transmit power and its default value is 100% of the maximum transmit power. The maximum transmit power varies with the country/region code and RF type. By default, there are four levels: 12.5% of the maximum transmit power, 25% of the maximum transmit power, 50% of the maximum transmit power, and 100% of the maximum transmit power. To configure the maximum transmit power, use the following command in the WLAN configuration mode:

power-management level {**1** | **2** | **3** | **4**}

- **1** – 12.5% of the maximum transmit power.
- **2** – 25% of the maximum transmit power.
- **3** – 50% of the maximum transmit power.
- **4** – 100% of the maximum transmit power.

Enabling/Disabling Wireless Multimedia Function

After enabling the wireless multimedia function, the system will raise the transmission priorities of the multimedia traffic such as audio and video. By default, the system has enabled wireless multimedia function. To enable this function, use the following command in the WLAN configuration mode:

wmm enable

To disable this function, use the following command:

no wmm enable

Viewing WLAN Settings

To view the WLAN settings, use the show command in any mode.

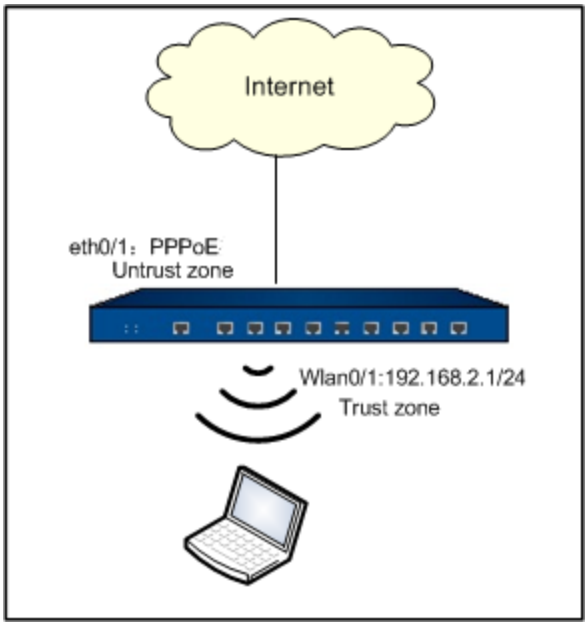
- View the configurations of WLAN Profile: **show wlan-profile** *number*
- View the information of the WLAN station: **show wlan-station** [**interface** *interface-name*][**mac** *mac-address*]
- View the global parameters: **show wlan**

WLAN Configuration Example

This section describes the configuration example of WLAN.

Requirement

Create a WLAN through the Hillstone device and ensure the users can access the LAN through wireless mode. The Hillstone device uses the routing mode. The ethernet0/1 uses the PPPoE mode to dial up and creates the WLAN whose SSID is test.



Configuration Steps

Step 1: Configure a DHCP address pool and PPPoE instance

```
#Create a DHCP address pool
hostname(config)# dhcp-server pool wlan_pool
hostname(config-dhcp-server)# address 192.168.2.2 192.168.2.254
hostname(config-dhcp-server)# netmask 255.255.255.0
hostname(config-dhcp-server)# gateway 192.168.2.1
hostname(config-dhcp-server)# dns 192.168.2.1
hostname(config-dhcp-server)# exit
#Create a PPPoE instance
hostname(config)# pppoe-client group pppoe1
hostname(config-pppoe-group)# auto-connect 10
```

```
hostname(config-pppoe-group)# idle-interval 5
hostname(config-pppoe-group)# user user1 password 123456
hostname(config-pppoe-group)# exit
hostname(config)#
```

Step 2: Configure the interface and the security zone

```
hostname(config)# internet wlan0/1
hostname(config-if-wla0/1)# zone trust
hostname(config-if-wla0/1)# ip address 192.168.2.1/24
hostname(config-if-wla0/1)# dhcp-server enable pool wlan_pool
hostname(config-if-wla0/1)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address pppoe setroute
hostname(config-if-eth0/1)# pppoe enable group pppoe1
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 3: Configure the DNS proxy

```
hostname(config)# dns-proxy rule
hostname(config-dns-proxy-rule)# ingress-interface wla0/1
hostname(config-dns-proxy-rule)# src-addr any
hostname(config-dns-proxy-rule)# dst-addr any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 202.106.1.1(The real DNS server )
hostname(config-dns-proxy-rule)# exit
hostname(config)# interface wla0/1
```

```
hostname(config-if-wla0/1)# dns-proxy
hostname(config-if-wla0/1)# exit
```

Step 4: Configure the SNAT rule

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from any to any eif ethernet0/1 trans-to eif-ip mode dynamicport sticky
rule id=1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 5: Configure the policy rule

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 6: Enable the WLAN function. By default, the WLAN function is enabled already

```
hostname(config)# wlan
hostname(config-wlan)# wlan enable
hostname(config-wlan)# exit
hostname(config)#
```

Step 7: Create the WLAN Profile

```
#The security mode is WPA2-PSK, the encryption method is CCMP, the pre-key is hillstone123
hostname(config)# wlan-profile 0
hostname(config-wlan-profile)# ssid test
hostname(config-wlan-profile)# security wpa2-psk encryption ccmp pre-shared-key pass-phrase hillstone123
hostname(config-wlan)# exit
hostname(config)#
#The security mode is WPA2, the encryption method is CCMP, the authentication server is radius1: 202.10.1.2
hostname(config)# aaa-server radius1 type radius
hostname(config-aaa-server)# host 202.10.1.2
hostname(config-aaa-server)# secret 123456
hostname(config-aaa-server)# exit
hostname(config)# wlan-profile 0
hostname(config-wlan-profile)# ssid test
hostname(config-wlan-profile)# security wpa2 encryption ccmp
hostname(config-wlan-profile)# radius-server radius1
hostname(config-wlan)# exit
hostname(config)#
```

Step 8: Bind the WLAN Profile to the WLAN interface

```
hostname(config)# interface wlan0/1
hostname(config-if-wla0/1)# wlan-profile 0
hostname(config-if-wla0/1)# exit
hostname(config)#
```

3G/4G

The third generation of mobile telecommunications technology supports the high speed data transmission. By configuring the 3G/4G function, users can access the Internet through wireless mode.

The 3G/4G function needs the support of ISP. Before configuring the 3G/4G function, you need to purchase the SIM card from the ISP, enable the data connection service, and obtain the following 3G/4G parameters: access point, username, password, dial-up string, and correctly installed SIM card.

Some A-series devices can access the Internet by external 4G modules of ZTE MF79U and MF833V being inserted into the USB port. Platforms that support external 4G modules are SG-6000-A200/A200W. The SIM card of the external 4G module is not hot swappable.

SG-6000-A200G4B support the wireless access mode. You can use the wireless mode to access the network.

Configuring 3G/4G Function

Configuring 3G/4G function includes the following items:

- Configuring basic parameters
- Managing the PIN code

Configuring Basic Parameters

You can configure the following basic parameters:

- Configuring the access point name
- Enabling/disabling the 3G/4G function
- Authenticating 4G module password
- Specifying the connection mode
- Configuring the dial-up string

- Specifying the verification method
- Specifying the route distance and weight
- Specifying the static IP
- Specifying the user information
- Configuring the schedule
- Manually connect/disconnect the 3G/4G connection

Configuring the Access Point Name

Before the 3G/4G dial-up, you must configure the APN (access potion name). You need to obtain the specific value of the APN from the ISP. To configure the APN, use the following command in the SIM card configuration mode:

apn *apn-name*

- *apn-name* – Specifies the access point name.

In the SIM card configuration mode, use the following command to delete the configuration of the APN:

no apn



Tip: To enter the SIM card configuration mode, use the **sim**command.

Enabling/Disabling the 3G/4G Function

By default, the 3G/4G function is enabled. After enabling the 3G/4G function, the system can trigger the 3G/4G dial-up. To enable the 3G/4G function, use the following command in the 3G/4G (cellular) interface configuration mode:

cellular enable

To disable the 3G/4G function, use the following command in the 3G/4G (cellular) interface configuration mode:

cellular disable



Tip: To enter the 3G/4G (cellular) interface configuration mode, use the command **interface cellular0/0**.

Authenticating 4G module password

If the device uses external 4G module of ZTE MF79U to access the Internet, the 4G module can be identified and used only after password authentication. Use the following command in the 3G/4G (cellular) interface configuration mode.

modem-loggin-password *password*

- *password* - Enter the authentication password for connecting the external 4G module. The value ranges from 1 to 31 characters.

Specifying the Connection Mode

You can specify the connection mode for the 3G/4G network, including 2G (GSM), 3G (WCDMA, CDMA2000, TD-SCDMA), 4G(FDD-LTE, TDD-LTE) and auto-adaption mode. By default, the system uses the auto-adaption mode. To specify the 3G/4G connection mode, use the following command in the 3G/4G (cellular) interface configuration mode:

connect-mode {**2G-only** | **3G-only** | **4G-only** | **auto**}

- **2G-only** – Uses the 2G network.
- **3G-only** – Uses the 3G network.
- **3G-only** – Uses the 4G network.
- **auto** – Uses the auto-adaption mode.

In the 3G/4G (cellular) interface configuration mode, use the following command to restore the connection to the default option:

no connect-mode

Configuring the Dial-up String

Ask your ISP to provide the dial-up string. To configure the dial-up string, use the following command:

dial *dial-number*

- *dial-number* – Specifies the dial-up number. The value ranges from 1 to 31 characters.

To restore the dial-up number to the default value, use the following command in the 3G/4G (cellular) mode:

no dial

Specifying the Verification Method

When 3G/4G dial-up establishes the connection, it needs to pass the PPP protocol verification. The device supports the following verification method: CHAP, PAP, and Any. To specify the verification method, use the following command in the 3G/4G (cellular) mode:

ppp authentication {chap | pap | any}

- **chap** – Uses the verification method of CHAP.
- **pap** - Uses the verification method of PAP.
- **any** - Uses the verification method of CHAP or PAP. any is the default option.

To restore the verification method to the default option, use the command **no ppp authentication**.

Specifying the Route Distance and Weight

To specify the route distance and weight, use the following command in the 3G/4G (cellular) interface mode:

ppp route {**distance** *value*| **weight** *value*}

- **distance** *value* – Specifies the route distance. The value ranges from 1 to 255. The default value is 1.
- **weight** *value* – Specifies the route weight. The value ranges from 1 to 255. The default value 1.

To restore the settings to the default values, use the following command:

no ppp route {**distance** | **weight**}

Specifying the Static IP Address

You can specify a static IP address and negotiate for using this static IP address, which can avoid the IP address changing. To specify a static IP address, use the following command in the 3G/4G (cellular) interface mode:

ppp static-ip *ip-address*

- *ip-address* – Specifies the static IP address.

To cancel the static IP address setting, use the following command:

no ppp static-ip

Specifying the Online Mode

3G/4G dial-up has two online modes as follows:

- Redial automatically: when the 3G/4G connection disconnects due to certain reasons and the disconnection time lasts the specified length of time, the system will redial automatically.
- Hang up after a specified idle time: When the idle time of the 3G/4G (cellular) interface reaches the specified value, the system will disconnection the 3G/4G connection.

The above two modes cannot be used meanwhile. Without configuring the schedule, the system will use the "hang up after a specified idle time" mode by default.

In the "redial automatically" mode, to specify the time between redial attempts, use the following command in the 3G/4G(cellular) interface configuration mode:

ppp redial-option auto-connect *time*

- *time* – Specifies the time (in seconds) between redial attempts. The value ranges from 0 to 10000 seconds. The default value is 0, which represents that the system does not use the "redial automatically" mode.

In the "hang up after a specified idle time" mode, to specify the idle time before hanging up, use the following command in the 3G/4G (cellular) interface configuration mode:

ppp redial-option idle-interval *time*

- *time* – Specifies the idle time (in seconds) before hanging up. The value ranges from 0 to 10000 seconds. The default value is 0, which represents that the system does not use the "hang up after a specified idle time" mode.

Use the **no ppp redial-option** command to restore the setting to the default value.

Specifying the User Information

You need to obtain the 3G/4G username and password from the ISP. To specify the user information, use the following command in the 3G/4G (cellular) interface configuration mode:

ppp user *user-name* **password** *password*

- *user-name* – Specifies the 3G/4G username.
- *password* – Specifies the corresponding password.

Use the following command to cancel the specified 3G/4G user information:

no user

Configuring the Schedule

The device supports the schedule. You can specify a schedule entry to make the 3G/4G (cellular) interface keep connected and disconnected individually during the specified time period. To

configure the schedule, use the following command in the instance configuration mode:

ppp schedule *schedule-name* [**connect** | **disconnect**]

- *schedule-name* – Specifies the name of the schedule entry.
- **connect** – The system will use the "on-demand dial-up" mode to connect to the internet during the period specified by the schedule entry.
- **disconnect** – The system will disconnect the connection during the period specified by the schedule entry.

To cancel the schedule settings, use the **no ppp schedule** command.

Manually Connect/Disconnect the 3G/4G Connection

You can manually connect/disconnect the 3G/4G connection. In any mode, use the following command to manually connect/disconnect the 3G/4G connection:

exec dial interface cellular0/0 {**connect** | **disconnect**}

- **connect** – Connect the 3G/4G connection.
- **disconnect** – Disconnect the 3G/4G connection.

Managing the PIN Code

PIN (Personal Identification Number) code is used to identify the user of the SIM card avoid the illegal use of the SIM card.

Managing the PIN code includes the following configurations:

- Enabling/Disabling the PIN code protection
- Automatically verifying the PIN code
- Manually verifying the PIN code

- Modifying the PIN code
- Unlocking the PIN code

Enabling/Disabling the PIN Code Protection

To enable the PIN code protection, you must first enter the correct PIN code. After the PIN code is verified, you can use the SIM card. The PIN code consists of 4-8 decimal numbers and you can obtain the PIN code from your ISP. To enable/disable the PIN code protection, use the following command in any mode:

exec pin verification {**enable** | **disable**} *pin*

- **enable** – Enables the PIN code protection.
- **disable** – Disables the PIN code protection.
- *pin* – Specifies the PIN code. The PIN code consists of 4-8 decimal numbers.



Notes: After three consecutive failed attempts at PIN code, the SIM card will be locked.

Automatically Verifying the PIN Code

After enabling the PIN code protection, you can save the PIN code in the system. After the system reboots, it can automatically verify the PIN code. To automatically verify the PIN code, use the following command in the SIM card configuration mode:

pin-verify-cipher *pin*

- *pin* – Specifies the PIN code. The PIN code consists of 4-8 decimal numbers.

Use **no pin-verify-cipher** to cancel the configurations of automatically verifying the PIN code.

Manually Verifying the PIN Code

To verify the PIN code manually, use the following command in any mode:

exec pin verify *pin*

- *pin* – Specifies the PIN code. The PIN code consists of 4-8 decimal numbers.

Modifying the PIN Code

To modify the PIN code, you must first enter the correct PIN code. After three consecutive failed attempts at PIN code, the SIM card will be locked. To modify the PIN code, use the following command in any mode:

exec pin modify *current-pin new-pin*

- *current-pin* – Specifies the current PIN code. The PIN code consists of 4-8 decimal numbers.
- *new-pin* – Specifies the new PIN code. The PIN code consists of 4-8 decimal numbers.

Unlocking the PIN Code

If the SIM card is locked, you need to obtain the PUK code from the ISP to unlock the SIM card and set the new PIN code. To use the PUK code to unlock the SIM card, use the following command:

exec pin unlock *puk new-pin*

- *puk* – Specifies the PUK code.
- *new-pin* – Specifies the new PIN code. The PIN code consists of 4-8 decimal numbers.



Notes: After ten consecutive failed attempts at PUK code, the SIM card will be invalid.

Viewing the 3G/4G Configurations

To view the 3G/4G configurations, use the corresponding show commands in any mode:

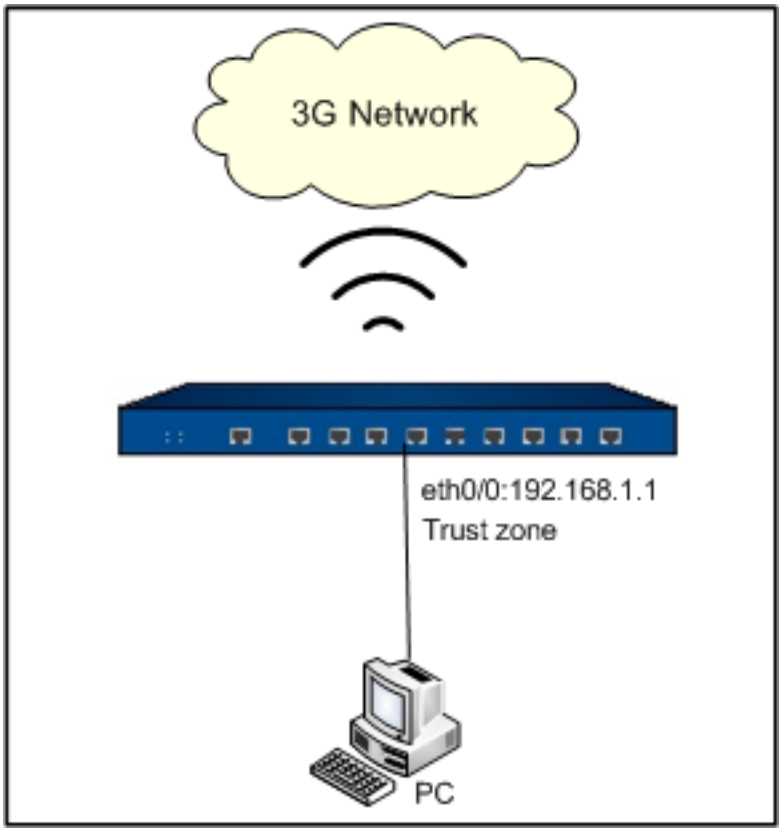
- View the 3G/4G data card information and 3G/4G connection configurations: **show cellular**
- View the corresponding configurations of PPP: **show ppp**
- View the SIM card information: **show sim**

3G Configuration Example

This section describes the configuration example of 3G.

Requirement

Use the Hillstone device with the 3G data card inserted to access the 3G network by 3G dial-up. The Hillstone device uses the routing mode. The ethernet0/1 belongs to the trust security zone and user's PC connects to this ethernet0/1.



Configuration Steps

Step 1: Configure basic parameters of 3G, for example, WCDMA

```
hostname(config)# sim
hostname(config -sim)# apn uninet
hostname(config -sim)# exit
hostname(config)# interface cellular0/0
hostname(config -if-cel0/0)# dial *99#
hostname(config -if-cel0/0)# ppp authentication any
hostname(config-if-cel0/0)# ppp user none password none
hostname(config -if-cel0/0)# end
hostname# exec dial interface cellular0/0 connect
```

Step 2: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 3: Configure the IP address, gateway, and DNS of the user's PC. The IP address must be at the same subnet as the IP address of the ethernet0/0. The DNS address must be a public DNS address

LLDP

Network devices are increasingly diverse, and their configurations are respectively complicate. Therefore, mutual discovery and interactions in information of system and configuration between

devices of different manufacturers are necessary to facilitate management. LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol defined in IEEE 802.1ab, which provides a discovery method in link layer network. By means of the LLDP technology, the system can quickly master the information of typology and its changes of the layer-2 network when the scale of network expands rapidly.

By means of LLDP, the LLDP information of the device, including the device information, system name, system description, port description, network management address and so on, can be sent in the form of standard TLV (Type Length Value) multicast message from the physical port to the directly-connected neighbor. If the neighbor enables LLDP too, then neighbor relations will be established between both sides. When the neighbor receives these messages, they are stored in the form of MIB in the SNMP MIB database, in order to be utilized by the network management system to search and analyze the two-layer topology and the problems in it of the current network.

LLDP Work Mode

The 4 work modes of LLDP are listed below:

- txrx: the system transmits and receives LLDP messages.
- tx: the system only receives LLDP messages.
- rx: the system only transmits LLDP messages.
- disable: the system neither transmits nor receives LLDP messages.

Configuring LLDP

Configuring LLDP can enable neighbor devices' collection of network typology changes.

- Enabling/Disabling global LLDP
- Enabling/Disabling LLDP of port
- Configuring LLDP work mode
- Configuring the initialization delay of port

- Configuring the transmission delay of LLDP messages
- Configuring the transmission interval of LLDP messages
- Configuring TTL multiplier
- Displaying LLDP local information
- Displaying LLDP neighbor information of port
- Displaying LLDP statistical information
- Displaying LLDP status information

Enabling/Disabling Global LLDP

LLDP is enabled only when the "Global LLDP" and the "LLDP of Port" are enabled at the same time, so the corresponding port can transmit and receive LLDP messages.

- By default, the global LLDP and the LLDP of port are both disabled.
- When the global LLDP is enabled, the LLDP of all the ports of the system will be enabled.
- When the global LLDP is disabled, the LLDP of all the ports of the system will be disabled.
- When the global LLDP is enabled, the user does not have to modify LLDP configuration, for LLDP can be enabled by default configuration.

To enable or disable the global LLDP, in the global configuration mode, use the following command:

- Enable: **lldp global enable**
- Disable: **lldp global disable**

Enabling/Disabling LLDP of Port

Before enabling LLDP of port, in the global configuration mode, use **interface** *ethernetm/n* command to enter the configuration mode of the port which needs to enable LLDP.

To enable or disable LLDP of port, in the interface configuration mode, use the following command:

- Enable: **lldp enable**
- Disable: **lldp disable**



Notes: Only the physical port of the device supports enabling LLDP. Logical port does not support this function.

Configuring LLDP Work Mode

The user can configure the work mode of LLDP , specifying whether the port transmits or receives the LLDP messages. By default, the LLDP work mode of port is txrx (transmits and receives the LLDP messages).

To configure the LLDP work mode of port, in the interface configuration mode, use the following command:

lldp admin-status {disable | rx | tx | txtx}

- disable: the port neither transmits nor receives LLDP messages.
- rx: the port only transmits LLDP messages.
- tx: the port only receives LLDP messages.
- txrx: the port transmits and receives LLDP messages.

Recover the default LLDP work mode, use the following command:

no lldp admin-status

Configuring the Initialization Delay of Port

When the LLDP work mode of the port changes, the system will operate initialization on the port. Configuring the initialization delay of the port can avoid continuous initialization of the port due to frequent changes of the LLDP work mode.

To configure the initialization delay of port, in the global configuration mode, use the following command:

lldp reinit-delay *delay-value*

- *delay-value* - Specifies the initialization delay of port. The measurement is second-based, and the range is from 1 to 10.

To recover the default initialization delay of port, use the following command:

no lldp reinit-delay

Configuring the Transmission Delay of LLDP Messages

Transmission delay refers to the minimal delay time before the LLDP messages are sent to the neighbor device when the state of the local device frequently changes.

To configure the transmission delay of LLDP messages, in the global configuration, use the following command:

lldp message-transmission delay *delay-value*

- *delay-value* - Specifies the transmission time delay of LLDP messages. The measurement is second-based, and the range is from 1 to 900.

To recover the default transmission delay of LLDP messages, use the following command:

no lldp message-transmission delay

Configuring the Transmission Interval of LLDP Messages

Transmission interval refers to the time period of transmitting the LLDP message to the neighbor device when the state of the local device state remains stable.

To configure the transmission interval of LLDP messages, in the global configuration mode, use the following command:

lldp message-transmission interval *interval*

- *interval* - Specifies the transmission interval of LLDP messages. The measurement is second-based, and the range is from 1 to 3600, the default value is 30s.

To recover the default transmission interval of LLDP messages, use the following command:

no lldp message-transmission interval

Configuring TTL Multiplier

TTL (Time to Live) refers to the living time of the local device information in the neighbor device.
TTL multiplier is used to adjust the living time of the local device information in the neighbor device. The computational formula is: TTL = Transmission Interval × TTL Multiplier.

To configure TTL multiplier, in the global configuration mode, use the following command:

lldp message-transmission hold-multiplier *hold-multiplier*

- *hold-multiplier* - Specifies the TTL multiplier value. The range is from 1 to 100, and the default value is 4.

To recover the default TTL multiplier value, use the following command:

no lldp message-transmission hold-multiplier

Displaying LLDP Local Information

To view the DDLP local information, in any mode, use the following command:

show lldp local-information [**global** | *interface-name*]

- **global** - Displays the LLDP local information to be sent to the neighbor device.
- *interface-name* - Displays the LLDP local information to be sent from the specified port to the neighbor device.

Displaying LLDP Neighbor Information of Port

To view the LLDP neighbor information of port, in any mode, use the following command:

show lldp neighbor-information [*interface-name*]

- *interface-name* - Displays the LLDP information sent from the neighbor device to the local device and received by the specified port. If this parameter is not specified, the LLDP neighbor information of all the ports will be shown.

Displaying LLDP Statistical Information

To view the LLDP statistical information, in any mode, use the following command:

show lldp statistics [**global** | *interface-name*]

- **global** - Displays the global statistical information.
- *interface-name* - Displays the LLDP statistical information of the specified port.

Displaying LLDP Status Information

To view the LLDP status information, in any mode, use the following command:

show lldp status [*interface-name*]

- *interface-name* - Displays the LLDP status information of the specified port.

Hardware Fast Forwarding

Introduction

In most cases, when a firewall receives a packet, it will upload the packet to the CPU and then send the processed packet to a specified egress interface for forwarding. To reduce the burden on the CPU, some firewall devices support the hardware fast forwarding function. For subsequent messages that meet the fast forwarding conditions, instead of sending them to the CPU for processing, the device quickly forward them by using the hardware acceleration engine. The use of the hardware fast forwarding function not only effectively reduces the burden on the CPU, but also significantly improves the service processing performance of the device, enabling the firewall device to more efficiently cope with high traffic and high concurrency network environment.

You can configure the hardware fast forwarding function only by using the CLI.

Precautions and Limits

Precautions

The following traffic needs to be uploaded to the CPU for processing and therefore will not be hardware fast-forwarded:

- Traffic that requires tunnel encapsulation and de-encapsulation on the firewall device;
- Traffic that requires complex traffic control or traffic statistics functions, such as traffic that requires iQoS, Netflow functions;
- Traffic that requires layer 7 application security detection, such as traffic requiring IPS, AV detection;
- Non-TCP/UDP messages, such as ICMP messages and DHCP messages;
- Messages sent and received by interfaces that do not support the hardware fast forwarding function, such as the HA interface and MGT interface of the device.

Limits

Because the messages of some functions need to be uploaded to the CPU for processing, there may be the following limitations on the use of some functions after the hardware fast forwarding function is enabled:

- If you adjust the configuration of iQoS/IPS when the hardware fast forwarding function is enabled, the new configuration will only take effect on the traffic of the newly created session after the configuration, and cannot take effect on the traffic that has already been hardware fast forwarded. To make the new configuration to take effect on the traffic that has already been hardware fast forwarded, you need to run the **clear session** command to clear the session corresponding to the traffic that has already been hardware fast forwarded.

Enabling/Disabling Hardware Fast Forwarding

Supported models

- A series: SG-6000-A7600 and SG-6000-A6800

On the device that supports hardware fast forwarding, the hardware fast forwarding function is enabled by default. To disable hardware fast forwarding, in global configuration mode, use the following command:

hardware fast-forward disable

In global configuration mode, use the following command to restore to the default configuration of the hardware fast forwarding function:

no hardware fast-forward disable

Enabling/Disabling the Fast Aging Function of TCP Hardware Fast Forwarding Flow Table Entries

Supported models

- A series: SG-6000-A7600 and SG-6000-A6800

The hardware fast forwarding flow table is the basis of whether the message can be forwarded quickly. After the firewall device receives a message, it first determines whether the message matches the corresponding hardware fast forwarding flow table entry. If the message matches the hardware fast forwarding flow table entry, the message will be forwarded quickly based on the information in the table entry and does not need to be sent to the CPU for processing. If the message does not match the hardware fast forwarding flow table entry, it will be sent to the CPU for processing and forwarding.

To save the space of the hardware fast forwarding flow table, the system will delete the TCP hardware fast forwarding flow table entries after they have not been matched continuously for a certain period of time (the time depends on the number of TCP sessions, the more the number, the longer the time, usually from 2 to 8 seconds). If, after the table entries is deleted, the system receives another TCP session that can match this table entry, the system will re-establish the TCP hardware fast forward flow table entry for it.

By default, this function is enabled. To disable this function, in global configuration mode, use the following command:

hardware fast-forward session fast-aging disable

In global configuration mode, use the following command to restore to the default configuration of the function:

no hardware fast-forward session fast-aging disable

Enabling Congestion Packet Loss on Egress Interface for Device

Supported models

- A series: SG-6000-A7600 and SG-6000-A6800

In some special high-traffic application scenarios, when congestion occurs on the egress interface of the device, some packets on all ingress interfaces on the device may be dropped, resulting in packet loss on the uncongested ingress interfaces as well. To avoid this issue, you can enable the congestion packet loss function on egress interface for the device. Once enabled, the device will only drop some packets on the egress interface, and the ingress interface will no longer lose packets. By default, this function is disabled, and you can enable it as needed.

To enable congestion packet loss on egress interface for device, in global configuration mode, use the following command:

fpga-egress-congest-avoid-enable

In global configuration mode, use the following command to restore to the default configuration of the function:

no fpga-egress-congest-avoid-enable

Viewing Configuration Information of Hardware Fast Forwarding

Supported models

- A series: SG-6000-A7600 and SG-6000-A6800

The configuration information of hardware fast forwarding of the device includes the status of hardware fast forwarding and the status of the fast aging function of hardware fast forwarding flow table.

To view configuration information of hardware fast forwarding, in any mode, use the following command:

show hardware fast-forward

Sample output:

```
hostname#show hardware fast-forward
=============================================================
=========================
Hardware Fast-forward Information
=============================================================
=========================
Hardware Fast-forward: enable
Hardware session Fast-aging: enable
=============================================================
=========================
```

Chapter 2 Policy

This section contains the following contents:

- "Security Policy" on Page 365: This section introduces the basic concepts of security policies, including policy rules, policy groups, web page redirection, and viewing policy rules.
- "Share Access" on Page 416: This section introduces how to configure shared access rules, configure shared access signature database, and share access logs.
- "ARP Defense" on Page 425: This section introduces how to configure the ARP defense functions to protect your network against various ARP attacks.

Security Policy

Overview

Policy is designed to control the traffic forwarding between security zones/segments. By default, Hillstone devices will deny all traffic between security zones/segments, while the policy can identify which flow between security zones or segments will be permitted and which will be denied based on the policy rules.

Basic Elements of Policy Rules

Policy rules permit or deny traffic between security zone(s)/segment(s). The basic elements of policy rules are service type of the traffic, source and destination address/zone, and action.

- Source zone/address - The source zone/address of the traffic.
- Destination Zone/Address - The destination zone/address of the traffic.
- Service - The service type of the traffic.
- Action - The actions for processing traffic include Permit, Deny, Tunnel, From tunnel and WebAuth.

Below is a CLI example which permits the ICMP traffic from any address in the trust zone to any address in the untrust zone to pass through.

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
```

- Source Address - Any, i.e., any address. It is the default address entry in the address book.
- Destination Address - Any, i.e., any address. It is the default address entry in the address book.
- Service – ICMP
- Action - Permit, i.e., this kind of traffic is permitted to pass through the device.

Defining a Policy Rule

Generally a policy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's source zone/address, destination zone/address, service type, and role. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in StoneOS are arranged in a specific order. When traffic flows into a Hillstone device, the device will query for policy rules in the list by turns, and processes the traffic according to the first matched rule.

The maximum global policy rule numbers may vary from different Hillstone models.

Introduction to Profile

The combination of the profile and security policy allows the Hillstone devices to implement fine-grained control over the application layer security policy. Profile defines different operations for different kinds of applications, which can simplify system configurations. StoneOS support nine types of profiles, namely URL filter profile, Web content profile, Web posting profile, email filter profile, IM control profile, HTTP/FTP control profile, anti-virus profile, IPS profile and GTP profile. Each profile category can be configured with an action for a specific application.

QoS Tag

StoneOS supports the QoS tag function in policy rules. You can add the QoS tag to a policy rule that permits the traffic to pass through.



Tip: For more information about QoS, see "QoS" of "Traffic Management".

Configuring Access Control for a Policy

The combination of the ACL Profile and policy rule allows the Hillstone devices to access control over the message based on a policy, such as source/destination MAC address etc.

Configuring an ACL Profile

The ACL profile needs to be configured in the ACL profile configuration mode. To enter the ACL profile configuration mode, in the global configuration mode, use the following command:

acl-profile*acl-profile-name*

- *acl-profile-name* – Specifies the name of the ACL profile. After executing the command, the system will create a ACL profile with the specified name, and enter the ACL profile configuration mode; if the specified name exists, the system will directly enter the ACL profile configuration mode. You can specify up to 64 ACL profiles.

To delete the specified ACL Profile, in the global configuration mode, use the command **no acl-profile***acl-profile-name*.

Configuring an Access Control Rule

To configure an Ipv4 access control rule, in the ACL Profile configuration mode, use the following command:

sequence *id* {**drop** | **pass**} [**both** | **forward** | **backward**] [**src-mac** *src-mac-address*] [**dst-mac***dst-mac-address*] [**dscp** *dscp-value*]

- *id* – Specifies the ID of the access control rule. .The range is 1 to 32.
- **drop** | **pass** – Specifies the action for the access control rule, drop or pass.
- **both** | **forward** | **backward** – Specifies the traffic direction of the access control rule.
- **src-mac***src-mac-address* – Specifies the source MAC address of the access control rule.
- **dst-mac***dst-mac-address* – Specifies the destination MAC address of the access control rule.
- **dscp** *dscp-value* – Specifies the DSCP value, the range is 0 to 63.

To delete the specified access control rule, in the ACL Profile configuration mode, use the command **no sequence** *id*.



Notes: For more information about configuring access control rules and control actions for an IPv6 policy, see Access Control for an IPv6 Policy.

Configuring the Default Action

When no access control rule is hit, the system will take the specified default access control action. To configure the default action, in the ACL Profile configuration mode, use the following command:

default-action {**drop** |**pass**}

- **drop** | **pass** – Specifies the default action for the access control rule, drop or pass. If default action is not specified, the system will adopt Pass.

To restore to the default control action Pass, in the ACL Profile configuration mode, use the command **no default-action**.

Viewing ACL Profile Information

To view the ACL profile configuration, in any mode, use the following command:

show acl-profile [*acl-profile-name*]

- *acl-profile-name* – Shows the configuration of the specified ACL profile. If this parameter is not specifies, the command will show the configurations of all the ACL profiles.

Configuring a Policy Rule

You can configure a policy rule via CLI to control the traffic destined to the device. The configuration includes:

- Switching to the multi-zone mode
- Creating a policy rule
- Editing a policy rule

- Specifying the default action
- Configuring Policy User-defined Attributes
- Specifying That the Policy Matches the Post-DNAT Destination Address

Entering the Policy Configuration mode

To enter the policy configuration mode, in the global configuration mode, use the following command:

policy-global

Switching to the Multi-Zone Mode

The system supports switches between the multi-zone mode and the single-zone mode. In the single-zone mode, one policy supports only one source zone and one destination zone. In the multi-zone mode, one policy supports multiple zones. In this case, users can manage policies more easily when there are fewer policies needed configuring in the system. One policy supports up to 16 source/destination zones. By default, the system applies the single-zone mode. To switch to the multi-zone mode, in the policy configuration mode, use the following command:

multi-zone-enable

In the policy configuration mode, use the following command to restore to the single-zone mode:

no multi-zone-enable



Notes: You can use this command to restore to the single-zone mode only when multi-zone policies are not configured in the system. Otherwise, the command fails.

Creating a Policy Rule

To create a policy rule, in the global configuration mode or policy configuration mode, use the following command:

rule [**id** *id*] [**name** *name*] [**top** | **before** {**name** *rule-name*| *id*} | **after** {**name** *rule-name*| *id*}] [**role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] [**from** {**host** *host-name* | **range** *min-ip max-ip* |*src-addr* }] [**to** {**host** *host-name* | **range** *min-ip max-ip* |*dst-addr* }] [**from-zone** *zone-name* **to-zone** *zone-name*] [**service** *service-name*] [**application** *app-name*] [**permit** | **deny** | **tunnel** *tunnel-name* | **from-tunnel** *tunnel-name* | **webauth** | **portal-server** *server-name*]

- **id** *id* - Specifies the ID of the policy rule. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system.
- **name** *name* – Specifies the name of the policy rule.
- **top** | **before** {**name** *rule-name*| *id*} | **after** {**name** *rule-name*| *id* - Specifies the location of the policy rule. By default, the newly-created policy rule is located at the end of all the rules.
    - **top** Specifies the location of the policy rule to the top of all rules.
    - **before** {**name** *rule-name*| *id*} – Specifies the location of the policy rule before the rule of specified ID or name.
    - **after** {**name** *rule-name*| *id* – Specifies the location of the policy rule after the rule of specified ID or name.
- **role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name* - Specifies the role/user/user group for the policy rule.
    - **role** {**UNKNOWN** | *role-name*} – Specifies the role name. **UNKNOWN** is the role reserved by the system, i.e., the role that is neither authenticated nor statically bound.
    - **user** *aaa-server-name user-name* – Specifies the user. *aaa-server-name* is the AAA server the user belongs to, and *user-name* is the name of the user.
    - **user-group** *aaa-server-name user-group-name* – Specifies the user group. *aaa-server-name* is the AAA server the user group belongs to, and *user-group-name* is the name of the user group.

- **from** {**host** *host-name* | **range** *min-ip max-ip* | *src-addr* } – Specifies the source address of the policy rule.
  - **host** *host-name* - The source address entry for the host defined in the address book.
  - **range** *min-ip max-ip* – The source address entry for the IP addresses defined in the address book.
  - *src-addr* – The address entry defined in the address book.
- **to** {**host** *host-name* | **range** *min-ip max-ip* | *dst-addr* } – Specifies the destination address of the policy rule.
  - **host** *host-name* – The destination address entry for the host defined in the address book.
  - **range** *min-ip max-ip* – The destination entry for the IP addresses defined in the address book.
  - *dst-addr* - The address entry defined in the address book.
- **from-zone** *zone-name* – Specifies the source zone of the policy rule.
- **to-zone** *zone-name* - Specifies the destination zone of the policy rule.
- **service** *service-name* - Specifies the service name of the policy rule. *service-name* is the service defined in the service book.
- **application** *app-name* – Specifies the application name for the policy rule. *app-name* is the application name you defined in the application book.
- **permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name*| **webauth** } - Specifies the action of the policy rule, including:
  - **permit** - Permits the traffic to pass through.
  - **deny** - Denies the traffic.

- **tunnel** - For the traffic from local to a peer, this option allows the traffic to pass through the VPN tunnel.
- **fromtunnel** - For the traffic from a peer to local, if this action is selected, StoneOS will first determine if the traffic originates from a tunnel. Only such traffic will be permitted.
- **webauth** - Performs Web authentication on the matched traffic.

After switching to the multi-zone mode, repeat the above commands to add more source/destination zones. Each policy supports up to 16 source/destination zones. If Any zone is configured, you cannot configure other zones at the same time.

For example, to create a policy rule that permits ICMP service from any address to any address, use the following commands:

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
Rule id 5 is created.
```

To delete the policy rule, in the global configuration mode or policy configuration mode, use the following command:

no rule {**id** *id* | **name** *name*}

- **id** *id* – Deletes the policy rule of the specified ID.
- **name** *name* - Deletes the policy rule of the specified name.



Tip: For information about how to configure parameters of a policy rule, see "Editing a Policy Rule".

Editing a Policy Rule

You can edit improper parameters for the policy rule in the policy rule configuration mode. To enter the policy rule configuration mode, in the global configuration or policy configuration mode, use the following command:

rule [**id** *id*] [**top** | **before** {**name** *name* | *id*} | **after** {**name** *name* | *id*]

After entering the policy rule configuration mode, to edit the policy rule, use the following commands:

- Name/rename a policy rule: **name** *policy-name*
- In the single-zone mode, use the following commands to specify/edit/delete zones:
    - To specify/edit a source security zone: **src-zone** *src-zone*
    - To delete a source security zone: **no src-zone**(When this command is executed, there is no source zone in the policy)
    - To specify/edit a destination security zone: **dst-zone** *dst-zone*
    - To delete a destination security zone: **no dst-zone**(When this command is executed, there is no destination zone in the policy)
- In the multi-zone mode, use the following commands to specify/edit/delete zones:
    - To specify/edit a source zone: **src-zone** *src-zone*(In the multi-zone configuration mode, when the source zone is not the Any, repeat this command to configure up to 16 zones.)
    - To delete a source zone: **no src-zone** [*src-zone*](By repeating this command, you can delete specific zones one by one. If the zone is not selected, this command deletes all zones. In this case, there is no source zone in the policy.)

    - To specify/edit a destination zone: **dst-zone** *dst-zone*(In the multi-zone configuration mode, when the destination zone is not the Any, repeat this command to configure up to 16 zones.)
    - To delete a destination zone: **dst-zone** [*dst-zone*](By repeating this command, you can delete specific zones one by one. If the zone is not selected, this command deletes all zones. In this case, there is no destination zone in the policy.)
- Add the source address of the address entry type: **src-addr** *src-addr*
- Delete the source address of the address entry type:**no src-addr** *src-addr*
- Add the source address of the IP member type: **src-ip** *ip/netmask*
- Delete the source address of the IP member type: **no src-ip** *ip/netmask*
- Add the source address of the host member type: **src-host** *host-name*
- Delete the source address of the host member type: **no src-host** *host-name*
- Add the source address of the IP range type: **src-range** *min-ip* [*max-ip*]
- Delete the source address of the IP range type: **no src-range** *min-ip* [*max-ip*]
- Add the source device: **src-device** *device-name*
- Delete the source device: **no src-device** *device-name*
- Add the destination address of the address entry type: **dst-addr** *dst-addr*
- Delete the destination address of the address entry type: **no dst-addr** *dst-addr*
- Add the destination address of the IP member type: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destination address of the IP member type: **no dst-ip** {*ip/netmask* | *ip-address net-mask*}

- Add the destination address of the host member type: **dst-host** *host-name*
- Delete the destination address of the host member type: **no dst-host** *host-name*
- Add the destination address of the IP range type: **dst-range** *min-ip* [*max-ip*]
- Delete the destination address of the IP range type: **no dst-range** *min-ip* [*max-ip*]
- Add the destination device: **dst-device** *device-name*
- Delete the destination device: **no dst-device** *device-name*
- Add the domain name: **domain***domain-name* （The *domain-name* field can be 1 to 255 characters in length. You can add up to 1,024 domain names. The domain, destination address, and application cannot be configured at the same time.）
- Delete the domain name: **no domain***domain-name*
- Specify the host book: **domain-book***domain-book-name* （You can specify up to 8 host books. The host book, destination address, and application cannot be configured at the same time.）
- Delete the host book: **no domain-book***domain-book-name*
- Add the service type: **service** *service-name*
- Delete the service type: **no service** *service-name*
- Add / Delete the service rule: The service rule includes the protocol type and port number of the service. You can configure the service rule of the policy according to the required protocol and port number. For adding / deleting the service rule, refer to Configuring the Service Rule.
- Add the application type: **application** *application-name*
- Delete the application type: **no application** *application-name*

- Specify the role: **role** {**UNKNOWN** | *role-name*}
- Delete the role: **no role** {**UNKNOWN** | *role-name*}
- Specify the user: **user** *aaa-server-name user-name*
- Delete the user: **no user** *aaa-server-name user-name*
- Specify the user group: **user-group** *aaa-server-name user-group-name*
- Delete the user group: **no user-group** *aaa-server-name user-group-name*
- Edit the action: **action** {**permit** | **deny** | **tunnel** | **fromtunnel** | **webauth**}
- Configure the VLAN ID: **vlan-id** *vlan-id*
- Delete the VLAN ID: **no vlan-id** *vlan-id*
- Configure the schedule: **schedule** *schedule-name*
- Delete the schedule: **no schedule** *schedule-name*



Tip: By default, the configured policy rule will take effect immediately. If you apply a schedule to the policy rule, the rule will only take effect in the specified time defined in the schedule. You can configure up to 8 schedules for a policy rule, and the effective time of the policy rule is the sum of all time configured in the schedules.

- Adding the description: **description** *description*(the length of *description* is 1 to 255 bytes)
- Delete the description: **no description** *description*
- Edit the QoS tag of the rule: **policy-qos-tag** *tag*(the value range of *tag* is 1 to 1024)
- Delete the QoS tag of the rule: **no policy-qos-tag** *tag*

- Bind the anti-virus profile: **av** {*av-profile-name* | **no-av**} (**no-av** indicates binding the pre-defined Anti-Virus Profile named no-av, i.e., no Anti-Virus detection.)
- Cancel the anti-virus profile binding: **no av**
- Bind the IPS profile: **ips** {*ips-profile-name* | **no-ips**} (**no-ips** indicates binding the predefined IPS Profile named no-ips, i.e., no IPS detection.)
- Cancel the IPS profile binding: **no ips**
- Bind the HTTP/FTP control profile: **behavior** {*behavior-profile-name* | **no-behavior**} (**no-behavior** indicates binding the predefined HTTP/FTP control profile named no-behavior, i.e., no HTTP/FTP control.)
- Cancel the HTTP/FTP control profile binding: **no behavior**
- Bind the Web content profile: **contentfilter** {*contentfilter-profile-name* | **no-contentfilter**} (**no-contentfilter** indicates binding the predefined Web content profile named no-contentfilter, i.e., no Web content filter.)
- Cancel the Web content profile binding: **no contentfilter**
- Bind the Email filter profile: **mail** {*mail-profile-name* | **no-mail**} (**no-mail** indicates binding the predefined Email filter Profile named no-mail, i.e., no Email filter.)
- Cancel the Email filter profile binding: **no mail**
- Bind the IM control profile: **im** {*im-profile-name* | **no-im**} (**no-im** indicates binding the pre-defined IM control Profile named no-im, i.e., no IM control.)
- Cancel the IM control profile binding: **no im**
- Bind the Web posting profile: **webpost** {*webpost-profile-name* | **no-webpost**} (**no-webpost** indicates that you bind the predefined profile no-webpost to the policy rule and the system will not check the Web posting information.)

- Cancel the Web posting profile binding: **no webpost**
- Bind the URL filter profile: **url** {*url-profile-name* | **no-url**} (**no-url** indicates that you bind the predefined profile no-url to the policy rule and the system will not check and filter the URLs.)
- Cancel the URL filter profile binding: **no url**
- Bind the GTP profile: **gtp-profile** *profile-name*
- Cancle the GTP profile binding: **no gtp-profile**
- Bind the ACL profile: **acl** *acl-profile-name*
- Cancel the ACL profile binding: **no acl**.

Enabling/Disabling a Policy Rule

By default, the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule. To enable or disable the policy rule, in the policy rule configuration mode, use the following commands:

- Disable: **disable**
- Enable: **enable**

Log Management of Policy Rules

- For the policy rules of action Permit, logs will be generated when the matched traffic session starts and ends.
- For the policy rules of action Deny, logs will be generated when the matched traffic is denied.

Before using this function, make sure the log function for the traffic is enabled. In the global configuration mode, use the command **logging traffic on**. To configure the log management of policy rules, in the policy rule configuration mode, use the following command:

log {**policy-deny** | **session-start** | **session-end**}

- **policy-deny** - Generates logs when the matched traffic is denied. This parameter is applicable to the policy rules of action Deny.
- **session-start** - Generates logs when the matched traffic starts its session. This parameter is applicable to the policy rules of action Permit.
- **session-end** - Generates logs when the matched traffic ends its session. This parameter is applicable to the policy rules of action Permit.

To cancel the log management configuration, in the policy rule configuration mode, use the command **no log** {**policy-deny** | **session-start** | **session-end**}.

In addition, for the traffic from the source security zone to the destination security zone that is not matched to any policy rule, you can specify whether to generate logs. By default, the system does not generate log for such kind of traffic. To generate log for such traffic, in the global policy configuration mode, use the following command:

log policy-default

To restore to the default value, in the global policy configuration mode, use the following command:

no log policy-default

Configuring the Service Rule

When configuring the service rule of the policy rule, you can add a predefined or user-defined service that have been configured in the service book. When the required service does not exist in the service book, the administrator can specify the protocol type and port number of the service by configuring the service rules, thus simplifying the configuration steps of the policy.

To add a service rule of TCP or UDP type, in the policy configuration mode, use the following command:

service-rule {**tcp** | **udp**} **dst-port***min-port* [*max-port*] [**src-port***min-port* [*max-port*]]

- **tcp** | **udp** - Specifies the protocol type of the service rule: TCP or UDP.
- **dst-port***min-port* [*max-port*] – Specifies the destination port number of the service rule. If the destination port number is a number range, then *min-port* is the minimum destination port number, and *max-port* is the maximum destination port number. If *max-port* is not configured, system will use *min-port* as the single destination port number. The value range is 0 to 65535
- **src-port***min-port* [*max-port*] – Specifies the source port number of the service rule. If the source port number is a number range, then *min-port* is the minimum source port number, and *max-port* is the maximum source port number. If *max-port* is not configured, system will use *min-port* as the single source port number. The value range is 0 to 65535.

To add a service rule of ICMP type, in the policy configuration mode, use the following command:

service-ruleicmp type*type-value* [**code***min-code* [*max-code*]]

- *type-value* – Specifies the ICMP type value of the user-defined service. The value range is 0（Echp-Reply）, 3（Destination-Unreachable）, 4（Source Quench）, 5（Redirect）, 8（Echo）, 11（Time Exceeded）, 12（Parameter Problem）, 13（Timestamp）, 14（Timestamp Reply）, 15（Information Request）, 16（Information Reply）, 17（Address Mask Request）, 18（Address Mask Reply）, 30（Traceroute）, 31（Datagram Conversion Error）, 32（Mobile Host Redirect）, 33（IPv6 Where-Are-You）, 34（IPv6 I-Am-Here）, 35（Mobile Registration Request）, 36（Mobile Registration Reply）.
- **code** *min-code* [*max-code*] – Specifies the ICMP code value for the user-defined service. If the ICMP code is a number range, then *min-port* is the minimum code, and *max-port* is the maximum code. If *max-port* is not configured, system will use *min-port* as the single code. The value range is 0 to 15.

To add a service rule of ICMPv6 type, in the policy configuration mode, use the following command:

service-ruleicmpv6 type*type-value* [**code** *min-code* [*max-code*]]

- *type-value* – Specifies the ICMPv6 type value. For more information about the value range, see Appendix 1: ICMPv6 Type and Code.
- **code** *min-code* [*max-code*] – Specifies the ICMPv6 code value for the user-defined service. If the ICMPv6 code is a number range, then *min-port* is the minimum code, and *max-port* is the maximum code. If *max-port* is not configured, system will use *min-port* as the single code. The value range is 0 to 255.

To add a service rule of SCTP type, in the policy configuration mode, use the following command:

service-rule sctp dst-port *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]

- **dst-port** *min-port* [*max-port*] – Specifies the destination port number of the service rule. If the destination port number is a number range, then *min-port* is the minimum destination port number, and *max-port* is the maximum destination port number. If *max-port* is not configured, system will use *min-port* as the single destination port number. The value range is 0 to 65535
- **src-port** *min-port* [*max-port*] – Specifies the source port number of the service rule. If the source port number is a number range, then *min-port* is the minimum source port number, and *max-port* is the maximum source port number. If *max-port* is not configured, system will use *min-port* as the single source port number. The value range is 0 to 65535.

To add a service entry of other types, in the policy configuration mode, use the following command:

service-ruleprotocol*protocol-number*

- *protocol-number* – Specifies the protocol number of the service rule. The value range is 1 to 255.

To delete the specified service rule, use one of the following commands.

- **noservice-rule**{**tcp** | **udp**} **dst-port***min-port* [*max-port*] [**src-port***min-port* [*max-port*]]
- **no service-rule icmp type***type-value* [**code***min-code* [*max-code*]]

- **no service-rule icmpv6 type***type-value* [**code** *min-code* [*max-code*]]
- **no service-rule sctp dst-port** *min-port* [*max-port*] [**src-port** *min-port* [*max-port*]]
- **no service-rule protocol***protocol-number*

Specifying the Default Action

You can specify the default action for the traffic that is not matched to any configured policy rule. StoneOS will process the traffic according to the specified default action. By default StoneOS will deny such traffic. To specify the default action as Permit, in the global policy configuration mode, use the following command:

default-action permit

To restore to the default action of Deny, in the global policy configuration mode, use the following command:

no default-action permit

Moving a Policy Rule

Each policy rule is labeled with a unique ID and name. When traffic flows into a Hillstone device, the device will query policy rules by turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed by the command show policy is the query sequence for policy rules (in the descending order). You can also specify the position for the policy rule when creating it, or modifying the position of the policy rule in the policy configuration mode. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. To move a policy rule, in the policy rule configuration mode, use the following command:

move {**name** *name* | *id*} {**top** | **bottom** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} }

- **name** *name* | *id* – Specifies the policy rule ID or name that you want to move.
- **top** – Moves the policy rule to the top of all rules.

- **before** {**name** rule-name | id} – Moves the policy rule before the rule of specified ID or name.
- **after** {**name** rule-name | id} – Moves the policy rule after the rule of specified ID or name.

Viewing Resource Usage in Policy Rules

To view the resource usage of the source address, destination address, and service in policy rules, that is, to view the proportion of the number of source address, destination address, and service configured in policy rules to the total available number, in any mode, use the following command:

show policy resource

For example:

```
hostname(config)# show policy resource
Resource usage:
address: 2%(10000 of 480000; src-addr usage: 5000; dst-addr usage: 5000; current available: 470000)
service: 4%(10000 of 240000; current available: 230000)
```

In the above case, there are 5000 configured source addresses and 5000 configured destination addresses in the policy rules. The configured source and destination addresses account for 2% of the total number of configurable addresses in the system, and the number of remaining available addresses in the system is 470000. The number of configured services in the policy rules is 1000, accounting for 4% of the total number of configurable services in the system.

Rule Redundancy Check

To ensure the validity of policy rules, the system can perform redundancy check on policy rules to check whether redundant or conflict policies exist. The system considers the source zone, source address, destination zone, destination address, service, application, and VLAN ID of policy rules as redundancy check items. It sequentially compares high-priority policies with low-

priority policies for analysis and lists the analysis results in the redundancy check list for further processing, which helps you streamline policies.



Notes: The Redundancy Check function takes effect only on policy rules whose action is "Permit" or "Deny".

Specifying the Issue Types of Redundancy Check

Before you perform redundancy check, you need to specify the issue types of redundancy check, including four types: completely conflict (**completely-conflict**), completely redundancy (**completely-redundancy**), partly conflict (**partly-conflict**), and partly redundancy (**partly-redundancy**).

The four issue types are described as follows:

- Completely redundancy: The redundancy check items of Policy A are completely covered by Policy B. When Policy A has lower priority than Policy B and the actions are the same, Policy A will be checked as completely redundant.
- Partly redundancy: Each redundancy check item of two policy rules has partial overlap, and the actions are the same. The policy rule with a lower priority will be checked as partially redundant.
- Completely conflict: The redundancy check items of Policy A are completely covered by Policy B. When Policy A has lower priority than Policy B and the actions conflict, Policy A will be checked as completely conflict.
- Partly conflict: Each redundancy check item of two policy rules has partial overlap, and the actions conflict. The policy rule with a lower priority will be checked as partly conflict.

To specify the issue types of redundancy check, in policy configuration mode, use the following command:

redundancy-check-type {[**completely-conflict**] [**completely-redundancy**] [**partly-conflict**] [**partly-redundancy**]}

- [completely-conflict] [completely-redundancy] [partly-conflict] [partly-redundancy] – Specifies the issue types of redundancy check. You can specify multiple issue types at the same time. Different issue types are separated with spaces.

If not specified, the default issue types of redundancy check are Completely redundancy and Completely conflict.

To restore to the default issue types of redundancy check, in policy configuration mode, use the command **no redundancy-check-type**.

Viewing the Issue Types of Redundancy Check

To view the issue types of current redundancy check, in any mode, use the following command:

show policy redundancy-check-type

Starting Redundancy Check

To start redundancy check of policy rules, in any mode, use the following command:

exec policy redundancy-check start

Stopping Redundancy Check

To stop redundancy check of policy rules, in any mode, use the following command:

exec policy redundancy-check stop

Viewing Redundancy Check Results

To view the redundancy check results of policy rules, including the policy ID, policy name, issue type, and policy status, in any mode, use the following command:

show policy redundancy-check-result [[**id***id*] [**name***name*] [**type***type*]]

- **id***id* – Shows the redundancy check results of the specified policy ID. Valid values: 1 to 4000.

- **name***name* – Shows the redundancy check results of the specified policy name. Valid values: 1 to 95 characters.
- **type***type* – Shows the redundancy check results of the specified issue type. The issue types include completely conflict (**completely-conflict**), completely redundancy (**completely-redundancy**), partly conflict (**partly-conflict**), and partly redundancy (**partly-redundancy**).

Viewing the Coverage of Policy Rules

To view the coverage of policy rules in the redundancy check results of policy rules, including the policy ID and covered policy ID, in any mode, use the following command:

show policy redundancy-check

Configuring Ignored Time of Redundant Policy Rules

For the redundant policy rules checked by the system, you can ignore the redundant policy rules as required and specify the ignore time for them. The system will no longer check the redundancy of the policy rule during the ignore time. You can configure the ignored time of redundant policy rules in one of the following ways:

- Configuring Ignored Days
- Configuring Expiration Time for Ignorance

Configuring Ignored Days

To configure ignore days of redundant policy rules, in policy rule configuration mode, use the following command:

redundancy-ignore-days {*time_value* | **forever**}

- *time_value* – Specifies the ignored time. Valid values: 1 to 3650 days. Within the ignored time, the system no longer check the redundancy of the policy rule.

Configuring Expiration Time for Ignorance

To configure expiration time for ignored redundant policy rules, in policy rule configuration mode, use the following command:

redundancy-expire-time*time_value*

- *time_value* – Specifies the expiration timestamp for ignorance, ranging from -1 to 9223372036854775807. The timestamp indicates the total number of seconds from January 1, 1970 (00:00:00 GMT, or 08:00:00 Beijing time) until now. Once specified, the system will no longer check redundancy in the policy rule until the expiration of the specified ignore duration. Setting it to -1 indicates permanent ignorance of the redundant policy rule.



Notes: If the same redundant policy rule is configured to be ignored by using two different methods simultaneously, only the ignore time configured later will take effect. It is recommended to use the "Configuring Ignored Days" method.

Unignoring Redundant Policy Rules

In policy rule configuration mode, use the **no redundancy-ignore-days** or **no redundancy-expire-time** command to unignore redundant policy rules.

Viewing Ignored Redundant Policy Rules

To view ignored redundant policy rules, including the policy ID, policy name, and expiration time, in any mode, use the following command:

show policy redundancy-ignore

Clearing Redundant Check Results

To clear the redundant check results of policy rules, in any mode, use the following command:

exec policy redundancy-check clear

Configuring the Session Timeout Period of Policy Rule

The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. After the timeout period is reached, the session is disconnected. To configure the session timeout of policy rule, in policy configuration mode, use the following command:

session-timeout {**day***day_value* | **second***second_value*}

- **day***day_value* – Specifies the timeout period. Valid values: 1 to 1000. Unit: days.
- **second***second_value* – Specifies the timeout period. Valid values: 1 to 65535. Unit: seconds.

Viewing the Status of Persistent-Connection Session

The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. To view the status of persistent-connection session, in any mode, use the following command:

Configuring Policy Audit Function

System support the policy audit function. When you create or modify the policy rule/, you can use this function to add policy audit comments of the policy rule/aggregation policy so that you can understand the change reasons and change history of the policy rule.



Notes: The policy audit function is available only for :

- SG-6000 A-Series devices installed with hard disks (excluding SG-6000-A1600/A1800/A2200).
- SG-6000 K-Series devices installed with hard disks.
- SG-6000 X-Series devices installed with hard disks (excluding SG-6000-X9180/X10800).
- SG-6000 CloudEdge devices installed with hard disks.



For details about whether the device supports hard disks, see the Hardware Reference Guide.

Enabling/Disabling the Policy Audit Function

By default, the policy audit function is disabled. To enable this function, in the global configuration mode, use the following command:

audit-comment-enable

To disable this function, in the global policy configuration mode, use the following command:

no audit-comment-enable

Adding the Audit Comment

To add policy audit comments to the policy rule, in any mode, use the following command:

audit-comment rule id *id* **comment** *comment*

- **rule id** *id* - Specifies the ID of the policy rule that needs to add audit comments.
- **comment** *comment* - Specifies the audit comment content. The range is 1-255 characters.

Viewing Policy Audit Enabled Status

To view the policy audit function enabled status, in any mode ,use the following command:

show audit-comment-status



Notes:

- Policy audit comment is optional. When you create or modify the policy rule, you can add policy audit comments to policy rules according to requirements.
- For viewing the audit history information of policy rules, you can only view it via WebUI. Please refer to **StoneOS_WebUI_User_Guide**.

Policy Group

You can organize some policy rules together to form a policy group, and configure the policy group directly.

Configuring Policy Group

You can perform the following operations on a policy group through CLI:

- Creating/Deleting a policy group
- Enabling/Disabling a policy group
- Modifying/Deleting the Descriptions of a policy group
- Adding/Deleting a policy rule member
- Renaming a Policy Group
- Configuring a policy group for VSYS Profile

Creating/Deleting a Policy Group

To create a policy group, in the global configuration mode, use the following command:

policy-group *group-name*

- *group-name* – Specifies the name of the policy group. The length is 1 to 95 characters.

After executing this command, the CLI will enter the policy group configuration mode.

To detele a policy group, in the global configuration mode, use the following command:

no policy-group *group-name*

Enabling/Disabling a Policy Group

Policy group is enabled by default. To disable or enable the policy group, in the policy group configuration mode, use the following command:

- Enable: **enable**
- Disable: **disable**



Notes:

- After disable or enable the policy group, the enabled status of policy rules in policy group are modified at the same time.
- Policy rules cannot be disabled or enabled when they are referenced.

Modifying/Deleting the Descriptions of a policy group

In the policy group configuration mode, use the following command to modify the description of a policy group.

description *description*

- *group-name* – Specifies the new description. You can enter at most 255 characters.

In the policy group configuration mode, use the following command to delete the description of a policy group.

no description

Adding/Deleting a Policy Rule Member

To add a policy rule member to the policy group, in the policy group configuration mode, use the following command:

rule *id*

- *id* – Specifies the policy rule ID.

To delete a policy rule member to the policy group, in the policy group configuration mode, use the following command:

no rule *id*



Notes: A policy rule only can be added to a policy group.

Renaming a Policy Group

To rename a policy group entry, in the global configuration mode, use the following command:

rename policy-group *old-name new-name*

- *old-name* – Specifies the old name for the policy group.
- *new-name* – Specifies the new name for the policy group.

Configuring a policy group for VSYS Profile

To configure a policy group for VSYS Profile, in the VSYS Profile configuration mode, use the following command:

policy-group max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – Specifies the maximum quota (*max-num*) and reserved quota (**reserve** *reserve-num*) of policy group in VSYS. The reserved quota and maximum quota vary from different platforms. The reserved quota should not exceed the maximum quota.

Viewing Policy Group Information

To view the policy group information, in any mode, use the following command:

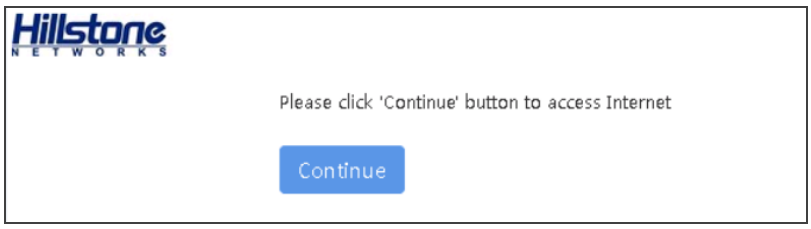
show policy-group [*name*]

- *name* – Specifies the name of policy group for viewing the information.

User Online Notification

The user online notification function redirects your HTTP request to a new notification page when you visit Internet for the first time. In the process, a prompt page (see the picture below)

will be shown first, and after you click **Continue** on this page, the system will redirect to the specified notification page. If you want to visit your original URL, you need to type the URL address in your Web browser.



To configure the user online notification function, take the following steps:

1. Enable WebAuth.
2. Create a policy rule to specify the traffic that will be redirected and the network resources accessible to the traffic.
3. Configure the notification page URL for the controlled traffic.

Notes: To make the user online notification function take effect, the action for the policy rule must be Permit.

Configuring the User Online Notification URL

To configure the user online notification URL, in the policy rule configuration mode, use the following command:

web-redirect [*url*]

- *url* – Specifies the user online notification URL. The length is 1 to 127 characters. The URL format should be http://www.abc.com or https://www.abc.com. If the parameter is not specified, the webpage will be redirected to the URL originally specified by the user.

To cancel the user online notification URL, in the policy rule configuration mode, use the following command:

no web-redirect



Notes: For more information about how to enter the policy rule configuration mode, see Entering the Policy Configuration mode

Configuring the Idle Time

The idle time refers to the time that a user keeps online without traffic transmitting. If an HTTP request exceeds the idle time, it will be redirected to the user online notification page again. To configure the idle time, in the global configuration mode, use the following command:

web-redirect idle-time *time-value*

- *time-value* – Specifies the idle time. The value range is 3 to 1440 minutes. The default value is 30.

To restore to the default idle time, in the global configuration mode, use the following command:

no web-redirect idle-time

Customizing the Logo Picture

You can change the logo picture and customize your own user online notification page. To import the logo picture, you need zip the picture first, and then in the execution mode, use the following command:

import customize webredirect from {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**user** *user-name* **password** *password* [**vrouter** *vrouter-name*]] - Obtains the logo picture from the FTP server, and specifies the IP address, VRouter, username and password of the server. If no username and password are specified, you will log into the server anonymously.
- **tftp server** *ip-address* [**vrouter** *vrouter-name*] - Obtains the logo picture from the TFTP server, and specifies the IP address and VRouter of the TFTP server.
- *file-name* - Specifies the name of the zip file.



Notes: The uploaded zip file should include the "logo.jpg" file.

To restore to the default logo picture, in any mode, use the following command:

exec customize webredirect default

Viewing Online Notification Users

To view the detailed information of online notification users, in any mode, use the following command:

show web-redirect-user

Configuring Policy Custom Attributes

To facilitate the management and query of policies, the system supports to configure custom attributes for policies and filter policies based on these attributes.

Custom attributes greatly facilitate administrators in filtering, categorizing, and querying policies. For example, in a company where the network administrator has deployed thousands of policies and is not fully aware of the usage of certain policies, custom attributes can be used to clearly view information such as the user and expiration date of the current policy. By configuring a custom attribute for the policy as 'User' and setting the 'User' in the policy rule to 'Zhang San,' you can quickly filter and find policy rules where the user is 'Zhang San' by using 'Zhang San' as the filter condition.

The procedure is as follows:

1. Configure custom attributes mapping
2. Configure custom attributes for policy rules
3. View custom attributes

Configuring Custom Attributes Mapping

Configure the mapping of policy custom attributes. That is to say, specify the mapping between different custom attribute IDs and their names. The system supports a maximum of 8 policy

custom attributes, each corresponding to an ID. You can configure attribute names based on your needs.

To configure policy custom attributes mapping, in global configuration mode, take the following steps:

user-defined-attribute policyattribute-index*id***attribute-name***name*

- **attribute-index***id* - Specifies the ID of the policy custom attribute. Valid values: 1 to 8.
- **attribute-name***name* - Specifies the name of the policy custom attribute, which can be 1 to 31 characters in length.

In global configuration mode, use the **no user-defined-attribute policyattribute-index***id* command to delete the configured policy custom attributes mapping.

Configuring Custom Attributes for Policies

You can configure the content of custom attributes for policies as required.



Notes: After you configure the policy custom attributes mapping, the custom attributes configuration item is displayed in the policy, enabling you to configure the custom attribute. For more information, see Configuring Policy Custom Attributes Mapping.

To configure custom attributes for policies, in policy configuration mode, use the following command:

user-defined-attribute {**attribute-index***id* | **attribute-name***name*} **content***content*

- **attribute-index***id* - Specifies the ID of the configured policy custom attribute.
- **attribute-name***name* - Specifies the name of the configured policy custom attribute.
- **content***content* - Specifies the content of the custom attribute, which can be 1 to 31 characters in length.

In policy configuration mode, use the **no user-defined-attribute** {**attribute-index***id* | **attribute-name***name*} command to delete the configured custom attribute content.

Viewing Policy Custom Attribute Information

In any mode, use the following command to view information about the policy custom attributes mapping, including the attribute ID, attribute name, and the number of times the attribute is used by the policy.

show user-defined-attribute policy

In any mode, use the following command to view information about the policy that contains the specified custom attribute content.

show policy user-defined-attribute {**attribute-index***id* | **attribute-name***name*} **content***content* [**accurate**]

- **attribute-index***id* - Specifies the ID of the configured policy custom attribute.
- **attribute-name***name* - Specifies the name of the configured policy custom attribute.
- **content***content* - Specifies the content contained in the custom attribute that you want to view, which can be 1 to 31 characters in length.
- **accurate** - Specifies to use exact match to search for the policy that matches the custom attribute content. If not specified, fuzzy match is used.

Specifying That the Policy Matches the Post-DNAT Destination Address

The system allows you to specify that the policy matches the pre-DNAT destination address or post-DNAT destination address. By default, the policy matches the pre-DNAT destination address.

To specify that the policy matches the post-DNAT destination address, in policy configuration mode, use the following command:

match-after-dnat

In policy configuration mode, use the no form of the command above to restore that the policy matches the pre-DNAT destination address.

no match-after-dnat

Viewing Policy Rules That Contain Specified Service Keywords

A service contains information such as protocol type and port number. After services are referenced by policy rules, you can filter policy rules by service content with a fuzzy search.

To view policy rules that contain specified service keywords, in any mode, use the following command:

show policy service keyword*string*

- *string* – Specifies the keyword, which needs to be 1 to 95 characters in length.

Viewing Policy Rule Information

You can view the detailed information of all policy rules or a specified policy rule. And also you can view the detailed information of the policy matching the five-tuple filtering conditions (including source IP address, destination IP address, protocol, source port and destination port).

To view the detailed information of the policy rules, in any mode, use the following command:

show policy [**id** *id*] [**from** *src-zone*] [**to** *dst-zone*] [**src-addr** *src-addr*] [**dst-addr** *dst-addr*] [**protocol** | **service** *service-name*] [**application** *application-name*] [**description** *description*] [**name** *name*] [**name-filter** *filter-name*] [**user** {**filter-fuzzy** *filter-name* | **filter-precise** *aaa-server-name filter-name*}] [**user-group** {**filter-fuzzy** *filter-name* | **filter-precise** *aaa-server-name filter-name*}] [**role filter-fuzzy** *filter-name*][**family** {*ipv4* | *ipv6*}]

- **id** *id* - Shows the detailed information of the specified policy rule.
- **from** *src-zone* - Shows the detailed information of the policy rule whose source security zone is the specified zone.
- **to** *dst-zone* - Shows the detailed information of the policy rule whose destination security zone is the specified zone.
- **src-addr** *src-addr* – Shows the detailed information of the specified source address of the IP range type.

- **dst-addr** *dst-addr* – Shows the detailed information of the specified the destination address of the address entry type.
- **protocol** | **service***service-name* - Shows the detailed information of the specified protocol (**protocol**) or service (**service***service-name*).
- **service** *service-name* – Shows the detailed information of the specified service type.
- **application** *application-name* – Shows the detailed information of the specified application type.
- **description** *description* – Shows the detailed information of the specified name rule.
- **name** *name* – Shows the detailed information of the specified name rule.
- **name-filter** *filter-name* – Shows the detailed information of all rules whose name includes the specified keyword.

  user – Shows policy rules with the specified user name.
- **user-group** – Shows policy rules with the specified user group name.
- **role** – Shows policy rules with specified role name.
- **filter-fuzzy** *filter-name* | **filter-precise** *aaa-server-namefilter-name* – Specifies the query method is fuzzy query (**filter-fuzzy**) or precise query (**filter-precise**).
    - **filter-fuzzy** *filter-name* – Specifies the query method is fuzzy query. Fuzzy query is performed by specifying the keyword of the user name / user group name/ role name. By fuzzy matching the specified keyword, a list of all policies that contain this keyword in their user name/ user group name/ role name will be returned.
    - **filter-precise** *aaa-server-name filter-name* – Specifies the query method is precise query. Precise query is performed by specifying a precise user name/ user group name. By precise matching the specified user name/ user group name, a list of all policies that

have the same user name/ user group name will be returned. If a policy's user group contains the specified user name/ user group name, this policy will also be listed in the search results.

- **family** {**ipv4** | **ipv6**} – Shows the detailed information of the IPv4 or IPv6 policy rules. Note: This keyword is available only when the system version is IPv6.



Notes:

- Fuzzy query and precise query are mutually exclusive and cannot be selected at the same time.
- If the filter condition User is selected together with other filter conditions (relationship between each filter condition is **AND**), filter condition User should be placed last.

To view the policy rules corresponding to TCP or UDP protocol types, in any mode, use the following command:

show policy protocol {**tcp** | **udp**} [**dst-port** {*port-number* | **range** *min-port max-port*}] [**src-port** {*port-number* | **range** *min-port max-port*}]

- **tcp** | **udp** – Shows the detailed information of the policy rule with the protocol type of TCP or UDP.
- **dst-port**{ *port-number*| **range** *min-port max-port*} – Shows the detailed information of the specified destination port. *port-number*is a single destination port number. If the destination port number is in a range, *min-port* is the minimum destination port number, *max-port* is the maximum destination port number, and the range is 0 to 65535.
- **src-port** {*port-number*| **range** *min-port max-port*} - Shows the detailed information of the specified source port. *port-number*is a single source port number. If the source port number is in

a range, *min-port* is the minimum source port number, *max-port* is the maximum source port number, and the range is 0 to 65535.



Notes: *min-port*must be less than or equal to *max-port*. When *min-port* is equal to *max-port*, it means that a single port number is specified.

To view the policy rules corresponding to ICMP or ICMPv6 protocol types, in any mode, use the following command:

show policy protocol {**icmp** | **icmpv6**} [**type** *type-number* [**code** {*code-number* | **range***min-code max-code*}]]

- **icmp** | **icmpv6** – Shows the detailed information of the policy rule with the protocol type of ICMP or ICMPv6.
- **type***type-number* – Shows the detailed information of the policy rule with the specified ICMP type or ICMPv6 type.
- **code** {*code-number*| **range** *min-code max-code*} - Shows the detailed information of the policy rule with the specified ICMP code or ICMPv6 code. *code-number*is a single code. If the code is in a range, *min-code*is the minimum code, *max- code*is the maximum code. The code value of ICMP Protocol type ranges from 0 to 15, and that of ICMPv6 protocol type ranges from 0 to 255.



Notes: *min-code*must be less than or equal to *max- code*. When*min-code*is equal to *max- code*, it means that a single code.

show policy protocol sctp [**dst-port** {*port-number* | **range** *min-port max-port*}] [**src-port** {*port-number* | **range** *min-port max-port*}]

- **dst-port**{ *port-number*| **range** *min-port max-port*} – Shows the detailed information of the specified destination port. *port-number*is a single destination port number. If the destination

port number is in a range, *min-port* is the minimum destination port number, *max-port* is the maximum destination port number, and the range is 0 to 65535.

- **src-port** {*port-number*| **range** *min-portmax-port*} - Shows the detailed information of the specified source port. *port-number*is a single source port number. If the source port number is in a range, *min-port* is the minimum source port number, *max-port* is the maximum source port number, and the range is 0 to 65535.



Notes: *min-port*must be less than or equal to *max-port*. When *min-port* is equal to *max-port*, it means that a single port number is specified.

To view the policy rules corresponding to other specified protocol types, in any mode, use the following command:

show policy protocol *protocol-number*

- *protocol-number* – Shows the detailed information of the policy rule with the specified protocol number. The protocol number is from 1 to 255.

Viewing the current policy configuration information of the device

To view the current policy configuration information of the device, in any mode, use the following command:

show configuration policy [**name** *name* | **id** *id* | **by-line**]

- **name** *name* – Shows the policy configuration information of the specified policy name in a single line.
- **id** *id* – Shows the policy configuration information of the specified policy ID in a single line.
- **by-line** – Shows all the policy configuration information in a single line.

Policy Hit Count

StoneOS supports statistics on policy hit counts, i.e., it counts how many times the traffic matches a policy rule. Each time the inbound traffic matches a certain policy rule, the hit count will increment by one automatically. To view the policy hit count statistics, in any mode, use the following command:

show policy hit-count [**id** *id* | **name** *name* | [**from** *src-zone*] [**to** *dst-zone*] **top** {10 | 20 | 50 | **all** }]

- **id** *id* - Shows the policy hit count statistics of the specified ID rule.
- **name** *name* – Shows the policy hit count statistics of the specified name rule.
- **from** *src-zone* - Shows the policy hit count statistics of the rule whose source security zone is the specified zone.
- **top** {10 | 20 | 50 | **all** } - Shows the policy hit count statistics of the top 10, 20, 50 matched rules , or shows the policy hit count statistics of all policy rules in descending order.

Examples:

```
Shows the policy hit count statistics of all matched
rules.
hostname(config)# show policy hit-count
Most hit policy rules:
=============================================================-
============================
No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count
------------------------------------------------------------------------------
1 14 trust trust Any Any Any PERMIT 0
2 4 untrust trust Any Any Any PERMIT 1
3 3 trust untrust Any Any Any PERMIT 761697
```

4 1 Any Any Any Any Any PERMIT 64203455

==========

Show the policy hit count statistics of the specified ID rule.

hostname(config)# **show policy hit-count id 1**

Policy id 1 is hit 342424 times

Show the policy hit count statistics of the specified name rule.

SG-6000(config)# **show policy hit-count name a**

Policy "a" is hit 0 times

Show the policy hit count statistics of the top 10 matched rules.

hostname(config)# **show policy hit-count top 10**

Most hit policy rules:

==========

No. Id Src-zone Dst-zone Src-addr Dst-addr Service Action Hit-count

---

1 4 trust trust any any http permit 40029

2 6 zone2 untrust addr1 any any deny 7487

3 3 zone2 untrust s1 d1 ftp permit 3834

4 29 trust untrust any any any permit 2899

5 14 zone1 zone2 s2 any pop3 permit 2046

Show the policy hit count statistics of the all policy rules in descending order.

hostname(config)# **show policy hit-count top all**

Most hit policy rules:

```
=============================================================-
============================

No. Id Src-zone Dst-zone Src-addr Dst-addr Service Applica~ Action Hit-count

-----------------------------------------------------------------------

1 1 Any Any Any Any Any PERMIT 64212319

2 3 trust untrust Any Any Any PERMIT 762070

3 4 untrust trust Any Any Any PERMIT 1

4 14 trust trust Any Any Any PERMIT 0

=============================================================-
============================
```

Viewing Statistics on Policy Rule Hits

In any mode, you can use the corresponding show commands to view statistics on policy rule hits, including rule ID, hit counts, first-hit time, last-hit time, days since last-hit time, policy created time, and policy status (enabled/disabled).

To view hit statistics of all policy rules:

show policy statistic-info

To view hit statistics of the policy rule whose ID is the specified ID:

show policy statistic-info id *id*

- **id** *id* - Specifies the policy rule ID.

To view hit statistics of the policy rule whose days since created are longer than the specified days:

show policy statistic-info days-since-created *value*

- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the policy rule whose days since first hit are longer than the specified days:

show policy statistic-info days-since-first-hitted *value*

- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

To view hit statistics of the policy rule whose days since last hit are longer than the specified days:

show policy statistic-info days-since-last-hitted *value*

- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days.

Use the following command to view hit statistics of the combinedly filtered policy rules. The filters include that policy rules' days since last hit are longer than the specified days, policy rules' days since first hit are longer than the specified days, and policy rules' days since created are longer than the specified days.

show policy statistic-info [**days-since-last-hitted** *value*] [**days-since-first-hitted** *value*] [**days-since-created** *value*]

- **days-since-last-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the policy rule whose days since last hit are longer than the specified days.
- **days-since-first-hitted** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the policy rule whose days since first hit are longer than the specified days.
- **days-since-created** *value* - Specifies the days. The value range is from 1 to 3650 days. View hit statistics of the policy rule whose days since created are longer than the specified days.

To view hit statistics of all policy rules in ascending or descending order of rule ID:

show policy statistic-info sorted-by id {**ascending** | **descending**}

- **id** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of rule ID.

To view hit statistics of all policy rules in ascending or descending order of hit counts:

show policy statistic-info sorted-by hit-count {**ascending** | **descending**}

- **hit-count** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of hit counts.

To view hit statistics of all policy rules in ascending or descending order of policy creation time:

show policy statistic-info sorted-by created-time {**ascending** | **descending**}

- **created-time** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of policy creation time.

To view hit statistics of all policy rules in ascending or descending order of policy first hit time:

show policy statistic-info sorted-by first-hitted-time {**ascending** | **descending**}

- **first-hitted-time** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of policy first hit time.

To view hit statistics of all policy rules in ascending or descending order of days since policy last hit:

show policy statistic-info sorted-by last-hitted-days {**ascending** | **descending**}

- **last-hitted-days** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of days since policy last hit.

To view hit statistics of all policy rules in ascending or descending order of policy last hit time:

show policy statistic-info sorted-by last-hitted-time {**ascending** | **descending**}

- **last-hitted-time** {**ascending** | **descending**} - Specifies that hit statistics of all policy rules are displayed in ascending or descending order of policy last hit time.

Clearing Statistics on Policy Rule Hits

In any mode, use the following command to clear statistics on policy rule hits:

clear policy statistic-info {**all** | **id** *id*}

- **all** | **id** *id* - Clear rule hit statistics of all policy rules (**all**), or specified ID rules (**id** *id*).

Enabling/Disabling Traffic Statistics of Policies

The Traffic Statistics function of policies can be used to collect statistics of the system traffic that hits policy rules, including the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes. By default, the Traffic Statistics function is disabled. To enable this function, run the following commands:

policy-traffic-statistic

In policy configuration mode, run the **no policy-traffic-statistic** command to disable the Traffic Statistics function of policies.

Viewing the Status of Policy Traffic Statistics

To check whether the Traffic Statistics function of policies is enabled, run the following command in any mode:

show policy traffic-statistic-status

Enabling/Disabling the Delay Address Update Time Function

The system supports the Delay Address Update Time function. After you modify multiple addresses in the address book at a time, the system does not immediately synchronize the modified addresses to the policy referencing the address book. Instead, synchronization occurs after a specified delay period. This avoids slow configuration deployment due to frequent updates in address book members. By default, the Delay Address Update Time function is disabled.

To enable the Delay Address Update Time function, in policy configuration mode, use the following command:

delay-address-update-time *time_value*

- *time_value* – Specifies the delay time. Valid values: 1 to 3 seconds. After you specify the delay time, if an address in the address book referenced by a policy changes, the system does not immediately synchronize the modified address to the policy. Instead, synchronization occurs after the specified delay time.

To disable the Delay Address Update Time function, in policy configuration mode, use the following command:

no delay-address-update-time

Configuring the Policy Assistant

The policy assistant can help users generate targeted policies more quickly and accurately. With the function, system can analyze the traffic of a specified policy ID, generate service on the basis of the traffic, optimize the traffic via setting replacement conditions and aggregation conditions, and then generate the target policies.



Tips: You can implement the complete configuration of Policy Assistant by using the WebUI. For more information, refer to the **Configuring the Policy Assistant** topic in *StoneOS WebUI User Guide*.

Enabling/Disabling the Policy Assistant

Before configuring policy assistant related function, please enable the function first. To enable the policy assistant, in the policy configuration mode, use the following command:

assistant enable



Notes: For the root VSYS, at most 4 policies are allowed to enable the policy assistant function, while for the non-root VSYS, only 1 policy can enable the function.

To disable the policy assistant, in the policy configuration mode, use the following command:

assistant disable

Example:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# assistant enable
```

Viewing the Policy of the Policy Assistant Enabled

To view the policy of the policy assistant enabled, in any mode, use the following command:

show policy assistant-enable

Enabling Traffic Statistics of Policy Assistant

The Traffic Statistics function of Policy Assistant can be used to collect statistics of the traffic extracted by Policy Assistant, including the number of hits, the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes. By default, the Traffic Statistics function is disabled. To enable this function, run the following command in policy configuration mode:

policy-assistant-traffic-statistic

In policy configuration mode, run the **no policy-assistant-traffic-statistic** command to disable the Traffic Statistics function of Policy Assistant.

Viewing the Status of Policy Assistant Traffic Statistics

To check whether the Traffic Statistics function of Policy Assistant is enabled, run the following command in any mode:

show policy assistant-traffic-statistic-status

Aggregate Policy

According to the needs of different scenarios, you can create an aggregate policy, and add some policy rules with the same effect or the same attributes to the aggregation policy. If the administrator adjusts the position of an aggregate policy, the positions of all its members will be adjusted accordingly, so as to manage policy rules in bulk.

The aggregate policy configurations includes:

- Creating an aggregate policy
- Adding an aggregate policy member

- Removing an aggregate policy member
- Deleting an aggregate policy
- Adjusting position
- Enabling/Disabling an aggregate policy
- Adding/Deleting an aggregate policy description

Creating an Aggregate Policy

To create an aggregation policy, you need to do the following two steps:

1. Create a policy rule with a name.
2. After entering the policy rule configuration mode, specify the created policy rule as an aggregate policy.



Notes: If you need to specify an existing policy rule as an aggregate policy, the configuration of the policy rule must meet the following requirements, otherwise it cannot be specified as an aggregate policy:

- Must contain a configuration with a name.
- It can contain an enabled state or a description configuration, and no configuration is included except the name, enabled state, or description configuration.

To create an aggregate policy, in the global configuration mode, use the following command:

rule [**id** *id*] { **name** *name*} **aggregate-type**

- **id** *id* - Specifies the ID of an aggregate policy. If not specified, system will automatically assign an ID to the policy. The ID should be unique in the system.

- **name** *name* - Specifies the name of an aggregate policy. The range is 1 to 95 characters and the name is required.
- **aggregate-type** - Specifies the created policy rule as an aggregate policy.

Adding an Aggregate Policy Member

After creating an aggregate policy, the administrator can add a policy rule to the aggregate policy to be an aggregate policy member. First, use the**rule id** *id*to enter the configuration mode of the policy rule to be added, and then, use the following command:

aggregate-rule { **name** *name* | *id*}

- **name** *name* | *id* - Specifies a name or an ID of the aggregate policy to be added to.



Notes:

- A policy rule can only be added to one aggregate policy.
- If a policy rule has already been added to an aggregate policy, the policy rule will be added to the newly specified aggregate policy after executing the command.
- An aggregate policy cannot be added to another aggregate policy as a member
- A policy member in the policy group cannot be added to an aggregate policy

Removing an Aggregate Policy Member

To remove a member from an aggregate policy, use the command **rule id** *id* to enter the configuration mode of the member to be removed, and then use the following command:

no aggregate-rule

Notes:

- If the member at the **top** position is removed from an aggregate policy, the removed member will be put before the aggregate policy
- If a member at a non-top position is removed from an aggregate policy, the removed member will be put after the aggregate policy

Deleting an Aggregate Policy

To delete an aggregate policy and remove its members, in the global configuration mode, use the following command:

no rule {**id** *id* | **name** *name*}

- **id** *id* – Deletes the aggregate policy with the specified ID.
- **name** *name* – Deletes the aggregate policy with the specified name.

To delete an aggregate policy and its members, that is, delete the aggregate policy together with all the members in it, in the global configuration mode or policy configuration mode, use the following command:

no rule {**id** *id* | **name** *name*} **include-member**

Adjusting Position

To adjust the position of an aggregate policy or an aggregate policy member, in the policy configuration mode, use the following command:

move {**name** *name* | *id*} {**top** | **bottom** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} }

- **name** *name* | *id* – Specifies an ID or a name of an aggregate policy or an aggregate policy member whose position you want to adjust.

- **top** – If an **aggregate policy**is moved, specifies the policy to be put at the top of all other policy rules; if an **aggregate policy member**is moved, specifies the member to be put at the top of all other members in the policy to which it belongs.
- **bottom** - If an **aggregate policy**is moved, specifies the policy to be put at the bottom of all other policy rules; if an **aggregate policy member**is moved, specifies the member to be put at the bottom of all other members in the policy to which it belongs.
- **before** {**name** *rule-name* | *id*} – Specifies an aggregate policy to be put before an ID or name. If an **aggregate policy member** is moved, the *rule-name*or *id*can only be specified as the ID or name of another member in the policy to which it belongs.
- **after** {**name** *rule-name* | *id*} – Specifies an aggregate policy to be put after an ID or name. If an **aggregate policy member** is moved, the *rule-name*or *id*can only be specified as the ID or name of another member in the aggregate policy to which it belongs.



Notes:

- After adjusting the position of an aggregate policy, the positions of all aggregate policy members will be adjusted accordingly.
- It is not supported to add a policy rule to or remove a policy rule from an aggregate policy by adjusting the position of the policy rule.

Enabling/Disabling an Aggregate Policy

By default, the configured aggregate policy will take effect immediately. By disabling an aggregate policy, the administrator can terminate its control over the traffic. To disable or enable an aggregate policy, in the configuration mode of the aggregate policy, use the following commands:

- Disable: **disable**
- Enable: **enable**

Notes:

- After disabling an aggregate policy, its members will be disabled too.
- After enabling an aggregate policy, the original status (enabled/disabled) of its members will remain unchanged. For example, if the original status of an aggregate policy member is "disabled", the status will remain unchanged after the policy to which it belongs is enabled

Adding/Deleting an Aggregate Policy Description

To add a description to an aggregate policy, in the configuration mode of the aggregate policy, use the following command:

description *description*

- *description* – Specifies an aggregate policy description. The range is 1 to 95 characters.

To delete the description of an aggregate policy, in the configuration mode of the policy, use the following command:

no description

Share Access

Share access means multiple endpoints access network with the same IP. The function of share access can block access from unknown device and allocate bandwidth for users, so as to prevent possible risks and ensure good online experience.

Share Access Rule

You can change the update configurations of share access rules as needed. The update configurations include:

- Creating share access rules
- Configuring share access rules
- Viewing share access rules

Creating Share Access Rules

To create the name of share access rule and enter the share access configuration mode, in the global configuration mode, use the following commands:

share-access-detect rule *rule-name* [**ipv6**]

- *rule-name* – Specifies the name of share access rule. If the rule of specified name already exists, enter the share access configuration mode directly.
- [**ipv6**] - Specifies the share access rule as the type of IPv6. If not specified , it will be the type of IPv4.

To delete the share access rule, in the global configuration mode, use the following command:

no share-access-detect rule *rule-name*

Configuring Share Access Rules

To configure a share access rule, in the share access configuration mode, use the following commands:

- Specify the source zone of share access: **src-zone** *zone-name*
- Delete the source zone of share access: **no src-zone**
- Specify the source IP address segment (IPv4/IPv6) of share access: **src-ip**{*ipv4/mask-len* |*ipv4 netmask*}/ **src-ip** {*ipv6 prefix/ prefix length*}
- Delete the source IP address segment (IPv4/IPv6) of share access: **no src-ip**{*ipv4/mask-len* |*ipv4 netmask*}/ **no src-ip** {*ipv6 prefix/ prefix length*}
- Specify the source IP address range (IPv4/IPv6)of share access: **src-range** *begin-ipv4 end-ipv4*/ **src-range** *begin-ipv6 end-ipv6*
- Delete the source IP address range (IPv4/IPv6) of share access: **no src-range** *begin-ipv4 end-ipv6*/ **no src-range** *begin-ipv6 end-ipv6*
- Specify the source IP address book (IPv4/IPv6) of share access: **src-addr** *ipv4-addr*/ **src-addr** *ipv6-addr*
- Delete the source IP address book (IPv4/IPv6) of share access: **no src-addr** *ipv4-addr*/ **no src-addr** *ipv6-addr*
- Enable/Disable the share access rule: **enable** | **disable**(enabled by default)
- Specify the schedule of share access: **schedule** *schedule-name*(The share access rule takes effect in the period specified by the schedule. If the schedule is not configured, the share access rule will always be effective.)
- Delete the schedule of share access: **no schedule**

- Specify the maximum number of share access endpoints: **access-limit** *limit-num* ((The range is 1-15. The default value is 2)
- Restore the default number of share access endpoints:**no access-limit**
- Specify the action: When the number of endpoints with the same IP address exceeds the maximum allowed to be shared by system, the IP address of the endpoints will be processed according to the specified action. The actions include: block and log, log only, warning and log. The default action is log only.

  action {**block** | **log-only** | **warning**}

  - **block** – When the number of shared access endpoints exceeds the maximum, system will block the IP address of the endpoints out of the limit and record logs during the specified period.
  - **log-only** – When the number of shared access endpoints exceeds the maximum, system will only record logs of the IP address out of limit, without affecting the normal connection of the access endpoints.
  - **warning** – When the number of shared access endpoints exceeds the maximum, system will send warnings to endpoints out of limit and record logs during the specified period.
- Restore to the default action (log only): **no action**
- Specify the control duration of block or warning: **control-duration** *duration* (The range is 60-3600s and the default value is 60s. After the duration, system will detect whether the number of access endpoints exceeds the maximum again.)
- Restore the default control duration of block or warning: **no control-duration**

- Specify the timeout time of endpoint: **detected-endpoint-timeout** *time*(After the timeout time, when the endpoint no longer accesses network with the IP, system will clear the end-point information. The range is 300-86400s. The default value is 600s)
- Restore the default timeout time of endpoint: **no detected-endpoint-timeout**
- Specify the sequence number of share access rules: **sequence** {**first** | **last** | *seq-id*}
  - **first** – Specifies the sequence number of share access rule as No.1.
  - **last** – Specifies the sequence number of share access rule as the last.
  - *seq-id* – Specifies the sequence number of share access rules. The range is 1-8. The smaller the number, the higher the priority.
- Specify the user-defined warning message: **warning-info** *string*
- Delete the user-defined warning message: **no warning-info**

Viewing Share Access Rules

To view share access rules, in any mode, use the flowing command:

show share-access-detect rule [*rule-name*]

- *rule-name* – Specifies the name of share access rule. If you do not specify the name of rule, system will display the configurations of all rules by default.

Share Access Signature Database

You can change the update configurations of share access signature database as needed. The update configurations include:

- Configuring the update mode of share access signature database
- Updating now

- Importing a share access signature file
- Viewing update information of share access signature database
- Viewing information of share access signature database



Tips: Non-root VSYS also supports the share access function, but does not support the update configurations of share access signature database.

Configuring the Update Mode of Share Access Signature Database

To update the share access signature database, in the global configuration mode, use the following command:

share-access-detect signature update [**mode** {**auto** | **manual**} | **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* | **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] | **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **protocol HTTP**]

- **mode** {**auto** | **manual**} – Specifies the update mode of share access. System supports automatic and manual update modes. The default mode is automatic update.
- **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* – Specifies the proxy server of share access database update.
- **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] – Specifies the automatic update schedule of share access database.
- **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 1.

- **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] − Specifies the domain, IP address and VRouter of update server 2.
- **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*] − Specifies the domain, IP address and VRouter of update server 3.
- **protocol HTTP** - Specifies the update protocol as HTTP, and the default protocol is HTTPS.

Updating Share Access Signature Database

To update the share access signature database immediately, in the execution mode, use the following command:

exec share-access-detect signature update

Importing a Share Access Signature File

In some cases, your device may be unable to connect to the update server to update the share access signature database. To solve this problem, StoneOS provides the file import function of share access signature database, i.e., importing the share access signature files to the device from an FTP or TFTP server, so that the device can update the share access signature database locally. To import the share access signature file, in the execution mode, use the following command:

import share-access-detect signature from {**ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] − Specifies the IP address, VRouter, user name and password of FTP server to import share access signature files. You can log in the server anonymously without typing user name and password.
- **tftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] − Specifies the IP address and

VRouter of TFTP server to import share access signature files.

- *file-name* – Specifies the name of the share access signature file to be imported.

Viewing Update Information of Share Access Signature Database

To view the update information of share access signature database, in any mode, use the following command:

show share-access-detect signature update

Viewing Information of Share Access Signature Database

To view the information of share access signature database, in any mode, use the following command:

show share-access-detect signature info

Viewing Statistics of Share Access

To view the statistics of share access, in any mode, use the following command:

show share-access-detect statistics [**rule** *rule-name*] [**src-ip** *ip-address*] [**src-zone** *zone-name*] [**status** {**blocking** | **normal** | **logging** | **warning**}] [**endpoint-num** {**gt** | **lt** | **eq**} *number*]

- **rule** *rule-name* – Displays the endpoints statistics of the specified share access rule.
- **src-ip** *ip-address* – Displays the endpoints statistics of the specified source IP.
- **src-zone** *zone-name* – Displays the endpoints statistics of the specified source zone.
- **status** {**blocking** | **normal** | **logging** | **warning**} – Displays the endpoints statistics in the specified status.
    - **blocking** - Displays the endpoints statistics when the status of endpoint IP address is blocking.

    - **normal** – Displays the endpoints statistics when the status of endpoint IP address is normal.
    - **logging** – Displays the endpoints statistics when the status of endpoint IP address is logging.
    - **warning** – Displays the endpoints statistics when the status of endpoint IP address is warning.
- **endpoint-num** {**gt** | **lt** | **eq**} *number* – Displays the statistics of endpoints which meets the specified number.
    - **gt** – Displays the statistics of endpoints whose number is more than the specified number.
    - **lt** – Displays the statistics of endpoints whose number is less than the specified number.
    - **eq** – Displays the statistics of endpoints whose number is equal to the specified number.
    - *number* – Displays the number of endpoints.

Share Access Log

You can change the update configurations of share access log as needed. The update configurations include:

- Configuring the status of share access log
- Configuring the output destination of share access log
- Viewing share access logs

Configuring the Status of Share Access Log

To enable the share access log, in the global configuration, use the following command. The function is enabled by default.

logging share-access-detect on

To disable the share access log, in the global configuration, use the following command:

no logging share-access-detect on

Configuring the Output Destination of Share Access Log

You can specify the output destination of share access log as needed, including syslog server, buffer and console. The default destination is buffer. In the global configuration mode, use the following command:

logging share-access-detect to { **syslog** | **buffer** [**size** *buffer-size*] | **console**}

- **syslog** – Sends the share access logs to the syslog server.
- **buffer** [**size** *buffer-size*] – Sends the share access log to the buffer and specifies the memory of buffer. The range is 4096-524288 bytes. The default value is 524288.
- **console** – Sends the share access log to the console.

To cancel the output destination configuration of share access log, in the global configuration mode, use the following command:

no logging share-access-detect to { **syslog** | **buffer** [**size** *buffer-size*] | **console**}

Viewing Share Access Logs

To view the share access log, in any mode, use the following command:

show logging share-access-detect

ARP Defense

IP-MAC Binding

Hillstone devices support IP-MAC binding, MAC-port binding and IP-MAC-port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings. Besides, the Hillstone devices are also designed with the ARP inspection function.

Static Binding

You can add static IP-MAC bindings and MAC-port bindings; you can also prevent the hosts that are enabled with dynamic ARP learning from accessing the Internet, and only allow the hosts with static IP-MAC bindings to access the Internet.

Adding a Static IP-MAC Binding

To add a static IP-MAC binding, in the global configuration mode, use the following command:

arp *ip-address mac-address* [**vrouter** *vrouter-name*]

- *ip-address* – Specifies the IP address for static binding.
- *mac-address* – Specifies the MAC address for static binding.
- **vrouter** *vrouter-name* – Adds the static IP-MAC binding to the specified VR. Parameter vrouter-name is used to specify the name of the VR. If the parameter is not specified, the static IP-MAC binding configured will belong to the default VR trust-vr.

To delete a static IP-MAC binding, in the global configuration mode, use the following command:

no arp {**all** | *ip-address*} [**vrouter** *vrouter-name*]

- **all** – Deletes all the static IP-MAC bindings in the system.
- *ip-address* – Deletes the static IP-MAC binding for the specified IP address in the system.

- **vrouter** *vrouter-name* – Deletes the static IP-MAC binding for the specified VR. Parameter *vrouter-name*is used to specify the name of the VR. If the parameter is not specified, the system will delete all the static IP-MAC bindings configured in the default VR or for the specified IP address.

Adding a Static IP-Port Binding

To add a static IP-port binding, in the global configuration mode, use the following command:

mac-address-static *mac-address* **interface** *interface-name*

- *mac-address* – Specifies the MAC address for static binding.
- **interface** *interface-name* – Specifies the interface for static binding.

To delete a static IP-port binding, in the global configuration mode, use the following commands:

- Delete all the static MAC-port bindings in the system:
  no mac-address-static all
- Delete all the static MAC-port bindings for the specified interface:
  no mac-address-static interface *interface-name*
- Delete the specified static MAC-port binding:
  no mac-address-static *mac-address* {**interface** *interface-name* | **vid** *vlan-id*}

Only Allowing Hosts with Static IP-MAC Binding Accessing the Internet

By default, the system allows hosts with dynamic ARP learning enabled to access the Internet. To only allow the hosts with IP-MAC binding enabled to access the Internet, in the interface configuration mode, use the following command:

arp-disable-dynamic-entry

To disable the function, in the interface configuration mode, use the following command:

no arp-disable-dynamic-entry

Dynamic IP-MAC-Port Binding

Devices can obtain dynamic IP-MAC-port binding information from:

- ARP learning
- MAC learning

ARP Learning

Devices can obtain IP-MAC bindings in an Intranet from ARP learning, and add them to the ARP list. By default this function is enabled. Hillstone devices will always keep ARP learning on, and add the learned IP-MAC bindings to the ARP list. If any IP or MAC address changes during the learning process, Hillstone devices will add the updated IP-MAC binding to the ARP list. If this function is disabled, only IP addresses in the ARP list can access Internet.

To configure the ARP learning function, in the VSwitch or BGroup interface configuration mode, use the following commands:

- Enable ARP learning: **arp-learning**
- Disable ARP learning: **no arp-learning**

ARP Learning Limit

After the ARP learning function is enabled, when a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached.

To enable the ARP learning limit function and specify the limit, in interface configuration mode, use the following command:

arp-learning-limit *number*

- *number* - Specifies the maximum number of IP-MAC bindings that can be learned on the interface. Valid values: 1 to capacity. The capacity varies based on device platforms.

In interface configuration mode, use the **no arp-learning-limit** command to disable the ARP learning limit function.

MAC Learning

Devices can obtain MAC-port bindings in an Intranet from MAC learning, and add them to the MAC list. By default this function is enabled. Devices will always keep MAC learning on, and add the learned MAC-port bindings to the MAC list. If any MAC address or port changes during the learning process, devices will add the updated MAC-port binding to the MAC list.

To configure the MAC learning function, in the VSwitch or BGroup interface configuration mode, use the following commands:

- Enable MAC learning: **mac-learning**
- Disable MAC learning: **no mac-learning**

Viewing IP-MAC-Port Binding Information

To view the IP-MAC binding information (static and dynamic) and the MAC-port binding information (static and dynamic) in the system, use the following commands:

- IP-MAC binding information:**show arp** [**vrouter** *vrouter-name*]
- • MAC-port binding information: **show mac**

Clearing ARP Binding Information

To clear the ARP binding information (dynamic), use the following command:

clear arp [**interface** *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*]

- **interface** *interface-name* – Clears the ARP binding information of the specified interface. Parameter interface-name is used to specify the interface name.

- *A.B.C.D* - Clears the ARP binding information of the specified IP address of the interface.
- **vrouter** *vrouter-name* – Clears the ARP binding information of the specified VRouter. Parameter *vrouter-name*is used to specify the VRouter name. If this parameter is not specified, the system will clear the ARP binding information of the default VRouter trust-vr.

Forcing Dynamic MAC-Port Binding

You can force to bind the dynamic MAC-Port binding information learned from the MAC learning function. To force to bind dynamic MAC-port binding, in any mode, use the following command:

exec mac-address dynamic-to-static

DHCP Snooping

DHCP (Dynamic Host Configuration Protocol) is designed to allocate appropriate IP addresses and related network parameters for sub networks automatically. DHCP snooping can create binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and server. When ARP inspection is also enabled, StoneOS will check if an ARP packet passing through can be matched to any binding of the list. If not, the ARP packet will be dropped. In the network that allocates addresses via DHCP, you can prevent against ARP spoofing attacks by enabling ARP inspection and DHCP Snooping.

DHCP clients look for the server by broadcasting, and only accept the network configuration parameters provided by the first reachable server. Therefore, an unauthorized DHCP server in the network might lead to DHCP server spoofing attacks. Hillstone devices can prevent against DHCP server spoofing attacks by dropping DHCP response packets on related ports.

Besides, some malicious attackers send DHCP requests to a DHCP server in succession by forging different MAC addresses, and eventually result in IP address unavailability to legal users by exhausting all the IP address resources. This kind of attacks is commonly known as DHCP starvation. Hillstone devices can prevent against such attacks by dropping request packets on related ports, setting rate limit or enabling validity check.

Enabling/Disabling DHCP Snooping

The BGroup interface, VSwitch interface and VLAN interface of StoneOS all support DHCP snooping. By default, this function is disabled. To enable DHCP snooping for the BGroup interface or VSwitch interface, in the VSwitch interface or BGroup interface configuration mode, use the following command:

dhcp-snooping

To disable the function, in the VSwitch interface or BGroup interface configuration mode, use the following command:

no dhcp-snooping

To enable DHCP snooping for the VLAN interface, in the global configuration mode, use the following command:

dhcp-snooping vlan *vlan-list*

- *vlan-list* – Specifies the VLAN ID that will be enabled with DHCP snooping. The value range is 1 to 4094, such as 1, 2-4, or 1, 2, 5. StoneOS reserves 32 VLAN IDs (from VLAN224 to VLAN255) for BGroup.

To disable the function, in the global configuration mode, use the following command:

no dhcp-snooping vlan *vlan-list*

Configuring DHCP Snooping

You can configure the DHCP snooping function on the device, including the processing methods of DHCP request and response packets, and the validity check. By default, all the DHCP request and response packets are permitted, and the validity check is disabled. To enable the DHCP snooping function, in the Ethernet interface (physical interface of the BGroup, VSwitch or VLAN interface) configuration mode, use the following command:

dhcp-snooping {**deny-request** | **deny-response** | **validity-check**}

- **deny-request** – Drops all the request packets sent by the client to the server.
- **deny-response** – Drops all the response packets returned by the server to the client.
- **validity-check** – Checks if the client's MAC address of the DHCP packet is the same with the source MAC address of the Ethernet packet. If not, the packet will be dropped.

To disable the function, in the Ethernet interface configuration mode, use the following command:

no dhcp-snooping {**deny-request** | **deny-response** | **validity-check**}

Configuring DHCP Packet Rate Limit

To configure the DHCP packet rate limit, in the Ethernet interface (physical interface of the BGroup, VSwitch or VLAN interface) configuration mode, use the following command:

dhcp-snooping rate-limit *number*

- *number* – Specifies the number of DHCP packets received per second on the interface. If the number exceeds the specified value, StoneOS will drop the excessive DHCP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the DHCP packet rate limit, in the Ethernet interface configuration mode, use the following command:

no dhcp-snooping rate-limit

Viewing DHCP Snooping Configuration Information

To view the DHCP snooping configuration information, in any mode, use the following command:

show dhcp-snooping configuration

DHCP Snooping List

With DHCP Snooping enabled, StoneOS will inspect all the DHCP packets passing through the interface, and create and maintain a DHCP Snooping list that contains IP-MAC binding information during the process of inspection. Besides, if the VSwitch, VLAN interface or any other Layer 3 physical interface is configured as a DHCP server, StoneOS will create IP-MAC binding information automatically and add it to the DHCP Snooping list even if DHCP Snooping is not enabled. The bindings in the list contain information like legal users' MAC addresses, IPs, interfaces, ports, lease time, etc. To view the DHCP snooping list, in any mode, use the following command:

show dhcp-snooping binding

To clear all or the specified DHCP snooping list entry, in any mode, use the following command:

clear dhcp-snooping binding [**interface** *interface-name* [*A.B.C.D*] | **vlan** *vlan-id* [*A.B.C.D*]]

- **clear dhcp-snooping binding** – Deletes all bindings in the DHCP snooping list.
- **interface** *interface-name* – Specifies the interface name to delete the bindings of the interface.
- **interface** *interface-name* [*A.B.C.D*] – Specifies the IP address under an interface to delete the bindings of the IP address.
- **vlan** *vlan-id* – Specifies the VLAN ID to delete the bindings of the VLAN.
- **vlan** *vlan-id* [*A.B.C.D*] – Specifies the IP address under a VLAN to remove the bindings of the IP address.

ARP Inspection

Devices support ARP Inspection for interfaces. With this function enabled, System will inspect all the ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list:

- If the IP address is in the ARP list and the MAC address is matched, the ARP packet will be forwarded;
- If the IP address is in the ARP list but the MAC address is not matched, the ARP packet will be dropped;
- If the IP address is not in the ARP list, continue to check if the IP address is in the DHCP snooping list;
- If the IP address is in the DHCP Snooping list and the MAC address is also matched, the ARP packet will be forwarded;
- If the IP address is in the DHCP snooping list but the MAC address is not matched, the ARP packet will be dropped;
- If the IP address is not in the DHCP snooping, the ARP packet will be dropped or forwarded according to the specific configuration.

Enabling/Disabling ARP Inspection

The BGroup, VSwitch and VLAN interface of StoneOS all support ARP inspection. By default, the function is disabled. To enable the function for BGroup or VSwitch interface, in the VSwitch or BGroup interface configuration mode, use the following command:

arp-inspection {**drop** | **forward**}

- **drop** – Drops the ARP packets whose IP address is not in the ARP table.
- **forward** – Forwards the ARP packets whose IP address is not in the ARP table.

To disable the function, in the VSwitch or BGroup interface configuration mode, use the following command:

no arp-inspection

To enable ARP Inspection for the VLAN interface, in the global configuration mode, use the following command:

arp-inspection vlan *vlan-list* {**drop** | **forward**}

- *vlan-list* – Specifies the VLAN ID that will be enabled with ARP Inspection. The value range is 1 to 4094, such as 1, 2-4, or 1, 2, 5. StoneOS reserves 32 VLAN IDs (from VLAN224 to VLAN255) for BGroup.

To disable the function, in the global configuration mode, use the following command:

no arp-inspection vlan *vlan-list*

Configuring a Trusted Interface

You can configure a device interface (physical interface of the BGroup, VSwitch or VLAN interface) as the trusted interface. The packets passing through the trusted interface will not be checked by ARP inspection. By default, none of the device interfaces is the trusted interface. To configure a device interface as the trust interface, in the interface configuration mode, use the following command:

arp-inspection trust

To cancel the trust interface, in the interface configuration mode, use the following command:

no arp-inspection trust

Configuring an ARP Rate

To configure the ARP rate, in the interface configuration mode, use the following command:

arp-inspection rate-limit *number*

- *number* – Specifies the number of ARP packets received per second on the interface. If the number exceeds the specified value, system will drop the excessive ARP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the ARP rate, in the interface configuration mode, use the following command:

no arp-inspection rate-limit



Notes: You can only configure ARP rate on physical interfaces that are bound to Layer 2 zones.

ARP Defense

Powered by the ARP learning, MAC learning and ARP inspection functions, system is capable of providing defense against ARP spoofing attacks. Besides, system can also gather statistics on the ARP spoofing attacks. To view the ARP spoofing attacks statistics, in any mode, use the following command:

show arp-spoofing-statistics [*number*]

- *number* – Shows the statistics of the top *number* records.

To clear the ARP spoofing attacks statistics, in the execution mode, use the following command:

clear arp-spoofing-statistics

Host Defense

With this function enabled, StoneOS can send gratuitous ARP packets for different hosts to protect them against ARP attacks. To configure the host defense function, in the global configuration mode, use the following command:

gratuitous-arp-send ip *ip-address* **mac** *mac-address* **switch-interface** *interface-name* **except-interface** *interface-name* **rate** *rate-value*

- **ip** *ip-address* – Specifies the IP address of the host that uses the device as a proxy.
- **mac** *mac-address* – Specifies the MAC address of the host that uses the device as a proxy.
- **switch-interface** *interface-name* – Specifies the interface that sends gratuitous ARP packets. It can be either a VSwitch or BGroup interface.

- **except-interface***interface-name* – Specifies the excluded port, i.e., the port that does not send gratuitous ARP packets. Typically it is the port connected to the host that uses the device as a proxy.
- **rate***rate-value* - Specifies a gratuitous ARP packet send rate. The value range is 1 to 10 packets/sec. The default value is 1.

Repeat the command to configure the gratuitous ARP packets for more hosts. You can configure the Hillstone device to send gratuitous ARP packets for up to 16 hosts.

To disable the function, in the global configuration mode, use the following command:

no gratuitous-arp-send ip*ip-address***switch-interface***interface-name*

Chapter 3 Routing

Routing is the process of forwarding packets from one network to a destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

Hillstone devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. The routings supported by the Hillstone devices include Destination Routing, ISP Routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), Proximity Routing, Dynamic Routing (including RIP, OSPF and BGP), Equal Cost MultiPath Routing (ECMP) and Static Multicast-routing.

This section contains the following contents:

- "Destination Route" on Page 442: A manually-configured route which determines the next routing hop according to the destination IP address.
- "Destination Interface Route" on Page 444: A manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.
- "ISP Route" on Page 446: A kind of route which determines the next hop based on different ISPs.
- "Source Route" on Page 463: Source IP based route which selects routers and forwards data according to the source IP address.
- "Src-If Route " on Page 464: Source IP and ingress interface based route.
- "Policy-based Route" on Page 466: A route which forwards data based on the source IP, destination IP address and service type.
- Proximity routing: Selects routers and forwards data according to the result of proximity detection.

- "Dynamic Routing" on Page 478: Selects routers and forwards data according to the dynamic routing table generated by dynamic routing protocols (RIP, OSPF, IS-IS, or BGP).
- "ECMP" on Page 555: Load balancing traffic destined to the same IP address or segment in multiple routes with equal administration distance.
- "Static Multicast Routing" on Page 556: a manually-configured route which broadcasts packets from a multicasting source to all the members within a group.

When forwarding the inbound packets, the Hillstone device selects a route in the following sequence: PBR > SIBR > SBR > DIBR > Destination Routing/ISP Routing/Proximity Routing/Dynamic Routing.

Enabling/Disabling Static Routing Query

For PBR, SBR , SIBR and DIBR, you can control the query on them separately (the system requires that the destination routing query must be enabled). By default, the BR, SBR , SIBR and DIBR query are enabled. To enable/disable the query on them, in the global configuration mode, use the following commands (applicable to all VRouters):

- Enable: **route enable** {**pbr** | **sibr** | **sbr** |**dibr**}
- Disable: **route disable** {**pbr** | **sibr** | **sbr** | **dibr**}



Tip: For the configuration example of enabling/disabling static routing query, see "Example of Configuring Static Route Query".

Enabling/Disabling the Route Rematch by Session

By default, the function of route rematch by session is enabled. When you add, modify or delete the route, the session will match the optimal route again. During this process, the system will dispose sessions as follows:

- when the route that the session matched before is deleted:
    - if the keep-session function is disabled, the related session will be deleted.
    - if the keep-session function is enabled, the related session will not be deleted, and the routing information of the session will turn to invalid. When the route that the session matched before is added again, the session will match the optimal route again:
        - if the egress interface of the rematched route remains the same, the routing information of the session will turn to valid, and the session will be restored to normal status.
        - if the egress interface of the rematched route changes, the related session will be deleted.
- when the route that the session matched before is modified or a new route is added:
    - if the route that the session matched before is still the optimal route, the related session remains normal.
    - if the route that the session matched before is not the optimal route, yet the egress interface of the rematched route remains the same, the routing information of the related session will be updated.
    - if the route that the session matched before is not the optimal route and the egress interface of the rematched route changes, the related session will be deleted.

In some cases (such as adding or deleting the application bound with PBR rule), a large number of sessions may be deleted, which will lead to traffic anomaly. Meanwhile, you should disable the function of route rematch by session.

To enable or disable this function, in the Flow configuration mode, use the following command:

session rematch route {**enable** [**keep-session**] | **disable**}

- **enable** - Enable the route rematch by session.
- **keep-session** - Keep the related session. When the route rematch by session function is enabled and this parameter is specified, the related session will be not deleted and the routing information of the session will turn to invalid. By default, this parameter is not specified, namely, the keep-session function is disabled.
- **disable** - Disable the route rematch by session. If the keep-session function is enabled, it will be disabled at the same time.

VRouter

VR virtually acts as a router, and different VRouters have their own independent routing tables. A VRouter named trust-vr is bundled with the system. Hillstone devices support multiple VRouters (a function known as multi-VR). All the routing configuration of the Hillstone devices must be performed in an appropriate VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of VRouter.

In the VRouter Configuration mode, you can configure static routing entries, dynamic routing protocols, or specify the maximum number of routing entries supported by the VRouter, as well as import routing entries from other VRouters.

To use the multi-VR function, you need to run **exec vrouter enable** first, and then reboot the system to make multi-VR take effect.



Tip: For the multi-VR configuration examples, see "Example of Configuring Multi-VR".

Specifying the Maximum Number of Routing Entries

To specify the maximum number of routing entries permitted by a VRouter (including all direct routes, static routes and dynamic routes of the VRouter), in the VRouter configuration mode, use the following command:

max-routes *number*

- *number* - Specifies the maximum number of routing entries. The value range is 1 to 100000.

To cancel the specified maximum number of routing entries, in the VRouter configuration mode, use the following command:

no max-routes

When reaching the maximum number of routing entries, the system will issue an alarm.

Importing VRouter Routing Entries

You can import routing entries from other VRouters to your own VRouter. In the VRouter configuration mode, use the following command:

import vrouter *vrouter-name* {**connected** | **static** | **rip** | **ospf** | **bgp**}

- *vrouter-name*- Specifies the name of the VRouter the imported routing entry belongs to.
- **connected** | **static** | **rip** | **ospf** | **bgp** - Specifies the type of the routing entry that will be imported.

Repeat the above command to import routing entries of different types.



Notes: The priority of routing entries imported from other VRouters is lower than the priority of the entries bundled with the original VRouter.

Disable the Highest Priority of Direct Route

Direct route has the highest route priority, when you configure other roures in the same time, the direct route will be used first, makes the other route is not effective. Therefore, you can accord-

ing to need, disable the highest priority of direct route. In the VRouter configuration mode, use the following command:

fib-lookup connect-first-disable

To restore the he highest priority of direct route, in the VRouter configuration mode, use the following command:

no fib-lookup connect-first-disable

Destination Route

The destination route is a manually-configured routing entry that determines the next routing hop based on the destination IP address. Usually a network with a comparatively small number of outbound connections or stable Intranet connections will use a destination route. You can add a default routing entry at your own choice as needed.

Configuring a Destination Route

You can add a destination route and view the route's information through CLI.

Adding a Destination Route

You can add a destination routing entry to VRouter. However, before adding the entry, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To add a destination route, in the VRouter configuration mode, use the following command:

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**tag** *tag-value*] [**description** *description*] [**schedule** *schedule-name*] [**track***track-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The Hillstone devices support two formats: A.B.C.D/M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0

255.255.255.0.

- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface (for multi-tunnel interface, you must specify the next hop IP address of IPsec VPN, GRE or SSL VPN tunnel by the *A.B.C.D* parameter, and this address must be the same as the next hop IP address of the corresponding tunnel bound to the tunnel interface), Null0 interface or PPPoE interface. For more information about how to configure the next hop IP address of the VPN/GRE tunnel that is bound to the tunnel interface, see "Binding a Tunnel" in "Fire-wall".

- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.

- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

- **tag** *tag-value* – Specifies the tag value of the destination route. When OSPF redistributes routes, if the configured routing tag values here are matched to the rules in the routing map-ping table, the route will be redistributed to filter its information. The value range is 1 to 4294967295.

- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.

- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The con-figuration will only take effect during the specified period. Repeat the command to specify

more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add more destination routes.

To delete the specified static destination route, use the following command:

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

Viewing destination routing information

To view the destination routing information, in any mode, use the following command:

show ip route static [**vrouter** *vrouter-name*]

- *vrouter-name* - Specifies the destination route information of the specified VRouter.

Destination Interface Route

Destination-Interface-Based Routing(DIBR) is a manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.

Adding a Destination Interface Route

You can add a destination interface routing entry to VRouter. However, before adding the entry, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To add a destination interface route, in the VRouter configuration mode, use the following command:

ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*] [**track***track-name*

- **in-interface** *interface-name* - Specifies the ingress interface of the route.
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (*vrouter vrouter-name*). If the next hop type is interface, you can select a tunnel interface (for multi-tunnel interface, you must specify the next hop IP address of IPsec VPN, GRE or SSL VPN tunnel by the *A.B.C.D* parameter, and this address must be the same as the next hop IP address of the corresponding tunnel bound to the tunnel interface), Null0 interface or PPPoE interface. For more information about how to configure the next hop IP address of the VPN/GRE tunnel that is bound to the tunnel interface, see "Binding a Tunnel" in "Fire-wall".
- .*distance-value*- Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.
- **schedule** *schedule-name* - Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify

more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add more destination interface routes.

To delete the specified destination interface route, use the following command:

no ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

Viewing Destination Interface Route Information

To view the destination interface route information, in any mode, use the following command:

show ip route in-interface *interface-name*

- **in-interface** *interface-name* - Specifies the ingress interface of the route.

Viewing FIB Information about Destination Interface Route

To view the FIB information about destination interface route, in any mode, use the following command:

show [ipv6] fib in-interface *interface-name*

- **in-interface** *interface-name* - Specifies the ingress interface of the route.

ISP Route

Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not function based on the traffic's direction. If a server in ISP A is accessed through ISP B, the speed will be rather low. For such a scenario, StoneOS provides ISP Route which allows traffics from different ISPs to take their proprietary routes, thus accelerating network access.

To configure an IPv4/IPv6 ISP route, first you need to add a subnet to an IPv4/IPv6 ISP, and then configure the IPv4/IPv6 ISP route. The destination of the route is determined by the name of the IPv4/IPv6 ISP. You can customize ISP information, or upload and download custom profiles that contain different ISP information. You can implement remote or local update on predefined ISP profiles by using the ISP information database.

In an IPv4/IPv6 ISP route configuration, you can perform the following operations:

- Configuring ISP information database
- Configuring IPv4/IPv6 ISP information
- Configuring an IPv4/IPv6 ISP route
- Uploading/Saving an IPv4/IPv6 ISP route configuration file
- Viewing IPv4/IPv6 ISP route configuration information

Configuring the ISP Information Database

By default, the system automatically updates the ISP information database on a daily basis. You can modify the update configuration as needed.

The update configuration of the ISP information database includes:

- Configuring the update mode of the ISP information database
- Configuring the transmission protocol for update
- Configuring the update server
- Specifying the HTTP proxy server
- Specifying the update time
- Updating immediately
- Importing predefined ISP profiles

- Displaying information about the ISP information database
- Displaying the update configuration of the ISP information database

Configuring the Update Mode of the ISP Information Database

The ISP information database can be manually or automatically updated. To configure the update mode of the ISP information database, in global configuration mode, use the following command:

isp-information update mode {**auto** | **manual**}

- **auto** – Specifies to automatically update the ISP information database. This is the default update mode.
- **manual** – Specifies to manually update the ISP information database.

In global configuration mode, use the following command to return to the default update mode:

no isp-information update mode

Configuring the Transmission Protocol for Update

The ISP information database can be updated over HTTP or HTTPS. By default, HTTPS is used. To set the transmission protocol of updating the ISP information database to HTTP, in global configuration mode, use the following command:

isp-information update protocol HTTP

In global configuration mode, use the following command to return to the default transmission protocol:

no isp-information update protocol HTTP

Configuring the Update Server

The system provides the default update server of the ISP information database update1.hill-stonenet.com and update2.hillstonenet.com. You can also configure other update servers to download the latest predefined ISP profile as needed. At most 3 update servers can be configured. To configure an update server, in global configuration mode, use the following command:

isp-information update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*]

- **server1** | **server2** | **server3** – Specifies the server to be configured. The server supports both IPv4 and IPv6. The default value of **server1** is update1.hillstonenet.com and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server, which can be an IP address or domain name, such as update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router bound to the update server. By default, **trust-vr** is used.

To restore the default configuration of server1 or server2 or delete the configuration of server3, in global configuration mode, use the following command:

no isp-information update {**server1** | **server2** | **server3**}

Specifying the HTTP Proxy Server

If an HTTP proxy server is required for the device to access the Internet, you need to specify the IP address and port number of the proxy server on the device to ensure normal update.

To specify an HTTP proxy server for the ISP information database, in global configuration mode, use the following command:

isp-information update proxy-server {**main** | **backup**} *ip-addressport-number*

- **main** | **backup** – Uses the main field to specify the main proxy server and uses the backup field to specify the backup proxy server.
- *ip-addressport-number* – Specifies the IP address and port number of the proxy server.

To cancel the specified proxy server, use the **no isp-information update proxy-server** {**main** | **backup**} command.

Specifying the Update Time

By default, the system automatically updates the ISP information database on a daily basis. The daily update time is random to avoid high server traffic volume. To specify the update frequency and time of the ISP information database, in global configuration mode, use the following command:

isp-information update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly***<1-31>*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Updates the database every week. The **mon | tue | wed | thu | fri | sat | sun** field is used to specify the date when the database is updated every week.
- **monthly***<1-31>* – Updates the database every month. The *<1-31>* field is used to specify the date when the database is updated every month.
- *HH:MM* – Specifies the time when the database is updated, such as 09：00.

Updating Immediately

No matter whether the update mode is manual or automatic, you can use the following command to update the ISP information database at any time. To immediately update the ISP information database, in any mode, use the following command:

exec isp-information update

- **exec isp-information update** – Updates only different parts between the current ISP information database and the latest ISP information database released by the update server.

Importing Predefined ISP Profiles

In some cases, your device may fail to connect to the update server to update the ISP information database. To avoid this issue, StoneOS provides the ISP profile import function. You can import

predefined ISP profiles over FTP, FTPS, SFTP, or TFTP to update the ISP information database. To import a predefined ISP profile, in execution mode, use the following command:

import ispfile from {**ftp server***ip-address* [**user***user-name***password***password*] | **ftps server***ip-address* [**user***user-name***password***password*] | **sftp server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address* } [**vrouter***vr-name*] *file-name*

- *ip-address* - Specifies the IP address of the FTP/FTPS/SFTP/TFTP server.
- **user***username***password***password* - Specifies the username and password of the FTP/FTPS/SFTP server.
- **vrouter***vr-name* – Specifies the VRouter to which the FTP/FTPS/SFTP/TFTP server belongs.
- *file-name* - Specifies the name of the predefined ISP profile to be imported.

Deleting Predefined ISP Profiles

The predefined ISP profiles are encrypted. The device provides the built-in ISP information database, which contains predefined ISP profiles. The device can connect to the update server or import predefined ISP profiles over FTP, FTPS, SFTP, or TFTP to update the ISP information database. You can delete predefined ISP profiles from the ISP information database by using the CLI.

Deleting Predefined IPv4 ISP Profiles

To delete predefined IPv4 ISP profiles from the system, in execution mode, use the following command:

exec isp-network clear-predefine

After you run the command, restart the system and the system will restore the original predefined IPv4 ISP profiles (built-in predefined IPv4 ISP profiles).



Notes: To ensure that predefined IPv4 ISP profiles can be deleted as expected, delete nested IPv4 ISP information entries before you delete the predefined IPv4 ISP profiles.

Deleting Predefined IPv6 ISP Profiles

To delete predefined IPv6 ISP profiles from the system, in execution mode, use the following command:

exec isp-network clear-predefine ipv6

After you run the command, restart the system and the system will restore the original predefined IPv6 ISP profiles (built-in predefined IPv6 ISP profiles).



Notes: To ensure that predefined IPv6 ISP profiles can be deleted as expected, delete nested IPv6 ISP information entries before you delete the predefined IPv6 ISP profiles.

Displaying Information about the ISP Information Database

To view information about the ISP information database of the device at any time, in any mode, use the following command:

show isp-information info

Example:

```
hostname(config)# show isp-information info
DB vendor: Hillstone Networks (displays the database vendor)
Current version: 1.0.220902 (displays the current version of the ISP information database)
Release date: 2022/09/02 15:00:02 (displays the release date and time of the current version)
```

Displaying the Update Configuration of the ISP Information Database

You can view the update information about the ISP information database of the device by using corresponding show commands at any time. The update information includes but are not limited to the update server information, update mode, update frequency, time, and botnet prevention signature database update status. To view the update configuration of the ISP information database, in any mode, use the following command:

show isp-information update

Example:

```
hostname(config)# show isp-information update
ISP signature update options: (displays the update options of the ISP
information database)
protocol: HTTPS (displays the transmission protocol for ISP
information database update)
server1: update1.hillstonenet.com, 443, trust-vr (displays the information
about the update server of the ISP information database)
server2: update2.hillstonenet.com, 443, trust-vr (displays the information
about the update server of the ISP information database)
server3: 10.10.10.10, 443, trust-vr (displays the information about the
update server of the ISP information database)
proxy server status: enable (displays the proxy server status)
main proxy server: (displays the information about the main proxy
server)
backup proxy server: ip 10.10.10.10, port 12 (displays the information about
the backup proxy server)
mode: auto (displays the update mode of the ISP information data-
base)
schedule: daily 09:21 (displays the update cycle in auto mode)
current status: normal (displays the process status of the ISP inform-
ation database, in which normal indicates that the ISP
```

```
information database is in the not updated status)
last update result: Download signature failed; please confirm the servers are reachable (displays the result of the last ISP information database update)
last update time: Fri Nov 4 09:22:02 2022 (displays the time when the ISP information database was last updated)
```

Configuring IPv4 ISP Information

To configure IPv4 ISP information on the device, first, you need to enter the IPv4 ISP information configuration mode. To create an IPv4 ISP name and enter the IPv4 ISP information configuration mode, in the global configuration mode, use the following command:

isp-network *isp-name*

- *isp-name* - Specifies the name of IPv4 ISP. System allows up to 26 IPv4 ISP information to be created.

To delete the specified IPv4 ISP, in the global configuration mode, use the following command:

no isp-network *isp-name*

Adding a Subnet Entry

To add a subnet entry to IPv4 ISP, in the IPv4 ISP information configuration mode, use the following command:

subnet *A.B.C.D/M*

- *A.B.C.D/M* - Specifies the subnet for the IPv4 ISP, in the form of IP address/netmask, for example, 1.1.1.0/24. The maximum number of subnet entries that the system allows to add varies depending on the platform, and the range is 1000-6000.

In the IPv4 ISP information configuration mode, repeat the above command to add multiple subnets for the IPv4 ISP.

To delete the specified subnet, in the IPv4 ISP information configuration mode, use the following command:

no subnet *A.B.C.D/M*

Adding an IPv4 ISP Information Entry

To add an IPv4 ISP information entry, that is to add other configured IPv4 ISP information (pre-defined IPv4 ISP information or user-defined IPv4 ISP information), in the IPv4 ISP information configuration mode, use the following command:

member *isp-name*

- *isp-name* – Specifies the IPv4 ISP name. An IPv4 ISP can include up to 1 nested layers, but an IPv4 ISP cannot add itself as a member.

In the IPv4 ISP information configuration mode, repeat the above command to add multiple IPv4 ISP information entrys for the IPv4 ISP.

To delete the specified IPv4 ISP information entry, in the IPv4 ISP information configuration mode, use the following command:

no member *isp-name*



Notes: IPv4 ISP information and IPv6 ISP information are not allowed to be nested in each other.

Configuring an IPv4 ISP Route

To configure an IPv4 ISP route, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of VRouter.

To configure an ISP route, in the VRouter configuration mode, use the following command:

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* - Specifies an existing ISP in the system as the destination address of the route.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface, Null0 interface or PPPoE interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.
- **schedule** *schedule-name* - Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add multiple ISP routes.

To delete the specified ISP route, in the VRouter configuration mode, use the following command:

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

Viewing IPv4 ISP Route Configuration Information

To view the IPv4 ISP route configuration information, use the following commands:

- View the predefined IPv4 ISP information:

  show pre-isp-network {**all** | *isp-name*}

- View the user-defined IPv4 ISP information:

  show isp-network {**all** | *isp-name*}

- View the IPv4 ISP route:

  show ip route isp [*isp-name* | **vrouter** *vrouter-name*]

Uploading/Downloading a User-defined IPv4 ISP Profile

Hillstone devices support two types of IPv4 ISP profiles: user-defined IPv4 ISP profiles and pre-defined IPv4 ISP profiles.

- User-defined IPv4 ISP profiles: Follow the format example shown below to compile a user-defined profile. Otherwise, even if the file is uploaded successfully, it will not take effect in the system.

```
# Software Version 5.5 SG6000-MX_MAIN-68-V6-
r1018.bin 202211040258
!
Version 5.5R10
subVersion 1.0
isp-network test
subnet 1.1.1.1/32
subnet 2.2.2.2/32
member CERNET
exit
```

- Predefined IPv4 ISP profiles: The predefined IPv4 ISP profile shipped with StoneOS is encrypted. If the predefined profile has been updated, you need to upload the new profile.

Uploading a User-defined IPv4 ISP Profile

To upload a user-defined IPv4 ISP profile through FTP and TFTP server, in the execution mode, use the following command:

import ispfile from {**ftp server** *ip-address* [**user** *username* **password** *string*] | **tftp server** *ip-address*} *file-name*

- **ftp server** *ip-address* - Specifies the IP address of FTP server.
- **user** *username* **password** *string* - Specifies the user name and password accessing FTP server.
- **tftp server** *ip-address* - Specifies the IP address of TFTP server.
- *file-name* - Specifies the name of the user-defined IPv4 ISP profile.

Downloading a User-defined IPv4 ISP Profile

The custom ISP profiles can only be saved through WebUI. To save an IPv4 ISP profile to your PC, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select **IPv4** tab.
3. Click **Download** to open the **Download User Defined ISP File** panel.
4. Select an ISP profile from the **ISP profile** drop-down list.
5. Click **OK** to save the profile to a specified location in PC.

Configuring IPv6 ISP Information

To configure IPv6 ISP information on the device, first, you need to enter the IPv6 ISP information configuration mode. To create an IPv6 ISP name and enter the IPv6 ISP information configuration mode, in the global configuration mode, use the following command:

isp-network *isp-name* **ipv6**

- *isp-name* - Specifies the name of IPv6 ISP. System allows up to 26 IPv6 ISP information to be created.
- **ipv6** - Specifies the ISP information type as IPv6.

To delete the specified IPv6 ISP, in the global configuration mode, use the following command:

no isp-network *isp-name*

Adding an IPv6 Subnet Entry

To add a subnet entry to IPv6 ISP, in the IPv4 ISP information configuration mode, use the following command:

subnet *ipv6-address/prefix*

- *ipv6-address/prefix* - Specifies the subnet for the IPv6 ISP, in the form of IPv6 address/-prefix, for example, 1::1/64. The maximum number of subnet entries that the system allows to add varies depending on the platform, and the range is 1000-6000.

In the IPv6 ISP information configuration mode, repeat the above command to add multiple subnets for the IPv6 ISP.

To delete the specified subnet, in the IPv6 ISP information configuration mode, use the following command:

no subnet *A.B.C.D/M*

Adding an IPv6 ISP Information Entry

To add an IPv6 ISP information entry, that is to add other configured IPv6 ISP information (predefined IPv6 ISP information or user-defined IPv6 ISP information), in the IPv6 ISP information configuration mode, use the following command:

member *isp-name*

- *isp-name* – Specifies the IPv6 ISP name. An IPv6 ISP can include up to 1 nested layers, but an IPv6 ISP cannot add itself as a member.

In the IPv6 ISP information configuration mode, repeat the above command to add multiple IPv6 ISP information entrys for the IPv6 ISP.

To delete the specified IPv6 ISP information entry, in the IPv6 ISP information configuration mode, use the following command:

no member *isp-name*



Notes: IPv6 ISP information and IPv4 ISP information are not allowed to be nested in each other.

Configuring an IPv6 ISP Route

To configure an IPv6 ISP route, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of VRouter.

To configure an ISP route, in the VRouter configuration mode, use the following command:

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* - Specifies an existing ISP in the system as the destination address of the route.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface, Null0 interface or PPPoE interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.

- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.
- **schedule** *schedule-name* - Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add multiple ISP routes.

To delete the specified ISP route, in the VRouter configuration mode, use the following command:

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

Viewing IPv6 ISP Information

To view the IPv6 ISP route configuration information, use the following commands:

- View the predefined IPv6 ISP information:
  show ipv6 pre-isp-network {**all** | *isp-name*}
- View the user-defined IPv6 ISP information:
  show ipv6 isp-network {**all** | *isp-name*}

Uploading/Downloading a User-defined IPv6 ISP Profile

Hillstone devices support two types of IPv6 ISP profiles: user-defined IPv6 ISP profiles and predefined IPv6 ISP profiles.

- User-defined IPv6 ISP profiles: Follow the format example shown below to compile a user-defined profile. Otherwise, even if the file is uploaded successfully, it will not take effect in the system.

```
Software Version 5.5 SG6000-MX_MAIN-68-V6-r1018.bin
202211040257
!
Version 5.5R10
subVersion 1.0
isp-network testv6 ipv6
subnet 1::1/128
subnet 2::2/128
member CERNET-v6
exit
```

Uploading a User-defined IPv6 ISP Profile

To upload a user-defined IPv6 ISP profile through the FTP/FTPS/SFTP/TFTP server, in the execution mode, use the following command:

import ispfile from {**ftp server***ip-address* [**user***user-name***password***password*] | **ftps server***ip-address* [**user***user-name***password***password*] | **sftp server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address* } [**vrouter***vr-name*] *file-name*

- *ip-address* - Specifies the IP address of the FTP/FTPS/SFTP/TFTP server.
- **user***username***password***password* - Specifies the user name and password accessing the FTP/FTPS/SFTP server.
- **vrouter***vr-name* – Specifies the VRouter where the FTP/FTPS/SFTP/TFTP server belongs.
- *file-name* - Specifies the name of the user-defined IPv6 ISP profile.

Downloading a User-defined IPv6 ISP Profile

The custom ISP profiles can only be saved through WebUI. To save an IPv6 ISP profile to your PC, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select **IPv6** tab.
3. Click **Download** to open the **Download User Defined ISP File** panel.
4. Select an ISP profile from the **ISP profile** drop-down list.
5. Click **OK** to save the profile to a specified location in PC.

Source Route

The source route can only be configured in the VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

Adding a Source Route

To add a source route, in the VRouter configuration mode, use the following command:

ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*] [**track***track-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the destination address. The Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*).If the next hop type is interface, you can select a tunnel interface, Null0 interface or PPPoE interface.

- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

To delete the specified source route, in the VRouter configuration mode, use the following command:

no ip route source { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

Viewing Source Route Information

To view the source route information, in any mode, use the following command:

show ip route source [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the source route information of the specified VRouter.

Src-If Route

The Src-If route can only be configured in the VRouter configuration mode. To enter the VRouter configuration mode, in global configuration mode, use the following command:

ip vrouter *vrouter-name*

Adding a Src-If Route

To add a Src-If route, in the VRouter configuration mode, use the following command:

ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*] [**track***track-name*

- *interface-name* - Specifies the ingress interface of the route.
- *A.B.C.D/M | A.B.C.D A.B.C.D* - Specifies the destination address. The Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* - Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface or Null0 interface.
- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

To delete the specified Src-If route, in the VRouter configuration mode, use the following command:

no ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* }

Viewing Src-If Route Information

To view the Src-If route information, in any mode, use the following command:

show ip route source in-interface *interface-name*

Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet, and specify the next hop of the packets which match the policy.

Creating a PBR Policy

To create a PBR policy, in the global configuration mode, use the following command:

pbr-policy *name*

- *name* - Specifies the name of the PBR policy. The length is 1 to 31 characters. If the policy exists, the system will directly enter the PBR policy configuration mode.

To delete the specified PBR policy, use the command**no pbr-policy** *name*.

Creating a PBR Rule

To create a PBR rule, in the PBR policy configuration mode, use the following command:

{**match** | **match-v6** } [**id** *rule-id*] [**before***rule-id* | **after** rule-id | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id*- Specifies the ID of the new PBR rule. The value range is 1 to 255. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in its

corresponding PBR policy.

- **before** *rule-id* | **after** *rule-id* | **top** - Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the new rule at the end of all the rules.
- *src-addr* - Specifies the source address which should be an entry defined in the address book.
- *dst-addr* - Specify the destination address which should be an entry defined in the address book.
- *service-name* – - Specifies the name of the service.*service-name*should be the service defined in the service book.
- *application-name* – Specifies the name of the application.*application-name* should be the application defined in the application book.
- **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} - Specifies the next hop. *interface-name* is the name of egress interface, *A.B.C.D* is the IP address of the next hop, **vrouter** *vrouter-name* is a VRouter, and **vsys** *vsys-name* is the name of VSYS.
- **weight** *value* - Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, the system will distribute the traffic in proportion to the corresponding weight.
- **track** *track-object-name* - Specifies the track object for the next hop. If the track object fails, the PBR rule will fail as well. For more information about track object, see "Configuring a Track Object" in "System Management".

To delete the specified rule, in the PBR policy configuration mode, use the following command:

no match id *rule-id*

In addition, you can also use the following command in PBR policy configuration mode to create a PBR rule ID, and then in the PBR policy rules configuration mode, further configure other relevant parameters of the PBR rule:

match [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* - Specifies the ID of the new PBR rule. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in the whole system. However, the PBR rule ID is not related to the matching sequence.
- **top** | **before** *rule-id* | **after** *rule-id* - Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the newly created rule at the end of all the rules.



Notes: For more information about how to configure other policy-related parameter, see "Editing a PBR Rule" 。

Editing a PBR Rule

You can edit an existing PBR rule by modifying its inappropriate parameters. However, this modification can only be performed in the PBR policy configuration mode. To enter the PBR policy configuration mode, use the following commands:

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-id*(only applicable to the existing rule ID. To delete the rule, use the command**no match id** *rule-id*)

To edit the rule, in the PBR policy rules configuration mode, use the following commands:

- Add a source address of address entry type: **src-addr** *src-addr*
- Delete a source address of address entry type: **no src-addr** *src-addr*
- Add a source address of IP address type: **src-ip** {*ip/netmask* | *ip-addressnetmask*}
- Delete a source address of IP address type: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Add a source address of host name type: **src-host** *host-name*

- Delete a source address of host name type: **no src-host** *host-name*
- Add a source address of IP range type: **src-range** *min-ip max-ip*
- Delete a source address of IP range type: **no src-range** *min-ip max-ip*
- Add a destination address of address entry type: **dst-addr** *dst-addr*
- Delete a destination address of address entry type: **no dst-addr** *dst-addr*
- Add a destination address of IP address type: **dst-ip** *ip/netmask*
- Delete a destination address of IP address type: **no dst-ip** *ip/netmask*
- Add a destination address of host name type: **dst-host** *host-name*
- Delete a destination address of host name type: **no dst-host** *host-name*
- Add a destination address of IP range type: **dst-range** *min-ip* [*max-ip*]
- Delete a destination address of IP range type: **no dst-range** *min-ip* [*max-ip*]
- Add a source user of role type: **role** *role-name*
- Delete a source user of role type: **no role** *role-name*
- Add a source user of user type: **user** *aaa-server-name user-name*
- Delete a source user of user type: **no user** *aaa-server-name user-name*
- Add a source user of user group type: **user-group** *aaa-server-name user-group-name*
- Delete a source user of user group type: **no user-group** *aaa-server-name user-group-name*
- Add a service: **service** *service-name*
- Delete a service: **no service** *service-name*
- Add an application: **application** *application-name*

- Delete an application: **no application** *application-name*
- Specify the next hop: **nexthop** {*interface-name* | *A.B.C.D* | *vrouter-name* | **vsys** *vsys-name*}
- Cancel the next hop: **no nexthop**
- Specify a schedule: **schedule** *schedule-name*
- Delete the schedule: **no schedule**
- Add a rule description: **description** *string*
- Delete a rule description: **no description**
- Enable the logging function for PBR rules： **log enable**
- Disable the logging function for PBR rules： **no log enable**

Enabling/Disabling a PBR Rule

By default the configured PBR rules will take effect immediately. You can disable a rule to end its control over traffic. To enable or disable a PBR rule, in the PBR policy rules configuration mode, use the following commands:

- Disable: **disable**
- Enable: **enable**

Moving a PBR Rule

Each PBR rule is labeled with a unique ID. When traffic flows into a Hillstone device, the device will query for PBR rules by turn, and processes the traffic according to the first matched rule. However, the PBR rule ID is not related to the matching sequence during the query. The rule sequence displayed by the command show pbr-policy is the actual sequence for the rule matching (the system will match the rules from the top to the bottom). You can specify the location of a PBR policy rule when creating the rule or moving its position in the PBR policy rule configuration mode. The positions of a PBR policy rule can be either an absolute position, i.e., at the

top or bottom, or a relative position, i.e., before or after a specific rule ID. To move a PBR rule, in the PBR policy configuration mode, use the following command:

move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

Configuring Prioritized Destination Routing Lookup

By default, when forwarding the inbound packets, the device selects a route in the following sequence: PBR > SIBR > SBR > Destination Routing. In some cases, users need to prioritized the destination route for the packets that are matching a PBR rule, that is the sequence is Destination Routing >PBR. To configure the prioritized destination routing (DBR) lookup, in the PBR policy configuration mode, use the following command:

fib-lookup dbr-first

To cancel prioritized destination routing (DBR) lookup, in the PBR policy configuration mode, use the following command:**no fib-lookup dbr-first**

Applying a PBR Rule

You can apply a PBR rule by binding it to an interface, zone or VRouter. In the interface configuration mode , security zone configuration mode or VRouter configutation mode, use the following command:

bind pbr-policy *name*

- *name* - The interface , security zone or VRouter the specified PBR rule is bound to.

To cancel the PBR rule binding to the interface, security zone or VRouter, in the interface configuration mode , security zone configuration mode or VRouter configutation mode, use the following command:

no bind pbr-policy

Configuring the Global Match Order of PBR

By default, If the PRB rule is bound to both an interface , VRouter and the security zone the interface belongs to, the traffic matching sequence will be: Interface > Zone > VRouter. You can configure the global match order of PBR, in global configuration mode, use the following command:

pbr-match order *index*

- *index* – Specifies the index of global match order of PBR, including 1 to 6, the order index is expressed as follows:
  - 1 – Interface >Zone >Vrouter, it is the default match order of PBR.
  - 2 – Zone >interface >Vrouter.
  - 3 - Vrouter >Zone > Interface.
  - 4 - Interface -> Vrouter >Zone.
  - 5 - Vrouter > Interface > Zone.
  - 6 – Zone > Vrouter > Interface.

To restore to the default match order, in the global configuration mode, use the command **no pbr-match**.

Viewing the the Global Match Order of PBR

In any mode, use the following command:

show pbr-match order

Configuring TTL Range for a PBR Rule

You can configure TTL range of packets for a PBR rule, and packet which matches the PBR rule will be forwarded to the specific export link. To configure TTL range, you need to enter PBR policy rule configuration mode first, use the following commands:

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-i*d(only applicable to the existing rule ID)

In the PBR policy rule configuration mode, use the following commands:

ttl-range *min-ttl max-ttl*

- *min-ttl max-ttl* - Specifies the TTL range for the PBR rule. *min-ttl* specifies the minimum value of TTL, and it is in the range of 1 to 255. *max-ttl* specifies the maximum value of TTL, and it is in the range of 1 to 255.

In the PBR policy rule configuration mode, use **no ttl-range** command to cancel the TTL configuration.

Viewing PBR Rule Information

To view the specific PBR rule information, in any mode, use the following command to:

show pbr-policy [*name*]

- *name* - Shows the specified PBR rule information. If no name is specified, the command will show the details of all the PBR rules.

DNS Redirect

The DNS redirect function redirects the DNS requests to a specified DNS server. In this version, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy based route working together, the system can redirect the Web video traffic to different links, improving the user experience.

To enable or disable the DNS redirect function, in the global configuration mode, use the following command:

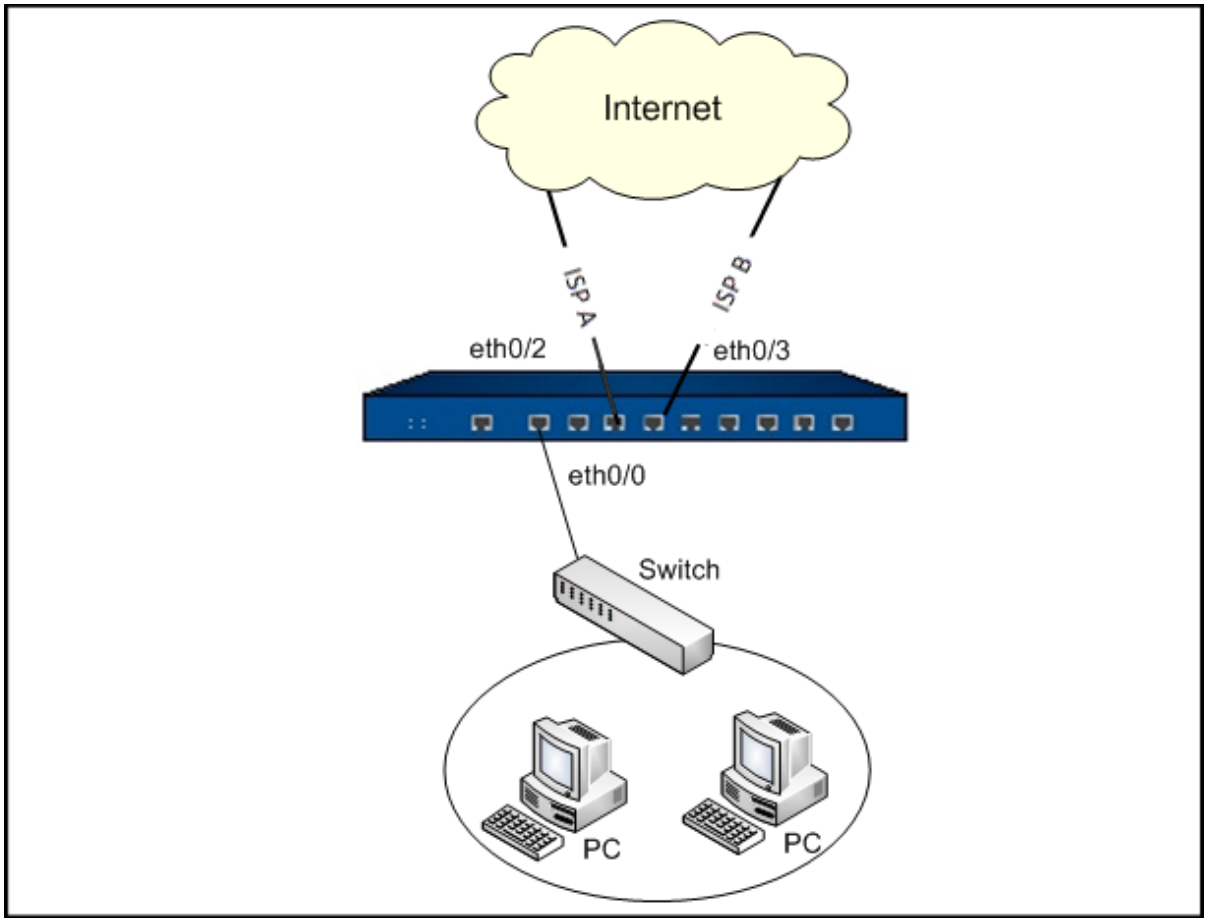
app cache dns-redirect {**enable** | **disable**}

- **enable** – Enable the DNS redirect function. After enabling this function, specify the DNS server address according to the prompts provided by the system. Then the DNS requests will be redirect to the specified DNS server.
- **disable** – Disable the DNS redirect function. It is the default status of the function.

In any mode, use the **show dns-redirect** command to show the binding status between the DNS server and the ingress interface that is bound to the PBR policy.

Configuration Example of Web Video Traffic Redirection

Hillstone device is deployed at the ingress interface of the internet. The ethernet0/0 interface connects to the PC, and the ethernet0/2 and ethernet0/3 interfaces connect to two ISP lines, ISP A and ISP B. After configuring the DNS redirect settings and the PBR policies, the traffic that matches the default route will flow out from the ethernet0/2, and the traffic that matches the policy-based route will flow out from the ehternet0/3. The topology is shown as below:



The configurations are shows as follows:

Step 1: Configure the interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone dmz
hostname(config-if-eth0/2)# ip address 10.180.41.52/20
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 172.31.1.240/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure the policies:

```
hostname(config)# rule id 1 from any to any service any permit
```

Step 3: Configure SNAT settings:

```
hostname(config)# nat
hostname(config-nat)# snatrule from any to any service any trans-to eif-ip mode dynamicport
```

Step 4: Configure the default routes:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 10.180.32.1
```

Step 5: Configure a policy-based route and bind it to the interface:

```
hostname(config)# pbr-policy test
hostname(config-pbr)# match top any any any YOUKU-DNS nexthop 172.31.1.1
Match id 1 is created.
hostname(config-pbr)# match id 1
hostname(config-pbr-match)# application YOUKU
hostname(config-pbr-match)# application RTMFP
```

```
hostname(config-pbr-match)# exit
hostname(config-pbr)# exit
hostname(config)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bind pbr-policy test
hostname(config-if-eth0/0)# exit
```

Step 6: Configuring ISP routes:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route China-netcom 172.31.1.1
hostname(config-vrouter)# exit
```

Step 7: Upgrading APP signature database:

```
hostname(config)# exec app update professional
```

Step 8: Enabling the application identification:

```
hostname(config)# zone trust
hostname(config-zone-trust)# application-identify
```

Step 9: Enabling the DNS redirect and configuring the IP address of the DNS server:

```
hostname(config)# app cache dns-redirect enable
Please specify the IP address for the DNS server
hostname(config)# ip name-server 58.240.57.33
```

Domain Name Route

The domain name route supports the configuration of destination domain name and next-hop address. It establishes and updates the mapping information between the destination domain name and the IP addresses through DNS Snooping active domain name resolution mode or passive domain name resolution mode, so as to generate routing entries. The system queries the des-

tination IP address in the routing entries and forwards the data. Meanwhile, domain name route can be redistributed to other routers with OSPF enabled.

For how to configure the DNS Snooping active domain name resolution mode or passive domain name resolution mode, refer to DNS Snooping. For how to redistribute domain name route, refer to Configuring Redistribute.

Configuring a Domain Name Route

You can add a domain name route and view the route's information.

Adding a Domain Name Route

You can add a domain name routing entry to VRouter. However, before adding the entry, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To add a domian name route, in the VRouter configuration mode, use the following command:

domain route *domain-name* {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- **domain route** - Specifies the destination domain name. It only supports the specific domain name (e.g., www.test.com).
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*- Specifies the type of next hop which can be a gateway address (*A.B.C.D*), interface (*interface-name*) or VRouter (**vrouter** *vrouter-name*). If the next hop type is interface, you can select a tunnel interface (for multi-tunnel interface, you must specify the next hop IP address of IPsec VPN, GRE or SSL VPN tunnel by the *A.B.C.D* parameter, and this address must be the same as the next hop IP address of the corresponding tunnel bound to the tunnel interface), Null0 interface or PPPoE interface.

- *distance-value* - Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- **weight** *weight-value* - Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description** *description* – Specifies the description of this route. You can enter at most 63 characters.
- **schedule** *schedule-name*- Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

Repeat the above command to add more domain name routes.

To delete the specified domain name route, use the following command:

no domain route *domain-name* {*A.B.C.D* | *interface-name A.B.C.D* | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

Viewing Domain Name Routing Information

To view the domain name routing information, in any mode, use the following command:

show domain-route status [**vrouter** *vrouter-name*]

- *vrouter-name* - Specifies the domain name routing information of the specified VRouter.

Dynamic Routing

Dynamic routing refers to the routing that will be automatically adjusted based on the operation status of network. Hillstone devices will automatically adjust the dynamic routing table according to the routing protocol being used. StoneOS support 4 dynamic routing protocols: RIP, OSPF, IS-IS, and BGP.

Configuring RIP

RIP, the abbreviation for Routing Information Protocol, is an internal gateway routing protocol that is designed to exchange routing information between routers. At present Hillstone devices support both RIP versions, i.e., RIP-1 and RIP-2.

RIP configuration includes basic options, redistribute, passive IF, neighbor, network and distance. Besides, you also need to configure RIP parameters for different interfaces, including RIP version, split horizon and authentication mode.

Basic Options

The basic options of RIP configuration include version, metric, distance, information originate and timer (update interval, invalid time, holddown time and flush time). You can configure RIP protocol for different VRouter respectively. The basic options of RIP must be configured in the RIP routing configuration mode. To enter the RIP routing configuration mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router rip (enters the RIP routing configuration mode, and at the same time enables the RIP function on the device)

To disable RIP, in the VRouter configuration mode, use the command **no router rip**.

Specifying a Version

Hillstone devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. To specify the RIP version, in the RIP routing configuration mode, use the following command:

version *version-number*

- *version-number* - Specifies the version number which can be 1 (RIP-1) or 2 (RIP-2). The default version number is 2.

To restore to the default version, in the RIP routing configuration mode, use the command **no version**.

Specifying a Metric

RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, and increments by 1 for every additional router between them. The maximum metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed. To specify the default metric, in the RIP routing configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 15. If no value is specified, the value of 1 will be used.

To restore to the metric value of 1, in the RIP routing configuration mode, use the command **no default-metric**.

Specifying a Distance

To specify the default distance for RIP, in the RIP routing configuration mode, use the following command:

distance *distance-value*

- *distance-value* - Specifies the default administration distance value. The value range is 1 to 255. If no value is specified, the value of 120 will be used.

To restore to the distance value of 120, in the RIP routing configuration mode, use the command **no distance**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. To configure the default information originate, in the RIP routing configuration mode, use the following commands:

Redistribute: **default-information originate**

Do not redistribute: **no default-information originate**

Specifying a Timer

The timers you can configure for RIP include update interval, invalid time, holddown time and flush time, as described below:

- Update interval: Specifies the interval at which all RIP routes will be sent to all the neighbors. The default value is 30 seconds.
- Invalid time: If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The default value is 180 seconds.
- Holddown time: If the metric becomes larger (e.g., from 2 to 4) after a route has been updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The default value is 180 seconds.
- Flush time: StoneOS will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the flush time ends, it will be deleted from the RIP information database. The default value is 240 seconds.

To modify the above four timers, in the RIP routing configuration mode, use the following command:

timers basic *interval-time invalid-time holddown-time flush-time*

- *interval-time* - Specifies the update interval time. The value range is 0 to 16777215 seconds. The default value is 30.
- *invalid-time* - Specifies the invalid time. The value range is 1 to 16777215 seconds. The default value is 180.
- *holddown-time* - Specifies the holddown time. The value range is 1 to 16777215 seconds. The default value is 180.
- *flush-time* - Specifies the flush time. The value range is 1 to 16777215 seconds. The default value is 240.

To restore to the default timer value, in the RIP routing configuration mode, use the command **no timers basic**.

Configuring Redistribute

RIP allows you to introduce information from other routing protocols (BGP, connected, static and OSPF) and redistribute the information. To configure the redistribute metric, in the RIP routing configuration mode, use the following commands:

redistribute {**bgp** | **connected** | **static** | **ospf** | **isis**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf** | **isis**- Specifies the protocol type which can be **bgp**, **connected**, **static** , **OSPF** or **isis**.
- **metric** *value*- Specifies a metric value for the redistribute. The value range is 1 to 15. If the value is not specified, the system will use the default RIP metric configured by the command default-metric value.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the RIP routing configuration mode, use the command**no redistribute** {**bgp** | **connected** | **static** | **ospf** | **isis**}.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the RIP routing configuration mode, use the following command:

passive-interface *interface-name*

- *interface-name* - Specifies the interface as a passive interface.

Repeat the above command to configure multiple passive interfaces.

To cancel the specified passive interface, in the RIP routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring a Neighbor

You can specify some neighbors to allow P2P (non-broadcasting) RIP information exchanges between the neighbors and Hillstone devices. To configure a neighbor, in the RIP routing configuration mode, use the following command:

neighbor *ip-address*

- *ip-address* - Specifies the IP address of the neighbor.

Repeat the above command to configure more passive neighbors.

To delete the specified neighbor, in the RIP routing configuration mode, use the command **no neighbor** *ip-address*.

Configuring a Network

You can configure some networks so that only the interfaces within the specified networks can receive and send RIP update. To configure a network, in the RIP routing configuration mode, use the following command:

network *ip-address/netmask*

- *ip-address/netmask* - Specifies the IP address of the network, for example, 10.200.0.0/16.

Repeat the above command to configure more networks.

To delete the specified network, in the RIP routing configuration mode, use the command **no network** *ip-address/netmask*.

Configuring a Distance

You can specify an administration distance for the routes that are obtained from the specified networks. To configure a distance, in the RIP routing configuration mode, use the following command:

distance *distance-value ip-address/netmask*

- *distance-value* - Specifies the administration distance value. The value range is 1 to 255. The priority of this distance is higher than that of the default distance configured in the basic RIP options specified by the command
- *ip-address/netmask* - Specifies the IP address of the network, for example, 10.200.0.0/16.

Repeat the above command to configure a distance for the routes that are obtained from different networks.

To delete the specified distance, in the RIP routing configuration mode, use the command **no distance** *ip-address/netmask*.

RIP Database

When a Hillstone device is running RIP, it will own a RIP route database which can store all routing entries for all the reachable networks. The routing entry information includes destination address, next hop, metric, source, and timer information. To view the RIP database information, in any mode, use the following command:

show ip rip database [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D/M* - Shows the RIP information of the specified destination IP address.
- **vrouter** *vrouter-name*- Shows the RIP information of the specified VRouter. At present StoneOS only supports VRouter named trust-vr.

Configuring RIP for Interfaces

The RIP configuration for the interfaces of Hillstone devices includes: authentication mode, transmit and receive version, and split horizon. The RIP configuration for the interfaces must be done in the interface configuration mode.

Configuring an Authentication Mode

Only RIP-2 supports authentication on RIP packets. The packet authentication mode includes plain text and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that

require high security. The default mode is plain text authentication. To configure the authentication mode and authentication string for the RIP packets, in the interface configuration mode, use the following commands:

- Authentication mode: **ip rip authentication mode** {**md5** | **text**}
- Authentication string: **ip rip authentication string** *string*

To cancel the specified authentication mode and authentication string, in the interface configuration mode, use the following commands:

- **no ip rip authentication mode**
- **no ip rip authentication string**

Specifying RIP Version

By default RIP-2 information will be transmitted. To specify the RIP version number that will be transmitted, in the interface configuration mode, use the following command:

ip rip send version [1][2]

- **1** - Only RIP-1 information will be transmitted.
- **2** - Only RIP-2 information will be transmitted.

To restore to the default version number, in the interface configuration mode, use the command **no ip rip send version**.

By default RIP-2 information will be received. To specify the RIP version number that will be received, in the interface configuration mode, use the following command:

ip rip receive version [1][2]

- **1** - Only RIP-1 information will be received.
- **2** - Only RIP-2 information will be received.

To restore to the default version number, in the interface configuration mode, use the command **no ip rip receive version**.

Configuring Split Horizon

In split horizon, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent. To enable or disable split horizon, in the interface configuration mode, use the following commands:

Enable: **ip rip split-horizon**

Disable: **no ip rip split-horizon**

Viewing System RIP Information

To view the RIP information of system, in any mode, use the following command:

show ip rip

To view the RIP route information, in any mode, use the following command:

show ip *route rip* [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the RIP router information of the specified VRouter.

Configuring OSPF

OSPF, the abbreviation for Open Shortest Path First, is an internal gateway protocol based on link state developed by IETF. The current version of OSPF is version 2 (RFC2328). OSPF is applicable to networks of any size. Its quick convergence feature can send update message immediately after the network topology has changed, and its algorithm assures it will not generate routing loops. OSPF also have the following characteristics:

- Area division: divides the network of autonomous system into areas to facilitate management, thereby reducing the protocol’s CPU and memory utilization, and improving performance.
- Classless routing: allows the use of variable length subnet mask.
- ECMP: improves the utilization of multiple routes.
- Multicasting: reduces the impact on non-OSPF devices.
- Verification: interface-based packet verification ensures the security of the routing calculation.



Tip: Autonomous system is a router and network group under the control of a management institution. All routers within an autonomous system must run the same routing protocol.

Configuring OSPF Protocol

You can configure OSPF protocol for different VRouters respectively. The configuration of OSPF protocol includes:

- Configuring a Router ID
- Configuring area authentication
- Configuring route aggregation for an area
- Configuring the default cost for an area
- Configuring the virtual link for an area
- Specify the ID and password for MD5 authentication.
- Configuring the default cost for sending OSPF packets
- Configuring a default metric
- Configuring the default information originate
- Configuring the default distance
- Configuring an OSPF timer
- Specifying the network that runs OSPF protocol
- Configuring redistribute
- Configuring a distance

- Configuring a Passive IF
- Configuring Route Filters Based on the Route Access-list
- Configuring OSPF GR

The basic options of OSPF protocol must be configured in the OSPF routing mode. To enter the OSPF routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router ospf [*process-id*] ((enters the OSPF routing mode, and at the same time enables OSPF on the device)

- *process-id* – Specify the OSPF process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPF process is individual, and has its own link state database and the related OSPF routing table. Each VRouter supports up to 4 OSPF processes and multiple OSPF processes maintain a routing table together.

When specifying the OSPF process ID, note the following matters:

- When running multiple OSPF processes in a VRouter, the network advertised in interfaces in each OSPF process cannot be same.
- When route entries with the same prefix exist in multiple OSPF processes, the system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table.
- If the OSPF route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPF will not be redistributed.

To disable OSPF, in the VRouter configuration mode, use the command **no router ospf** [*process-id*].

Configuring a Router ID

Each router running OSPF protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPF domain, represented in the form of an IP address. To configure a Router ID for the Hillstone device that is running OSPF protocol, in the OSPF routing mode, use the following command:

router-id *A.B.C.D* [**local**]

- *A.B.C.D* - Specifies the Router ID used by OSPF protocol, in form of an IP address.
- **local** - Specifies the Router ID as a local configuration. This kind of configuration is applicable to HA A/A mode, and is not synchronized to HA configuration. By default the router ID is not a local configuration.

Configuring Area Authentication

By default, there is no area authentication. To configure an area authentication mode, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **authentication** [**message-digest**]

- *id* | *A.B.C.D* - Specifies an area ID, in form of a 32-bit digital number, or an IP address.
- [**message-digest**] - Specifies the MD5 authentication. If the keyword is not specified, then the system will use the plain text authentication.

The authentication mode specified by the above command must be the same as that of the other routers within the area; the authentication password for routers that communicate over OSPF in the same network must be the same.

To cancel the specified area authentication mode, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **authentication**.

Specifying the Network Type for an Interface

In OSPF, the network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. To configure the network type of an interface, in the interface configuration mode, use the following command:

ip ospf network {point-to-point | point-to-multipoint}

- point-to-point – Specifies the network type of an interface as the point-to-point type.
- point-to-multipoint - Specifies the network type of an interface as the point-to-multipoint type.

To set the network type as the default broadcast type, use the following command:

no ip ospf network

Configuring Route Aggregation for an Area

Route aggregation refers to aggregating the routing information with the same prefix together through ABR, and then only advertising one route to other areas. You can configure multiple aggregation segments in one area, so that OSPF can aggregate multiple segments. By default, the route aggregation function is disabled. To configure route aggregation for an area, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} range {*A.B.C.D/M*} [advertise | not-advertise]

- *id* | *A.B.C.D*- Specifies an area ID that will perform the route aggregation, in form of a 32-bit digital number, or an IP address.
- range {*A.B.C.D/M*} - Specifies the network segment that will be aggregated.
- advertise - Specifies to aggregate the routes of the segment and advertises the aggregated route.
- not-advertise -Specifies to aggregate the routes of the segment, but do not advertise the aggregated route.

The route aggregation function is only applicable to an area border router (also known as ABR, the router that connects the backbone area and non-backbone area).

To cancel the route aggregation, in the OSPF routing mode, use the command no area {*id* | *A.B.C.D*} range {*A.B.C.D/M*} [advertise | not-advertise].

Configuring the Default Cost for an Area

The default cost of an area refers to the default routing cost for sending a packet to the stub area. To configure default cost for an area, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **default-cost** *cost-value*

- *id* | *A.B.C.D* - Specifies an area ID the default cost will be applied to, in form of a 32-bit digital number, or an IP address.
- *cost-value* - Specifies a cost value. The value range is 0 to 16777214. If no value is specified, the system will use the value of 1.

To restore to the cost value of 1, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **default-cost**.



Notes: This command is only applicable to NSSA.

Configuring the Virtual Link for an Area

Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. To configure virtual link parameters and its timer parameters, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval** *interval-value*] [**retransmit-interval** *interval-value*] [**transmit-delay** *interval-value*] [**dead-interval** *interval-value*]

- *id* | *A.B.C.D* - Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- **virtual-link** *A.B.C.D* - Specifies the Router ID that is used as a virtual link router.
- **hello-interval** *interval-value* - Specifies the interval for sending the Hello packets. The value range is 1 to 65535 seconds. The default value is 10.
- **retransmit-interval** *interval-value* - After sending a LSA packet to its neighbor, a router will wait for the acknowledge from the peer. If no ACK packet is received after the specified

interval, the router will retransmit this LSA packet to the neighbor. The parameter is used to specify the retransmit interval. The value range is 3 to 65535 seconds. The default value is 5.

- **transmit-delay** *interval-value* - Specifies the transmit delay time of the update packets. The value range is 1 to 65535 seconds. The default value is 1.
- **dead-interval** *interval-value* - If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. This parameter is used to specify the value of dead interval. The value range is 1 to 65535 seconds. The default value is 40.

To restore to the default timer values, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**dead-interval**].

To configure the authentication mode of the virtual link, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID* **md5** *string*] [**null**]

- *id* | *A.B.C.D* - Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- **virtual-link** *A.B.C.D* - Specifies the Router ID that is used as a virtual link router.
- **authentication-key** *string* - Specifies the password for the plain text authentication.
- **message-digest-key** *ID* **md5** *string* - Specifies to use MD5 authentication.
- **null** - No authentication.

To cancel the authentication mode, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID*].

Configuring a Stub Area

The stub area refers to the area that does not send or receive Type-5 LSA (AS-external-LSAs). For the network that generates large amount of Type-5 LSAs, this approach can effectively reduce the router LSDB size within the stub area, and the resource occupation arising from SPF calculation on the router. The stub area is usually located at the border of the autonomy system. To configure the stub area of OSPF, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **stub** [**no-summary**]

- *id* | *A.B.C.D* - Specifies an ID for the stub area, in form of a 32-bit digital number, or an IP address.
- **no-summary** - Stops ABR from sending Type 3 or Type 4 Summary LSA to the stub area.

To cancel the specified stub area, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **stub** [**no-summary**].

Configuring a NSSA Area

A stub area cannot redistribute routes. You can configure the area as an NSSA area to allow for route redistribution by keeping other stub area characteristics. To configure the NSSA area of OSPF, in the OSPF routing mode, use the following command:

area {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

- *id* | *A.B.C.D* - Specifies an ID for the NSSA area, in form of a 32-bit digital number, or an IP address.
- **no-summary** | **no-redistribution** | **default-information-originate** - **no-summary** allows an area to be a not-so-stubby area but not have summary routes injected into it. **no-redistribution** is used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area. **default-information-originate** is used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.

To cancel the specified NSSA area settings, in the OSPF routing mode, use the command **no area** {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

Configuring the Reference Bandwidth for OSPF

OSPF can calculate the cost of sending OSPF packets for an interface based on the interface bandwidth. To configure reference bandwidth, in the OSPF routing mode, use the following command:

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* - Specifies the bandwidth value. The value range is 1 to 4294967 Mbps. The default value is 100.

To calculate the cost of sending OSPF packets for an interface based on the interface type, in the OSPF routing mode, use the command**no auto-cost reference-bandwidth**

Configuring the Default Metric

The default metric configured here will take effect when redistributing. To specify the default metric for OSPF, in the OSPF routing configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 16777214.

To restore to the original metric value, in the OSPF routing configuration mode, use the command **no default-metric**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with OSPF enabled. By default OSPF will not redistribute the default route. To configure the default information originate, in the OSPF routing configuration mode, use the following command:

default-information originate [**always**] [**type** {1 | 2}] [**metric** *value*]

- **always** - OSPF unconditionally generates and redistributes the default route.
- **type** {**1** | **2**} - Specifies the type of the external route associated with the default route that is sent to OSPF routing area. 1 refers to type1 external route, 2 refers to type2 external route.
- **metric** *value* - Specifies the metric value for the default route that will be sent. If no default metric value is specified by this command or by the command default-metric value, then OSPF will use the value of 20. The value range is 0 to16777214.

To restore to the value of 20, in the OSPF routing configuration mode, use the command **no default-information originate**.

Configuring the Default Distance

To configure the default distance for OSPF route, in the OSPF routing configuration mode, use the following command:

distance *distance-value*

- *distance-value* - Specifies the default administration distance value. The value range is 1 to. 255. If no value is specified, OSPF will use the value of 110.

To restore to the value of 110, in the OSPF routing configuration mode, use the command **no distance**.

Configuring a Timer for OSPF

You can specify the following two OSPF protocol timers: how long OSPF will re-calculate the path after receiving an update, and the interval between the two OSPF calculations. To configure an OSPF timer, in the OSPF routing configuration mode, use the following command:

timers spf *delay1 delay2*

- *delay1* - After receiving the update, OSPF will re-calculate the path within the specified period. The value range is 0 to 65535 seconds. The default value is 5.
- *delay2* - Specifies the interval between the two calculations. The value range is 0 to 65535 seconds. The default value is 10.

To restore to the value of 5 or 10, in the OSPF routing configuration mode, use the command **no timers spf**.

Specifying an OSPF Network Interface

To specify the network interface that enables OSPF and add the network to the specified area, in the OSPF routing configuration mode, use the following command:

network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

- *A.B.C.D/M* - Specifies the network interface that enables OSPF protocol.
- **area** {*id* | *A.B.C.D*} - Specifies the area ID the network will be added to, in form of a 32-bit digital number, or an IP address.

To cancel the specified network interface, in the OSPF routing configuration mode, use the command **no network** *A.B.C.D/M* **area** {*id* | *A.B.C.D*}.

Configuring Redistribute

OSPF allows you to introduce information from other OSPF processes and routing protocols (BGP, IS-IS, connected, static, RIP, VPN and Domain Name routing) and redistribute the information. You can set the metric and type of the external route for the redistribute, or filter the routing information based on a route map and only distribute specific routing information. To configure the redistribute metric, in the OSPF routing configuration mode, use the following command:

redistribute {**bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn** | **domain** } [**type** {**1** | **2**}] [**metric** *value*] [**route-map** *name*] [**tag** *tag-value*]

- **bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn** - Specifies the protocol type which can be **bgp**, **connected**, **isis**, **ospf**, **static**, **rip**, **VPN** or **domain** (domain name routing). When introducing information from other OSPF processes, specify the process.
- **type** {**1** | **2**} - Specifies the type of the external route. **1** refers to type1 external route, **2** refers type2 external route.

- **metric** *value* - Specifies a metric value for the redistribute. The value range is 0 to 16777214. If the value is not specified, the system will use the default OSPF metric configured by the command default-metric value.
- **route-map** *name* - Specifies the route map that is used to filter the routing information introduced from other routing protocols. For more information about route map, see Configuring a Route Map.
- **tag** *tag-value* – Specifies the tag values of the redistributed route. The value range is 1 to 4294967295.

Repeat the above command to redistribute a different type of routes.

To cancel the redistribute of specified route, in the OSPF routing configuration mode, use the command **no redistribute** {**bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn** |**domain**}.

Configuring a Distance

You can specify the administration distance based on the type of route. To configure the distance, in the OSPF routing configuration mode, use the following command:

distance ospf {**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- **intra-area** *distance-value* - Specifies the administration distance for the routes within an area. The value range is 1 to 255. The default value is 110.
- **inter-area** *distance-value* - Specifies the administration distance for the routes between areas. The value range is 1 to 255. The default value is 110.
- **external** *distance-value*- Specifies the administration distance for the external type5 route. The value range is 1 to 255. The default value is 110.

To restore to the default value, in the OSPF routing configuration mode, use the command **no distance ospf**.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the OSPF routing configuration mode, use the following command:

passive-interface *interface-name*

- *interface-name* - Specifies the interface as a passive interface.

Repeat the above command to configure more passive interfaces.

To cancel the specified passive interface, in the OSPF routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring Route Filters Based on the Route Access-list

OSPF uses the route access-list to filter the introduced route. To configure the route filter function based on the route access-list, use the following command in the OSPF routing configuration mode:

distribute-list *access-list-name* **in** [*interface-name*]

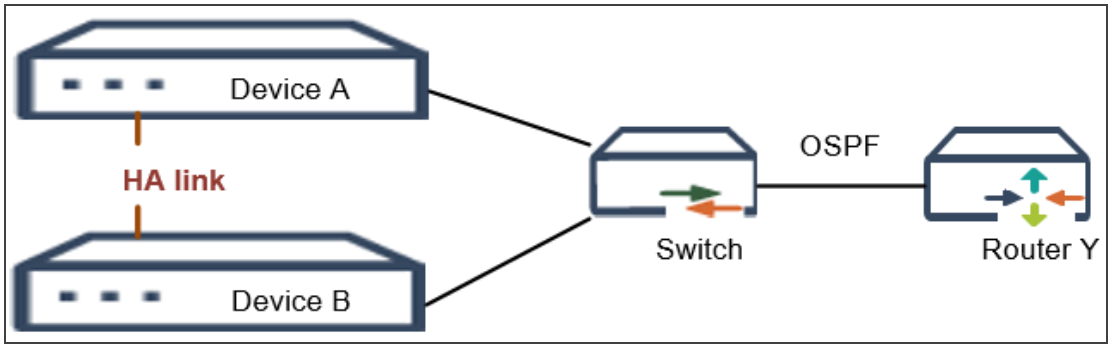
- *access-list-name* – Specifies name of the route access-list. For more information about route access-list, see Configuring a Route Access-list .
- **in** – Use **in** to filter the introduced routes.
- *interface-name* – Specifies name of the interface. After specifying this interface, the system will filter the OSPF route from the specified interface. If the interface name is not specified, the system will filter all OSPF routes.

Use the following command to cancel the above configurations:

no distribute-list *access-list-name* **in** [*interface-name*]

Configuring OSPF GR

Graceful Restart (GR) is also called Non-Stop Forwarding (NSF). In a network environment running the OSPF protocol, OSPF GR can ensure that network traffic is not interrupted during HA switchover.



As shown in the picture above, devices A and B form an HA Active-Passive (A/P) mode. During HA switchover, the OSPF neighborhood between the new primary device and the neighboring device Router Y will be disconnected and reestablished, causing route flapping and service interruption. After configuring the OSPF GR function, when performing HA switchover, the new primary device enters the GR Restarter state and sends a Grace LSA to neighbor Router Y, announcing information such as the GR interval, GR reason, and interface address. After receiving the Grace LSA, Router Y enters the GR Helper state and maintains neighborhood with the new primary device during the GR interval, assisting the new primary device in completing the GR and ensuring uninterrupted data forwarding.

Basic Concepts of OSPF GR:

- GR Restarter: GR Restarter is the device applying Graceful Restart during BGP restart or the switchover between backup and primary devices.
- GR Helper: Neighbor of the GR Restarter, a device that assists the GR Restarter in the GR process.
- Grace LSA: Grace LSA is a type of Type-9 LSA of Opaque LSA used to support the OSPF GR feature. It is generated during High Availability (HA) switchover and advertises information such as GR interval, GR reason, and interface address to OSPF neighbors.

Notes:

- OSPF GR feature supports HA Active-Passive (A/P) mode and SCM HA, but does not support HA Peer mode.

- Devices in the following scenarios can act as GR Restarter, while devices in other scenarios can only act as GR Helper:
  - The newly elected primary device after HA switchover
  - Devices (X6150/X6180/X7180/X9180/X10800/K9180) that perform SCM HA switchover.
- OSPF GR feature will not take effect if the HA connection between the primary and backup devices is disconnected.

Enabling Opaque LSA Capability

Opaque LSA is an extended universal mechanism for OSPF. It includes Type-9 LSA, Type-10 LSA, and Type-11 LSA. Opaque LSA supports OSPF GR functionality through the Grace LSA in Type-9 LSA.

Notes: Opaque LSA capability should be enabled before using the OSPF GR feature.

To enable Opaque LSA capability, in the OSPF routing mode, use the following command:

capability opaque

In the OSPF routing mode, use the command **no capability opaque** to disable Opaque LSA capability.

Enabling the GR function of the GR Restarter

To enable the GR function of the GR Restarter, in the OSPF routing mode, use the following command:

graceful-restart ietf enable

In the OSPF routing mode, use the command **no graceful-restart ietf enable** to disable the GR function of the GR Restarter.

Configuring GR Interval of the GR Restarter

GR interval refers to the timeout time of GR. During the GR interval, the GR Helper will maintain neighborhood with the GR Restarter. After the GR interval expires, regardless of whether the GR is complete or not, the GR Helper will exit the GR Helper state.

To configure the GR interval of the GR Restarter, in the OSPF routing mode, use the following command:

graceful-restart ietf interval*value*

- *value* - Specifies the GR interval of the GR Restarter. The value range is from 1 to 1,800 seconds. The default value is 120 seconds. It is recommended to extend the GR interval with this command when there are many neighbors.

In the OSPF routing mode, use the command **no graceful-restart ietf interval** to restore to the default value.

Enabling the GR Helper Feature

To enable the GR Helper feature, in the OSPF routing mode, use the following command:

graceful-restart ietf helper enable

In the OSPF routing mode, use the command **no graceful-restart ietf helper enable** to disable the GR Helper feature.

Enabling GR Helper Strict LSA Check

After configuring GR Helper Strick LSA Check, when the GR Helper device detects a change in LSA, it will exit the GR Helper state. To configure the GR Helper Strick LSA Check, in the OSPF routing mode, use the following command:

graceful-restart ietf helper strict-lsa-checking

In the OSPF routing mode, use the command **no graceful-restart ietf helper strict-lsa-checking** to disable GR Helper Strick LSA Check.

Viewing OSPF GR Information

To view information about OSPF GR, in any mode, use the following command:

show ip ospf graceful-restart [**vrouter***vrouter-name*]

- **vrouter***vrouter-name* - Shows the OSPF GR information of the specified VRouter. If no VRouter is specified, this command displays the OSPF GR information of the default VRouter (trust-vr).

Configuring OSPF for an Interface

The OSPF function for an interface must be configured in the interface configuration mode. The OSPF configuration for the Hillstone device's interfaces includes:

- Configuring OSPF authentication for an interface
- Specifying the link cost for an interface
- Configuring the timer for an interface
- Specifying the router priority for an interface
- Specifying the network type for an interface

Configuring OSPF Authentication for an Interface

The priority of OSPF authentication for an interface is higher than that of the OSPF authentication for an area. Hillstone devices support the plain text and MD5 authentication. By default the OSPF authentication for an interface is disabled. To enable or disable it, in the interface configuration mode, use the following commands:

ip ospf authentication

no ip ospf authentication

To configure the password for the plain text authentication, in the interface configuration mode, use the following command:

ip ospf authentication-key *string*

- *string* - Specifies the password (up to eight characters).

To cancel the specified password, in the interface configuration mode, use the command **no ip ospf authentication-key**.

To configure the MD5 authentication ID and password, in the interface configuration mode, use the following command:

ip ospf message-digest-key *ID* **md5** *string*

- *ID* - Specifies the authentication ID.
- *string* - Specifies the password.

To cancel the specified password, in the interface configuration mode, use the command **no ip ospf message-digest-key** *ID*.

Specifying the Link Cost for an Interface

To specify the link cost for an interface, in the interface configuration mode, use the following command:

ip ospf cost *cost-value* [**local**]

- *cost-value* - Specifies the link cost for an interface. The value range is 1 to 65535.
- **local** - Specifies the link cost for an interface as local. When the device is operating in the HA AA mode, the parameter will prevent the device from synchronizing the cost value to the backup device. Thus the two devices' link costs will be different, avoiding asymmetrical OSPF routes.

To cancel the specified link cost, in the interface configuration mode, use the command **no ip ospf cost** [**local**].

Configuring the Timer for an Interface

There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets.

To specify the interval for sending Hello packets for an interface, in the interface configuration mode, use the following command:

ip ospf hello-interval *interval*

- *interval* - Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10.

To restore to the default interval, in the interface configuration mode, use the command **no ip ospf hello-interval**.

If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. To configure the dead interval for an interface, in the interface configuration mode, use the following command:

ip ospf dead-interval *interval*

- *interval* - Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets).

To restore to the default dead interval, in the interface configuration mode, use the command **no ip ospf dead-interval**.

To specify the LSA retransmit interval for an interface, in the interface configuration mode, use the following command:

ip ospf retransmit-interval *interval*

- *interval* - Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5.

To restore to the default retransmit interval, in the interface configuration mode, use the command **no ip ospf retransmit-interval**.

To specify the transmit delay for updating packet for an interface, in the interface configuration mode, use the following command:

ip ospf transmit-delay *interval*

- *interval* - Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.

To restore to the default transmit delay, in the interface configuration mode, use the command **no ip ospf transmit-delay**.

Specifying the Router Priority for an Interface

The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and broadcast the received link information. To specify the router priority for an interface, in the interface configuration mode, use the following command:

ip ospf priority *level*

- *level* - Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router. If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.

To restore to the default priority, in the interface configuration mode, use the command **no ip ospf priority**.

Specifying the Network Type for an Interface

In OSPF, the network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. To configure the network type of an interface, in the interface configuration mode, use the following command:

ip ospf network {**point-to-point** | **point-to-multipoint**}

- **point-to-point** – Specifies the network type of an interface as the point-to-point type.。
- **point-to-multipoint** - Specifies the network type of an interface as the point-to-multipoint type.

To set the network type as the default broadcast type, use the following command:

no ip ospf network

Viewing OSPF Route Information

To view the OSPF route information, in any mode, use the following command:

show ip route ospf [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the OSPF route information of the specified VRouter name.

To view the OSPF information of the Hillstone device, in any mode, use the following command:

show ip ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* - Specifies the VRouter name.
- **process** *process-id* – Specifies the OSPF process.

To view the OSPF protocol’s database information of the Hillstone device, in any mode, use the following commands:

show ip ospf database {**asbr-summary** | **external** | **nssa-external** | **network** | **router** | **summary**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **asbr-summary** - Shows the LSAs of the AS border router
- **external** - Shows the LSAs of the external network.
- **nssa-external** - Shows the external LSAs information of NSSA.
- **network** Shows the LSAs of the network.
- **router** - Shows the LSAs of the router.
- **summary** - Shows the LSAs summary.
- *A.B.C.D* - Shows the IP address of link status ID.
- **adv-router** *A.B.C.D* - Shows the LSAs of the specified router.
- **self-originate** - Only shows self- originated LSAs(from local router).

- *vrouter-name* - Specifies the VRouter name.
- **process** *process-id* – Specifies the OSPF process.

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **max-age** - Specify the maximum age time.
- **self-originate** - Only shows self- originated LSAs(from local router).
- *vrouter-name* - Specifies the VRouter name.
- **process** *process-id* – Specifies the OSPF process.

To view the OSPF interface information, in any mode, use the following command:

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF virtual link information, in any mode, use the following command:

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF neighbor information, in any mode, use the following command:

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF route information, in any mode, use the following command:

show ip ospf route [*A.B.C.D*] [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the route map information, in any mode, use the following command:

show route-map [*name*]

To view the route access-list information, in any mode, use the following command:

show access-list route [*name*]

To view the route filtering information, in any mode, use the following command:

show ip ospf distribute-list [**vrouter** *vrouter-name*] [**process** *process-id*]

Configuring IS-IS

IS-IS (Intermedia System-to-Intermediate System) is a dynamic routing protocol that is designed by ISP for CLNP (Connection-Less Network Protocol). To make it support IP, IETF (Interface

Engineering Task Force) modified IS-IS in RFC 1195. With the modifications added, the new IS-IS, which is called Integrated IS-IS or Dual IS-IS, can be used in both TCP/IP environment and OSI environment. StoneOS supports the application of IS-IS in the TCP/IP environment.

You can configure the IS-IS for each virtual router. Configuring IS-IS includes the following sections:

- Configuring the Router Type
- Enabling IS-IS at Interfaces
- Configuring the Interface Type
- Configuring the Network as Point-to-Point Type
- Configuring the NET Address
- Configuring the Administrative Distance
- Configuring the Metric Style
- Configuring the Interface Metric
- Configuring Redistribute
- Configuring the Default Route Advertisement
- Configuring the Interval for Sending Hello Packets
- Configuring the Multiplier for Hello Packets
- Configuring Padding for Hello Packets
- Configuring the Passive Interface
- Configuring Priority for DIS Election
- Configuring LSP Generation Interval
- Configuring Maximum Age of LSPs

- Configuring LSP Refresh Interval
- Configuring SPF Calculation Interval
- Configuring the Overload Bit
- Configuring Hostname Mappings
- Configuring the Authentication Methods
- Configuring the Interface Authentication

Basic Settings

To configure the IS-IS dynamic routing protocol, you need to enter the IS-IS routing configuring mode by executing the following commands:

ip vrouter *vrouter-name* – In the global configuration mode, enter the VRouter configuration mode.

router isis – Enter the IS-IS routing configuration mode and create the IS-IS process. The IS-IS processes in each VRouter are independent.

To close the IS-IS process, use **no router isis** command in the VRouter configuration mode.

Configuring the Router Type

The types include Level-1 router, Level-2 router, and Level-1-2 router. To configure the router type, use the following command in the IS-IS routing configuration mode:

is-type [**level-1** | **level-1-2** | **level-2-only**]

- **level-1** | **level-1-2** | **level-2-only** – Configure the type as Level-1 router (**level-1**) , Level-2 router (**level-2-only**), or Level-1-2 router (**level-1-2**). The default type is Level-1-2. Only when the type is Level-1-2, you are allowed to configure the interface type as Level-1 or Level-2.

To cancel the type settings, use the **no is-type** command in the IS-IS routing configuration mode.

Enabling IS-IS at Interfaces

By default, the IS-IS function is disabled at the interface. After creating an IS-IS process at the current router, proceed to enable the IS-IS function at the interface. Use the following command in the interface configuration mode:

isis enable

Use the **no isis enable** command to disable the IS-IS function at the interface.

Configure the Interface Type

When the router type is Level-1, the interface type can only be Level-1 and it can only establish the Level-1 adjacency. When the router type is Level-2, the interface type can only be Level-2 and it can only establish the Level-2 adjacency. When the router type is Level-1-2, the interface type can be Level-1 and Level-2. To configure the interface type, use the following command in the interface configuration mode:

isis circuit-type [**level-1** | **level-1-2** | **level-2-only**]

- **level-1** | **level-1-2** | **level-2-only** – Specify the interface type as Level-1 interface (**level-1**), Level-2 interface (**level-2-only**), or Level-1-2 interface (**level-1-2**).

Configuring the Network as Point-to-Point Type

If there are two devices in the broadcast network, you can configure the link that the interface locates as the point-to-point type. For point-to-point type link, IS-IS does not execute the DIS election and CSNP flooding. Use the following command in the interface configuration mode:

isis network point-to-point

Use the **no isis network point-to-point** command to cancel the above settings.

Routing Information Settings

Configuring the NET Address

NET (Network Entity Title) represents the network layer information of the IS, excluding the transmission layer information. The NET address is used to mark the device with the IS-IS process enabled. An IS-IS process can have at most three NET addresses and these NET addresses

must have the same System IDs. To specify the NET address for the device, use the following command in the IS-IS routing configuration mode:

net *net* [**local**]

- *net* – Specify the NET address for the device. When you use this device as level-1 router, it must have the same area ID with other devices in the same area. When you use this device as level-2 router, the process of establishing the adjacency will not check the area ID.
- **local** - Specifies NET address as a local configuration. This kind of configuration is applicable to HA Peer mode, and is not synchronized to HA configuration. By default theNET address is not a local configuration.

To cancel the NET address configurations, use the **no net** *net* command.

Configuring the Administrative Distance

To configure the administrative distance, use the following command in the IS-IS routing configuration mode:

distance *distance-value*

- *distance-value* – Specify the administrative distance. The value ranges from 1 to 255. The default value is 115.

To cancel the configurations, use the **no distance** command.

Configuring the Metric Style

If the metric style is Narrow, the router only generates and receives packets whose metric field is narrow. The metric value of the interface ranges from 0 to 63. For the large network environment, the maximum allowed metric of a route is 1023. When the metric value exceeds 1023, the destination is considered to be unreachable. If the metric style is Wide, the router only generates and receives packets whose metric field is wide. The metric value of the interface ranges from 0 to 16777215. If the metric style is transition, the router can generate and receive packets whose metric field is wide or narrow. To configure the metric style, use the following command in the IS-IS routing configuration mode:

metric-style {**wide** | **narrow** | **transition**}

- **wide** - The router only generates and receives packets whose metric field is Wide.
- **narrow** - The router only generates and receives packets whose metric field is Narrow.
- **transition** - The router can generate and receive packets whose metric field is Wide or Narrow.

To cancel the metric style configurations, use the **no metric-style** command.

Configuring the Interface Metric

The metric is used to calculate the cost to the destination network via the selected link. To configure the metric of the link, use the following command in the interface configuration mode:

isis metric *value* [**level-1** | **level-2**]

- *value* – Configure the metric value of the link that the interface locates. The value ranges from 1 to 16777214 and the default value is 10.
- **level-1** | **level-2** – Use **level-1** to configure the metric value for Level-1 routes. Use **level-2** to configure the metric value for Level-2 routes. Without specifying **level-1** or **level-2**, the metric value is effective for both Level-1 and Level-2 routes.

Use the **no isis metric** command to restore the metric value to the default one.

Configuring Redistribute

IS-IS allows you to introduce routing information from other routing protocols (connected, static, OSPF, BGP and RIP) and redistribute the information. To configure the redistribute and the corresponding metric, in the IS-IS routing configuration mode, use the following commands:

redistribute {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *value*] [**metric-type** {**external** | **internal**}]

- **connected** | **static** | **ospf** | **bgp** | **rip** - Specify the protocol type which can be **connected**, **static**, **OSPF**, **bgp**, or **rip**.

- **level-1 | level-1-2 | level-2** – Specify the level for the introduced route, including the level-1 route (**level-1**), level-2 route (**level-2**), and both levels (**level-1-2**).
- **metric** *value* - Specify a metric value for the introduced route. The value range is 0 to 4294967296. The default value is 0. When the metric type of the router is narrow, the metric value of the introduced route cannot exceed 63.
- **metric-type {external | internal}** – If you select the external metric type (**external**), the metric value will be the sum of the value configured in metric value and 64. If you select the internal metric type (**internal**), the metric value will be the one you configured in the metric value command. The default option is internal.

To cancel the redistribute configurations, use the **no redistribute {connected | static | ospf | bgp | rip} [level-1 | level-1-2 | level-2]** command.

Configuring the Default Route Advertisement

The default route in the introduced routing information will not be used by the routers. To advertise the default route in the routing domain, in the IS-IS routing configuration mode, use the following command:

default-information originate

If there is a default route in the router with the above command configured, the IS-IS process in this router will advertise this route via Level-2 LSPs.

To cancel the default route advertisement, use the **no default-information originate** command.

Network Optimization

Configuring the Interval for Sending Hello Packets

To configure the interval that the interface sends Hello packets, use the following command in the interface configuration mode:

isis hello-interval *value* **[level-1 | level-2]**

- *value* – Specify the interval that the interface sends Hello packets. The value ranges from 1 to 600. The unit is second. The default value is 3.
- **level-1** | **level-2** – Use **level-1** to configure the interval for sending Level-1 Hello packets. Use **level-2** to configure the interval for sending Level-2 Hello packets.

Use the **no isis hello-interval** command to restore the interval to the default value.

Configuring the Multiplier for Hello Packets

Within the hold time, if a router does not receive Hello packets form its neighbor, it considers the neighbor down and will re-calculate the routes. The hold time is to multiply the Hello multiplier and the Hello interval. To configure the Hello multiplier, use the following command in the interface configuration mode:

isis hello-multiplier *value* [**level-1** | **level-2**]

- *value* – Specify the multiplier for Hello packets. The value ranges from 2 to 100. The default value is 10.
- **level-1** | **level-2** – Use **level-1** to configure the multiplier for Level-1 Hello packets. Use **level-2** to configure the multiplier for Level-2 Hello packets. Without specifying **level-1** or **level-2**, the multiplier value is effective for both Level-1 and Level-2 Hello packets.

To restore the multiplier value to the default value, use the **no isis hello-multiplier** command.

Configuring Padding for Hello Packets

Use the padding function to pad the hello packets and make them as large as the MTU of the interface. To configure the padding function, use the following command in the interface configuration mode:

isis hello padding

To cancel the padding function, use the **no isis hello padding** command.

Configuring Priority for DIS Election

In the broadcast network, you can specify the DIS priority for the interface to influence the DIS election. In the DIS election, the router whose interface has higher DIS priority will be selected as the DIS. If interfaces have the same priority, the router whose interface has larger MAC address will be selected as the DIS. To configure the DIS priority for the interface, use the following command in the interface configuration mode:

isis priority *value* [**level-1** | **level-2**]

- *value* – Specify the DIS priority for this interface. The value ranges from 0 to 127. The default value is 64.
- **level-1** | **level-2** – Use **level-1** to specify the priority for the Level-1 interface. Use **level-2** to specify the priority for the Level-2 interface. Without specifying **level-1** or **level-2**, the priority is effective for both Level-1 and Level-2 interfaces.

Use the **no isis priority** [**level-1** | **level-2**] command to restore the priority of the specified interface level to the default one.

Configuring the Passive Interface

After configure an interface as a passive interface, this interface will not send and receive any IS-IS packets, and it will not establish adjacency with neighbors. But you can redistribute the connected routing information about this network to other interfaces via LSPs. To configure an interface as a passive interface, use the following command in the interface configuration mode:

isis passive

Use the **no isis passive** command to cancel the above settings.

Configuring LSP Generation Interval

When the network topology changes, the router will generate LSPs. To avoid the frequent generation of LSPs consuming a larger amount of router resources and bandwidth, you can configure the LSP generation interval. In the IS-IS routing configuration mode, use the following command to configure the LSP generation interval:

lsp-gen-interval *value* [**level-1** | **level-2**]

- *value* – Specify the LSP generation interval. The value ranges from 1 to 120. The default value is 30. The unit is second.
- **level-1 | level-2** – Enter **level-1** to specify the LSP generation interval for level-1 LSPs only, and enter **level-2** to specify the LSP generation interval for level-2 LSPs only. If you enter no parameter, the configured interval value will be used for both level-1 LSPs and level-2 LSPs.

To restore the value to the default one, use the **no lsp-gen-interval** command.

Configuring Maximum Age of LSPs

Each LSP has a maximum age. The LSP with an age of 0 will be deleted from the LSDB. To configure the maximum age of LSPs, in the IS-IS routing configuration mode, use the following command:

max-lsp-lifetime *value*

- *value* – Specify the maximum age of LSP. The value ranges from 350 to 65535. The default value is 1200. The unit is second.

To restore the value to the default one, use the **no max-lsp-lifetime** command.

Configuring LSP Refresh Interval

Since each LSP has a maximum age, the router must refresh the LSPs generated by itself. To configure the LSP refresh interval, in the IS-IS routing configuration mode, use the following command:

lsp-refresh-interval *value*

- *value* – Specify the LSP refresh interval. The value ranges from 1 to 65535. The default value is 900. The unit is second. Hillstone recommends that the refresh interval is 300s less than the maximum age, which ensures that the LSP refresh can reach the routes within the area before the arrival of the maximum age.

Use the **no lsp-refresh-interval** command to restore the value to the default one.

Configuring SPF Calculation Interval

If the LSDB changes, the router will re-calculate the SPF. To configure the SPF calculation interval, use the following command in the IS-IS routing configuration mode:

spf-interval *value* [**level-1** | **level-2**]

- *value* – Specify the SPF calculation interval. The value ranges from 1 to 120. The default value is 10. The unit is second.
- **level-1** | **level-2** – Enter **level-1** to specify the SPF calculation interval for level-1 SPFs only, and enter **level-2** to specify the SPF generation interval for level-2 SPFs only. If you enter no parameter, the configured interval value will be used for both level-1 SPFs and level-2 SPFs.

Use the **no spf-interval** command to restore the value to the default one.

Configuring the Overload Bit

The lack of resources can lead to the result that the LSDB is inaccurate or incomplete. The router whose resource is lack will add the overload bit in the LSPs. After other routers receive these LSPs, they will not use this router whose resource is lack to forward packets. If the packets whose destination address is the network that is connected to this router, the packets will still be forward to this router. To configure the overload bit for the router, use the following command in the IS-IS routing configuration mode:

set-overload-bit

To cancel the overload bit configuration, use the **no set-overload-bit** command.

Configuring Hostname Mappings

In the IS-IS routing domain, System ID, as part of the NET address, is used to identify the host or the router. Hostname mapping maps the System ID to the hostname. The router will maintain a mapping table which records the mapping settings between the System ID and the hostname. To configure the hostname mapping, use the following command in the IS-IS routing configuration mode:

hostname dynamic

To cancel the hostname mapping, use the **no hostname dynamic** command.

Authentication

Configuring the Authentication Methods

Configure the authentication methods for the LSP packets, CSNP packets, and PSNP packets. With the authentication configured, routers will authenticate the preceding packets when they receive them. But this will not affect the Hello packets for establishing neighbors. There are two authentication methods, clear text authentication and MD5 authentication. As the default option, the clear text authentication cannot secure the communication and the password is forwarded together with the packets. To configure the authentication method, use the following command in the IS-IS routing configuration mode:

authentication {**md5** | **text**} [**level-1** | **level-2**]

- **md5** | **text** – Use the MD5 authentication (**md5**) or the clear text authentication (**text**).
- **level-1** | **level-2** – Use **level-1** to configure the authentication method for the packets between Level-1 routers, which prevents Level-1 routers learning the routing information from the untrusted routers . The Level-1 routers in the same area must use the same authentication method and password. Use **level-2** to configure the authentication method for the packets between level-2 routers, whichi prevents Level-2 routers learning the routing information from the untrusted routers. The Level-2 routers in the same routing domain must use the same authentication method and password.

To cancel the authentication configurations, use the **no authentication mode** command in the IS-IS routing configuration mode.

After configuring the authentication methods, proceed to configure the passwords. To specify the password for the packet authentication between level-1 routers, use the following command in the IS-IS routing configuration mode:

area-password *word*

- *word* – Specify the password. You can specify at most 32 characters. To delete the password, use the no area-password command.

To delete the password, use the **no area-password** command.

To specify the password for the packet authentication between level-2 routers, use the following command in the IS-IS routing configuration mode:

domain-password *word*

- *word* – Specify the password. You can specify at most 32 characters.

To delete the password, use the **no domain-password** command.

Configuring the Interface Authentication

Interface authentication is used to verify the legality of its neighbors and avoid the adjacency establishment with illegal routers. After configuring interface authentication, the password will be encapsulated in the Hello packets. After the packets were verified, the routers can become neighbors. To become neighbors, two interfaces must use the same interface authentication method and password. To configure the interface authentication, use the following command in the interface configuration mode:

isis authentication {**md5** | **text**} [**level-1** | **level-2**]

- **md5** | **text** – Use the MD5 authentication (**md5**or the clear text authentication (**text**).
- **level-1** | **level-2** – Use **level-1** to configure the authentication method for the Hello packets between Level-1 routers. Use **level-2** to configure the authentication method for the Hello packets between level-2 routers.

To cancel the interface authentication, use the **no isis authentication** command.

After configuring the interface authentication method, proceed to specify the password for the authentication. Use the following command in the interface configuration mode:

isis password *word* [**level-1** | **level-2**]

- *word* – Specify the password. You can specify at most 32 characters.
- **level-1** | **level-2** – Use **level-1** to configure the password for the Hello packets between Level-1 routers. Use **level-2** to configure the password for the Hello packets between level-2 routers.

Use the **no isis password** command to cancel the specified password.

Viewing IS-IS Information

To show the IS-IS process and corresponding information, use the following command in any mode:

show isis [**vrouter** *vrouter-name*]

- *vrouter-name* – Show the information of the specified vrouter.

To show the link state database, use the following command in any mode:

show isis database [**detail**] [**vrouter** *vrouter-name*]

- **detail** – Show the detailed information.
- *vrouter-name* – Show the information of the specified vrouter.

To show the IS-IS interface information, use the following command in any mode:

show isis interface [*interface-name*]

To show the IS-IS neighbor information, use the following command in any mode:

show isis neighbor [**detail**] [**vrouter** *vrouter-name*]

To show the dynamic host information, use the following command in any mode:

show isis hostname [**vrouter** *vrouter-name*]

To show the IS-IS routing information, use the following command in any mode:

show isis route [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

To show the routing redistribute information, use the following command in any mode:

show isis route redistribute [**level-1** | **level-2**] [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

Configuring BGP

BGP, the abbreviation for Border Gateway Protocol, is a routing protocol that is used to exchange dynamic routing information among the autonomous systems (An autonomous system is the router and network group under the control of a management institution. All the routers in the autonomous system must run the same routing protocol). It is also the protocol used between ISPs. BGP runs over port TCP 179, and supports Classless Inter-Domain Routing (CIDR). BGP

operates in two ways: when running between the autonomous systems, it is known as EBGP; when running within the autonomous system, it is know as IBGP. BGP has the following characteristics:

- After the initial TCP connection has been established, BGP neighbors exchange the entire BGP routing tables, then they only exchange the updated routing information.
- Periodically sending KEEPALIVE packets to check TCP connectivity.
- BGP routers only advertise the shortest path to the neighbors.
- BGP is a distance vector routing protocol that is designed to avoid the routing loop.

The router that sends BGP messages is known as a BGP speaker. The BGP speaker will receive or generate new routing information, and advertise to other speakers. When a speaker receives a new route from another autonomous system, if the route is shorter than all the known routes, or there is no known route at all, the speaker will advertise the route to all the other speakers. The BGP speaker that is exchanging information is knows as a peer to its counterpart, and multiple associated peers can constitute a peer group. The purpose of the peer group is to simplify the configuration. It does not affect the establishment of the actual peer relationship or the advertisement of routes.

There are four types of BGP packets: OPEN, UPDATE, NOTIFICATION, and KEEPALIVE. BGP peers send OPEN packets to exchange their versions, autonomous system numbers, hold-down time, BGP identifiers and other information, and negotiate with each other. The OPEN packet is mainly used to establish neighbor (BGP Peer) relationship. It is the initial handshake message between BGP routers, and should be sent before advertising any message. When a peer receives an OPEN message, it will respond with a KEEPALIVE message. Once the handshake has been completed successfully, these BGP neighbors will be able to exchange UPDATE, KEEPALIVE, NOTIFICATION and other messages. The UPDATE packet carries the routing update information, including the revoked routes, reachable routes and the reachable routes' paths. When detecting any error (connection interruption, negotiation error, packet error, etc.), BGP will send a NOTIFICATION packet, and drop the connection to the peer. The KEEPALIVE packets are transmitted between BGP peers periodically, in order to ensure connectivity.

Configuring BGP Protocol

You can configure the BGP protocol for different VRouters respectively. The BGP protocol configuration includes:

- Entering the BGP configuration mode
- Specifying a Router ID
- Creating a route aggregation
- Adding a static BGP route
- Configuring a timer
- Specifying the administration distance of BGP route
- Specifying the default metric
- Configuring redistribute
- Creating a BGP peer group
- Adding a BGP peer to the peer group
- Configuring a BGP peer
- Activating a BGP connection
- Configuring the default information originate
- Configuring description
- Configuring a BGP peer timer
- Configuring the next hop as itself
- Configuring EBGP multihop
- Disabling a peer or peer group

- Resetting a BGP connection
- Redistributing routes into BGP
- Configuring route filters based on the AS-path access list
- Sending communities path attributes to peers or peer groups
- Configuring route filters based on the route map
- Configuring equal cost multipath routing
- Enabling/Disabling multipath-relax of EBGP
- Configuring BGP GR

Entering the BGP Configuration Mode

The BGP protocol options must be configured in the BGP routing mode. To enter the BGP routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

router bgp *number*

- *number* - Specifies the number of the autonomous system. The value range is 1 to 4,294,967,295.

The above command will enable the BGP function on the system, create a BGP instance for the specified autonomous system, and switch to the BGP instance configuration mode.

To delete the specified BGP instance, in the VRouter configuration mode, use the command **no router bgp** *number*.

Specifying a Router ID

Each router running BGP protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole BGP domain, represented in the form of an IP address. If the Router ID is not specified, the system will set the largest IP address of the loopback interface on the device as the Router ID; if there is no loopback interface or the IP address of the loopback interface is not configured, the system will select the largest IP address of other

interfaces as the Router ID. To specify the Router ID, in the BGP instance configuration mode, use the following command:

router-id *A.B.C.D*

- *A.B.C.D* - Specifies the Router ID used by BGP protocol, in form of an IP address.

To cancel the specified Router ID, in the BGP instance configuration mode, use the following command:

no router-id

Creating a Route Aggregation

You can aggregate the routing entries in the BGP routing table. To create a route aggregation, in the BGP instance configuration mode, use the following command:

aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**as-set**] [**summary-only**]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the network address for the aggregation. Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D,* for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **as-set**- If this parameter is specified, the system will advertise the aggregated path information to other routers as its own path information.
- **summary-only** - If this parameter is specified, the system will only advertise the aggregated route.

To cancel the specified route aggregation, in the BGP instance configuration mode, use the following command:

no aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D}*

Adding a Static BGP Route

To add a static BGP route, in the BGP instance configuration mode, use the following command:

network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

- *A.B.C.D/M | A.B.C.D A.B.C.D* - Specifies the static BGP routing entry. Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.

To delete the specified static routing entry, in the BGP instance configuration mode, use the following command:

no network {*A.B.C.D/M | A.B.C.D A.B.C.D*}

Configuring a Timer

You can configure two BGP timers which are KEEPALIVE and HOLDDOWN, as described below:

- KEEPALIVE: The interval of sending the KEEPALIVE message to the BGP peer. By default StoneOS sends the message every 60 seconds.
- HOLDDOWN: If the local router still has not received the KEEPALIVE message from any peer after the HOLDDOWN time, then it will determine the peer is not active any more. The default value is 180 seconds.

To configure a timer, in the BGP instance configuration mode, use the following command:

timers *keepalive holddown*

- *keepalive* - Specifies the interval for sending the KEEPALIVE message. The value range is 0 to 65535 seconds, but should not be larger than HOLDDOWN/3. The default value is 60. If the value is larger than HOLDDOWN/3, the actual effective time will be HOLDDOWN/3. The value 0 indicates never sending the KEEPALIVE message.
- *holddown* - Specifies the HOLDDOWN time. The value range is 0 to 65535 seconds or 3 to 65535 seconds. The default value is 180. The value 0 indicates never checking the HOLDDOWN time.

To restore to the default timer value, in the BGP instance configuration mode, use the following command:

no timers

Specifying the Administration distance of BGP Route

You can specify the administration distance for the local BGP routes or the BGP routes acquired from other peers. To specify the administration distance for a BGP route, in the BGP instance configuration mode, use the following command:

distance *ebgp-distance ibgp-distance local-distance*

- *ebgp-distance* - Specifies the administration distance for the EBGP route. The value range is 1 to 255. The default value is 20.
- *ibgp-distance* - Specifies the administration distance for the IBGP route. The value range is 1 to 255. The default value is 200.
- *local-distance* - Specifies the administration distance for the local route. The value range is 1 to 255. The default value is 200.

To restore to the default administration distance for a BGP route, in the BGP instance configuration mode, use the following command:

no distance

Specifying the Default Metric

By default, the metric of the redistributed IGP route remains unchanged, and the metric of the redistributed connected route is 0. To specify the default metric of the redistributed routing, in the BGP instance configuration mode, use the following command:

default-metric *value*

- *value* - Specifies the default metric value. The value range is 1 to 4294967295. To restore to the default metric value, in the BGP instance configuration mode, use the following command:

To restore to the default metric value, in the BGP instance configuration mode, use the following command:

no default-metric

Creating a BGP Peer Group

The BGP peer group is designed to simplify the configuration, and update the information in a more effective way. To create a BGP peer group, in the BGP instance configuration mode, use the following command:

neighbor *peer-group-name* **peer-group**

- *peer-group-name* - Specifies a name for the new peer group.

To delete the specified BGP peer group, in the BGP instance configuration mode, use the following command:

no neighbor *peer-group-name* **peer-group**

Adding a BGP Peer-to-peer Group

To add a BGP peer-to-peer group, in the BGP instance configuration mode, use the following command:

neighbor *A.B.C.D* **peer-group** *peer-group-name*

- *A.B.C.D* - Specifies the IP address of the BGP peer that will be added.
- *peer-group-name* - Specifies the peer group that has been created in the system.

To delete the specified BGP peer from the BGP peer group, in the BGP instance configuration mode, use the following command:

no neighbor *A.B.C.D* **peer-group** *peer-group-name*

Configuring a BGP Peer

To exchange BGP routing information, you need to specify a BGP peer (peer group) for the device. To configure a BGP peer, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **remote-as** *number*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *number* - Specifies the number of autonomous system the configured peer or peer group belongs to.

To cancel the specified BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **remote-as**

Configuring BGP MD5 Authentication

To improve BGP security, you can configure MD5 authentication for the BGP peer or peer group. With this function enabled, the two ends of a peer will have to pass the MD5 authenticatoin in order to establish a TCP connection. To configure BGP MD5 authentication, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **password** *password*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of peer group.
- **password** *password* - Specifies the MD5 password string. The value range is 1 to 32 characters.

To cancel the BGP MD5 authentication,in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **password**



Notes: The MD5 password configured on the peers or peer groups must be consistent.

Activating a BGP Connection

By default, the BGP connection between the configured BGP peer or peer group and the device is activated. You can de-activate or re-activate the BGP connection. To activate the BGP connection, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **activate**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To de-activate the BGP connection to the specified BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **activate**

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other BGP peers or peer groups. By default BGP will not redistribute the default route.

To configure the default information originate, in the BGP instance configuration mode, use the following command:

default-information originate

If there is no default route in the routing table,the system will not redistribute default route any more.

To cancel the default information originate, in the BGP instance configuration mode, use the following command:

no default-information originate

To configure the default information originate, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **default-originate**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

If there is no default route in the routing table,the system will construct a default route to redistribute.

To cancel the default information originate, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **default-originate**

Configuring Description

To configure description for a peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **description** *description*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *description* - Specifies the description. The length is 1 to 80 characters.

To cancel the description of the specified peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **description**

Configuring a BGP Peer Timer

By default, the timer of BGP peers or peer groups in the whole BGP system is set to the value specified by timer keepalive holddown. You can specify a different timer value for a specific BGP peer or peer group. The priority of the specified value is higher than that of the value specified by timer keepalive holddown. To specify a timer value for a BGP peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **timers** *keepalive holddown*

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.
- *keepalive* - Specifies the interval for sending the KEEPALIVE message. The value range is 0 to 65535 seconds, but should not be larger than HOLDDOWN/3. The default value is 60. If the value is larger than HOLDDOWN/3, the actual effective time will be HOLDDOWN/3. The value 0 indicates never sending the KEEPALIVE message.
- *holddown* - Specifies the HOLDDOWN time. The value range is 0 to 65535 or 3 to 65535 seconds. The default value is 180. The value 0 indicates never checking the HOLDDOWN time.

To cancel the specified timer for the BGP peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **timers**

Configuring the Next Hop as Itself

With this function configured, the router will advertise the next hop of the BGP route for the BGP peer or peer group is the router itself. To configure the next hop as itself, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To cancel next hop as itself, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

Configuring EBGP Multihop

For BGP running between different AS (i.e., EBGP), if the BGP peers or peer groups are not directly connected, you need to configure EBGP multihop in order to establish neighbor between devices. To configure EBGP multihop, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **ebgp-multihop** [*ttl*]

- *A.B.C.D* | *peer-group* - Specifies the peer IP address or the name of peer group.
- *ttl*- Specifies the count of maximum hops to the peer IP address or peer group. The value range is 1 to 255, and the default value is 255. If no peer or peer group can be found after the maximum hops, the system will conclude neighbor cannot be established.

To cancel EBGP multihop, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **ebgp-multihop**

Disabling a Peer/Peer Group

If a peer or peer group is disabled, all the sessions to the peer or peer group will be dropped, and all the relevant routing information will be deleted. To disable a peer or peer group, in the BGP instance configuration mode, use the following command:

neighbor {*A.B.C.D* | *peer-group*} **shutdown**

- *A.B.C.D* | *peer-group* - Specifies the IP address of the peer or the name of the peer group.

To re-enable the specified peer or peer group, in the BGP instance configuration mode, use the following command:

no neighbor {*A.B.C.D* | *peer-group*} **shutdown**

Resetting a BGP Connection

To reset a BGP connection, in the execution mode, use the following command:

clear ip bgp {* | *A.B.C.D* | **external** | **peer-group** *peer-group-name* | *number*} [**vrouter** *vrouter-name*]

- * - Resets all the existing BGP connections.
- *A.B.C.D* - Resets BGP connections to the specified peer.
- **external** - Resets all the existing EBGP connections.
- **peer-group** *peer-group-name* Resets BGP connections to the specified peer group.
- *number* - Resets BGP connections in the specified autonomous system.
- **vrouter** *vrouter-name* - Specifies the VRouter where the reset operation is performed.

Redistributing Routes into BGP

The BGP supports the function that redistributes routes of other protocols into BGP and advertises the routing information. Besides, you can set the metric of the redistributed route and use the route map to filter the routing information. To redistribute routes into BGP, use the following command in the BGP instance configuration mode:

redistribute {**ospf** | **isis** | **connected** | **static** | **rip**} [**metric** *value*] [**route-map** *name*]

- **ospf** | **isis** | **connected** | **static** | **rip** - Specifies the protocol type which can be **ospf**, **isis**, **connected**, **static** or **rip**.

- **metric** *value* Specifies a metric value for the redistributed route. The value range is 0 to 4294967295. If the value is not specified, the system will use the default BGP metric configured by the **default-metric** *value* command.
- **route-map** *name* - Specifies the route map that is used to filter the routing information introduced from other routing protocols. For more information about route map, see Configuring a Route Map.

You can use the command above to redistribute route of different types.。

To cancel the redistributed route, use the following command: **no redistribute** {**ospf** | **isis** | **connected** | **static** | **rip**}.

Displaying Communities Attribute in the AA:NN Format

BGP communities attribute can be displayed in the AA:NN format (RFC 1997, BGP Comunities Attribute). When you use the show command to view the BGP communities attribute, the custom communities attribute is disaplyed in the AA:NN format. To view the communities attribute in the AA:NN format, in global configuration mode, use the following command:

ip bgp-community new-format

To cancel displaying the communities attribute in the AA:NN format, use the following command:

no ip bgp-community new-format



Notes: After this command is executed, if you use the **show configuration** command to view the result, the custom communities attribute is displayed in the decimal format; if you use the **show route-map**, **show ip community-list**, and **show ip bgp** [*A.B.C.D*] commands to view the result, the custom communties attribute is displayed in the AA:NN format.

Configuring Route Filters Based on the AS-path Access List

BGP uses the AS-path access list to filter the route introduced by the peers or peer groups or the route advertised. To configure the route filter function based on the AS-path access list, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **filter-list** *access-list-number* {**in** | **out**}

- *A.B.C.D* | *peer-group* – Specifies the IP address or the name of the BGP peer.
- *access-list-number* – Specifies number of the AS-path access list. For more information about AS-path access list, see Configuring an AS-path Access List.
- **in** | **out** – Use **in** to filter the introduced routes or use **out** to filter the advertised routes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **filter-list** {**in** |**out**}

Sending Communities Path Attributes to Peers or Peer Groups

To send communities path attributes to peers or peer groups, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **send-community** {**standard** | **extended** | **both**}

- *A.B.C.D* | *peer-group* - Specifies the IP address of the BGP peer or the name of the peer group.
- **standard** | **extended** | **both** – Specifies the type of the communities path attributes. There are three types: **standard** means the standard communities path attributes, **extended** means the extended communities path attributes, and **both** means both of the communities path attributes and extended communities path attributes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **send-community**

Configuring Route Filters Based on the Route Map

BGP uses the route map to filter the route introduced by the peers or peer groups or the route advertised. To configure the route filter function based on the route map, use the following command in the BGP instance configuration mode:

neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

- *A.B.C.D* | *peer-group* – Specifies the IP address of the BGP peer or the name of the peer group.
- **in** | **out** – Use **in** to filter the introduced routes or use **out** to filter the advertised routes.

Use the following command to cancel the above configurations:

no neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

Configuring Equal Cost Multipath Routing

To configure the maximum number of equal cost multipath (ECMP) routes for BGP, use the following command in the BGP instance configuration mode:

maximum-paths {**ebgp** | **ibgp**} *maximum-number*

- *maximum-number* – Specifies the maximum number of ECMP routes for IBGP/EBGP. When there are eligible ECMP paths, they will be added to the routing table according to the maximum number you specified. With these configurations, ECMP assists with load-balancing of BGP on multiple routes. The range is 1 to 8 and the default value is 1.

Use the following command in the BGP instance configuration mode to cancel the above settings:

no maximum-paths {**ebgp** | **ibgp**}



Notes: Before configuring this ECMP routing, you must first enable the ECMP function. For more information, see ECMP.

Viewing BGP Information

To view the BGP routing information , in any mode, use the following command:

show ip route bgp [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BGP routing information of the specified vRouter.

To view the routing information of the entire BGP routing table, in any mode, use the following command:

show ip bgp [*A.B.C.D* | *A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D* | *A.B.C.D/M* - Shows the BGP routing information of the specified network.
- *vrouter-name* - Shows the BGP routing information of the specified VRouter.

To view the path information of all the autonomous systems stored in the BGP database, in any mode, use the following command:

show ip bgp paths [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the paths information of autonomous systemof the specified VRouter.

To view the status parameters of all BGP connections, including the prefix, path, attribute, etc., in any mode, use the following command:

show ip bgp summary [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BGP connecting status parameters of the specified VRouter.

To view the BGP peer status, in any mode, use the following command:

show ip bgp neighbor [*A.B.C.D*] [**vrouter** *vrouter-name*]

- *A.B.C.D* - Specifies the peer.
- *vrouter-name* - Shows the BGP peer status of the specified VRouter.

To view the BGP community list, use the following commands in any mode:

show ip community [*community-list-name*]

- *community-list-name* – Shows the information of the specified community list. Without this parameter specified, the information of all community lists will be displayed.

show ip as-path-access-list [*access-list-number*]

- *access-list-number* – Shows the information of the specified AS-path access list. Without this parameter specified, the information of all AS-path access lists will be displayed.

Enabling/Disabling multipath-relax of EBGP

For EBGP to the same destination network through different AS paths, system supports enabling multipath-relax of EBGP function, so that EBGP can achieve load balancing on different AS

paths. In the BGP instance configuration mode,, use the following command:

- Enable: **bestpath as-path multipath-relax**
- Disable: **no bestpath as-path multipath-relax**

Configuring BGP GR

GR (Graceful Restart) is also called Non-Stop Forwarding (NSF).

The BGP GR ensures that the forwarding layer can continue to forward data during the switchover between backup and primary devices or device restart. Meanwhile, the operation of the forwarding layer is not affected by the re-establishment of neighbor relations and the routing computation of the control layer. In this scenario, BGP GR can help the system have less single point of failure, and reduce the influence of route flapping on the network during the switchover between backup and primary devices. Therefore, the network is more reliable and can avoid the influence of traffic interruption on users' important services.

Basic Concepts of BGP GR

- End-of-RIB marker: End-of RIB marker is a BGP Update message with no reachable Network Layer Reachability Information (NLRI) and its withdrawn NLRI is empty. When the current device receives the End-of-RIB marker from its peer, it indicates that this peer has sent all updates needing to be notified.
- Graceful Restart Capability: Graceful Restart Capability is a new BGP capability to better support GR functionality. It is advertised by the BGP with the Open message when a BGP connection is established. Graceful Restart Capability can indicate that the current device can preserve its forwarding state during BGP restart, and generate the End-of-RIB marker upon the completion of its initial updates.
- GR Restarter: GR Restarter is the device applying Graceful Restart during BGP restart or the switchover between backup and primary devices.
- GR Helper: GR Helper is the neighbor of GR Restarter, and is the device with GR Capability to assist GR Restarter in the Graceful Restart.

A device can be a GR Restarter or a GR Helper. Whether to become a GR Restarter or a GR Helper is determined according to the actual role the device plays in the procedures of BGP GR.

Take device HA as an example. The working procedures of BGP GR are as follows:

1. In device HA, the new primary device works as the GR Restarter and re-establishes the BGP connection with the GR Helper.
2. The GR Helper disconnects its BGP neighborhood with the previous primary device and marks the BGP routes learned from the previous primary device as stale. But the GR Helper still forwards data messages via these routes and enables the Graceful-Restart Stale-Path-Time. To configure the Graceful-Restart Stale-Path-Time, use the **graceful-restart stale-path-time** *time* command.
3. If the GR Restarter successfully establishes the BGP session with the GR Helper within the notified Graceful-Restart Restart-Time, they become neighbors and will exchange routing information. If the GR Restarter cannot establish a BGP neighborhood with the GR Helper within the notified Graceful-Restart Restart-Time, the GR Helper will delete routes related to the GR Starter immediately. To configure Graceful-Restart Restart-Time, use the **graceful-restart restart-time** *time* command.
4. GR Helper sends updates after becoming a neighbor of the GR Restarter and generates an End-of-RIB marker upon the completion of the updates. Even if the GR Helper does not have updates to be notified, it is required to send the End-of-RIB marker.
5. GR Restarter starts to select the optimum path after receiving the End-of-RIB markers from its peers. If GR Restarter does not receive all the necessary End-of-RIB markers, it will start to select the optimum path after the configured Graceful-Restart Wait-For-Rib-Time expires. To configure the Graceful-Restart Wait-For-Rib-Time, use the **graceful-restart wait-for-rib-time** *time* command.

6. After the selection of the optimum path, GR Restarter updates the RIB, then generates updates of the BGP route and sends the updates to its BGP neighbors. Whether there are updates or not, GR Restarter should notify the End-of-RIB marker.

7. After receiving the route updates, GR Helper removes the stale markers of relative routes. GR Helper will remove routes still with stale markers after receiving the End-of-RIB marker sent by the GR Restarter.

8. If routing information exchange is not completed within the Graceful-Restart Stale-Path-Time, GR Restarter is forced to quit GR and then GR Restarter updates RIB according to the learned BGP route information and deletes invalid RIB.



Notes:

- BGP GR cannot be applied in HA peer mode.
- Only when devices in the below scenarios can they work as the GR Restarter. Otherwise, they work as the GR Helper.
  - The newly elected primary device after HA switching;
  - Devices with SCM HA function (All platforms of X series, and K9180).
- BGP GR does not work if HA between primary and backup devices disconnects.

Enabling BGP GR

To enable the BGP GR functionality, in the BGP instance configuration mode, use the following command:

graceful-restart

To disabling the BGP GR functionality, in the BGP instance configuration mode, use the command **no graceful-restart**.

Configuring GR Restart-Time

To configure the longest time for a peer to wait for a BGP session to be re-established, in the BGP instance configuration mode, use the following command:

graceful-restart restart-time *time*

- *time* - Specifies the longest time for a peer to wait for a BGP session to be re-established. The time range from 1 to 3600 seconds. The default Graceful-Restart Restart-Time is 120 seconds.

To restore to the default value, in the BGP instance configuration mode, use the command**no graceful-restart restart-time**.

Configuring GR Stale-Path-Time

To configure the longest time to retain the stale routes of the restarted peers, in the BGP instance configuration mode, use the following command:

graceful-restart stale-path-time *time*

- *time* - Specifies the longest time to retain the stale routes of the restarted peers. The time range from 1 to 3600 seconds. The default Graceful-Restart Stale-Path-Time is 360 seconds.

To restore to the default value, in the BGP instance configuration mode, use the command **no graceful-restart stale-path-time**.

Configuring GR Wait-For-Rib-Time

To configure the longest time for the GR Restarter to wait for the End-of-RIB markers from the neighbors, in the BGP instance configuration mode, use the following command:

graceful-restart wait-for-rib-time *time*

- *time* - Specifies the longest time for the GR Restarter to wait for the End-of-RIB markers from the neighbors. The time range from 1 to 3600 seconds. The default Graceful-Restart Wait-For-Rib-Time is 180 seconds.

To restore to the default value, in the BGP instance configuration mode, use the command **no graceful-restart wait-for-rib-time**.

Route Object

The following route objects are provided:

- "Route Map" on Page 541
- "Access List Route" on Page 549
- "AS Path Access List" on Page 553
- "Community List" on Page 554

Route Map

The OSPF protocol, OSPFv3 protocol, BGP protocol, and IPv6 BGP protocol allow you to import routing information from other routing protocols and advertise the information. By default, the system imports all the routing information. You can filter the routing information imported from other routing protocols by referencing a route map. The route map mainly consists of two parts: matching rules and actions (permit or deny) for the matched routing information. If imported routing information hits any matching rule, the system will take the configuration action, i.e., permit or deny the imported routing information.



Notes:

- If the action is set to Permit, the system will only permit the matched routing information and deny all the unmatched routing information.
- If the action is set to Deny, the system will deny the matched routing information, but still permit all the unmatched routing information.

To configure a route map and filter the imported routing information, take the following steps:

1. Create a route map and add matching rules to the route map. Matching rules are differentiated by IDs. The smaller the ID is, the higher the matching priority will be. By default if the routing information hits any matching rule, the system will not continue to

match the subsequent rules; if no matching rule is hit, the system will take the Deny action.

2. Add matching conditions to the matching rules. The matching condition can be the AS path, community, next-hop interface, destination address, next-hop IP address, metric, or tag of the imported routing information. The matching conditions that can be configured vary based on imported routing protocols. One matching rule may contain multiple matching conditions, and the relation between these conditions is AND, i.e., in order to hit a matching rule, the routing information needs to meet all the matching conditions in the rule.

Match Condition	Support of different imported routing protocols for match conditions			
	OSPF	OSPFv3	BGP	IPv6 BGP
AS Path	x	x	Yes	Yes
Community List	x	x	Yes	Yes
Next Hop Interface	Yes	Yes	x	x
IPv4 Destination Address	Yes	x	Yes	x
IPv6 Destination Address	x	Yes	x	Yes
IPv4 Next Hop	Yes	x	Yes	x
IPv6 Next Hop	x	x	x	Yes
Metric	Yes	x	Yes	Yes
Tag	Yes	x	Yes	x

Note: "x" indicates that the match condition is not supported.

3. If the match condition is the destination address or next-hop IP address, also configure a route access-list that will be referenced. For more information about route access-list, see "Access List Route" on Page 549.

4. If needed, require the system to continue to match another rule after the routing information hits a matching rule.

5. If needed, modify partial attributes of the imported routing information before redistribution. The routing attributes that can be modified vary based on imported routing protocols.

Routing Attribute	Support of different routing protocols for modifying routing attributes			
	OSPF	OSPFv3	BGP	IPv6 BGP
AS Path	x	x	Yes	Yes
Community List	x	x	Yes	Yes
Community	x	x	Yes	Yes
Next Hop Interface	x	x	x	x
IPv4 Destination Address	x	x	x	x
IPv6 Destination Address	x	x	x	x
IPv4 Next Hop	x	x	Yes	x
IPv6 Next Hop	x	x	x	Yes
Metric	Yes	Yes	Yes	Yes
Metric Type	Yes	Yes	x	x
Origin	x	x	Yes	Yes
Tag	Yes	x	x	x
Local Preference	x	x	Yes	Yes

Note: "x" indicates that the routing attribute is not supported.

Configuring a Route Map

This topic consists of the following sections:

- Configuring a Route Map and Adding a Matching Rule
- Adding a Matching Condition
- Continuing to Match Another Matching Rule
- Modifying Attributes of Introduced Routing Information

Configuring a Route Map and Adding a Matching Rule

To create a route map and add a matching rule to the route map, in the global configuration mode, use the following command:

route-map*name* {**deny** | **permit**} *sequence*

- **route-map***name* - Specifies the name of the route map, and enters the route map configuration mode. The value range is 1 to 31 characters. If the name already exists in the system, you will directly enter the route map configuration mode.
- **deny** | **permit** - Specifies the action for the matched routing information.
- *sequence* - Specifies the sequence number for the matching rule in the route map. The value range is 1 to 65535.

To delete the specified route map, in the global configuration mode, use the following command:

no route-map*name* [*sequence*]

- *sequence* - Only deletes the specified matching rule from the route map.

Adding a Matching Condition

To add a matching condition to the matching rule, in the route map configuration mode, use the following command:

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [*exact-match*] | **interface** *interface-name* | **ip address** *access-list* | **ipv6 address** *access-list* | **ip next-hop** *access-list* | **ipv6 next-hop** *access-list* | **metric** *metric-value* | **tag** *tag-value* }

- **as-path***access-list-number* – Matches the AS path of the introduced routing information. *access-list-number* is the number of the AS-path access list configured by yourself. If the AS path of the route matches the AS path that is permitted in this AS-path access list, the system concludes that the matching is successful. For more information about configuring an AS-path access list, see Configuring an AS-path Access List.
- **community** {*community-list-name* | *community-list-number*} [*exact-match*] - Matches the communities path attributes of the introduced routing information. *community-list-name* is the name of the community list. *community-list-name* is the number of the community list. *exact-match* indicates that the system will execute the exact matching. For more information about configuring community list, see Configuring BGP Communities.
- **interface** *interface-name* - Specifies to match the next-hop interface of the introduced routing information.
- **ip address** *access-list* - Specifies to match the IPv4 destination address of the introduced routing information. *access-list* is the route access-list configured in the system. If the destination address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.
- **ipv6 address** *access-list* - Specifies to match the IPv6 destination address of the introduced routing information. *access-list* is the route access-list configured in the system. If the destination address of the routing information is the permitted address in the route access-list,

the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.

- **ip next-hop** *access-list* - Specifies to match the next-hop IPv4 address of the introduced routing information. *access-list* is the route access-list configured in the system. If the next-hop IP address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.
- **ipv6 address** *access-list* - Specifies to match the next-hop IPv6 address of the introduced routing information. *access-list* is the route access-list configured in the system. If the next-hop IP address of the routing information is the permitted address in the route access-list, the system will conclude the matching succeeds. For more information about route access-list, see Configuring a Route Access-list.
- **metric** *metric-value* - Specifies to match the metric of the introduced routing information. The value range is 0 to 4294967295.
- **tag** *tag-value* - Matches the route tag value of OSPF protocol. If the configured tag value of the route here matches the tag value in the static route, the match is considered successful. The value range is 1 to 4294967295.

Repeat the above command to add more matching conditions to the matching rule. To delete the specified matching condition from the matching rule, in the route map configuration mode, use the following command:

no match {**as-path** | **community** | **interface** | **ip address** | **ipv6 address** | **ip next-hop** | **ipv6 next-hop** | **metric** | **tag**}

Notes: If you only created a route map but did not add any matching rule, by default the system will conclude all the introduced routing information is matched.

For example, the following commands will only allow OSPF to redistribute the routing information from BGP with the next-hop interface set to eth0/1 and metric set to 50:

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Continuing to Match Another Matching Rule

By default if the introduced routing information hits any matching rule, the system will not continue to match any other matching rules. For fine-grained control, you can require the system to continue to match another matching rule even after hitting a matching rule. To continue to match another matching rule, in the route map configuration mode, use the following command:

continue [*sequence*]

- *sequence* – Specifies the sequence number for the matching rule that will be continued. The value range is 1 to 65535. This sequence number must be larger than the sequence number of the current matching rule. If this parameter is not specified, the system will continue to match the next rule after hitting the current rule.

To cancel the above configuration, in the route map configuration mode, use the following command:

no continue

For example, the following commands will also only allow OSPF to redistribute the routing information from BGP with the next-hop interface set to eth0/1 and metric set to 50:

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
```

```
hostname(config-route-map)# continue 20
hostname(config-route-map)# exit
hostname(config)# route-map test permit 20
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Modifying Attributes of Introduced Routing Information

For the introduced routing information, you can modify partial attributes before redistribution. To modify the attribute of the introduced routing information, in the route map configuration mode, use the following command:

set {**as-path prepend** *as-number* | **commu-list** {*community-list-name* | *community-list-number*} **delete** | **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] | **ip next-hop** *A.B.C.D* | **ipv6 next-hop** *X:X:X:X::X* | **metric** *metric-value* | **metric-type** {**type-1** | **type-2**} | **origin** {**egp** | **igp** | **incomplete**} | **tag** *tag-value* | **local-preference** *value*}

- **as-path prepend** *as-number* - Add a new AS path after the existing AS path of the introduced route. The rang is 1 to 65535 and you can use spaces to separate multiple values.
- **commu-list** {*community-list-name* | *community-list-number*} **delete** - Uses *community-list-name* to specifies the name of the community list or use *community-list-number* to specify the number of the community list. Delete the matched communities path attribute.
- **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] - Modifies the communities path attributes of the introduced route. You can specify

multiple communities path attributes at the same time and use spaces to separate multiple values. The range of *community-number* is 1 to 4294967295.

- **ip next-hop** *A.B.C.D* - Modifies the next-hop IPv4 address of the introduced route.
- **ipv6 next-hop** *X:X:X:X::X* - Modifies the next-hop IPv6 address of the introduced route.
- **metric** *metric-value* - Modifies the metric of the introduced routing information. The value range is 0 to 4294967295.
- **metric-type** {**type-1** | **type-2**} - Modifies the metric type of the external route. type-1 indicates type1 external route metric, and type-2 indicates type2 external route metric.
- **origin** {**igp** | **egp** | **incomplete**} - Modifies the source attribute of the introduced route. *igp* means the route comes from internal AS; *egp* means the route is obtained from EGP. *incomplete* means the route is obtained by other methods.
- **tag** *tag-value* - Specifies the tag value of the introduced route. The value range is 1 to 4294967295.
- **local-preference** *value* - Modifies the attribute of the local preference of the route. The range is 0 to 4294967295.

To cancel the modification and restore to the settings when the routing information was introduced, use the following command:

no set {**as-path prepend** | **commu-list** | **community** | **ip next-hop** | **ipv6 next-hop** | **metric** | **metric-type** | **origin** | **tag** | **local-preference**}

Access List Route

The matching of destination address and next-hop address in route matching rules is achieved by referencing the access list route. The access list route consists of two parts: IP address matching rule and the corresponding operation (allow or deny) to be performed upon successful match. If the destination address or next-hop address matches the specified IP address, the system proceeds to execute the specified action. An access list route can contain multiple IP address matching

rules. The system matches the rules in the order of the time when they were added. Once a rule is hit, the matching process immediately ends. If the matching fails, the system performs the deny operation.

Configuring a Route Access List

This topic consists of the following sections:

- Configuring an IPv4 Route Access List
- Configuring an IPv6 Route Access List

Configuring an IPv4 Route Access List

To configure an IPv4 route access-list, in the global configuration mode, use the following command:

access-list route *name* [{**deny** | **permit**} {{*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**exact-match**] | **any**}]

- *name* - Specifies the name of the route access-list and enters the configuration mode of the route access-list. The value range is 1 to 31 characters. If the name already exists, you will be directly redirected to the configuration mode of the route access-list.
- **deny** | **permit** - Specifies the action for the matched IPv4 address.
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* - Specifies the IPv4 address to be matched. The following two formats are supported: A.B.C.D/M or A.B.C.D A.B.C.D. Example: 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **exact-match** - Specifies to match the exact IPv4 address (including the netmask).
- **any** - Specifies to match any IPv4 address.

To delete the specified IPv4 route access-list, in the global configuration mode, use the following command:

no access-list route *name* [{**deny** | **permit**} {{*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**exact-match**] | **any**}]

If any IP address matching rule is specified, the command will only delete the rule from the route access-list, but will not delete the route access-list.

To add description to the IPv4 route access-list, in the global configuration mode, use the following command:

access-list route *name* **description** *description*

- *name* – Specifies the name of the route access-list. The value range is 1 to 31 characters.
- *description* – Specifies the description of the route access-list. The value range is 1 to 31 characters.

To delete the description, in the global configuration mode, use the following command:

no access-list route *name* **description**

For example, the following commands will disallow OSPF to redistribute the routing information from BGP with the next-hop IP address set to 192.168.1.1 or any IP address in 192.168.2.0 segment:

```
hostname(config)# route-map test deny 10
hostname(config-route-map)# match ip next-hop access_list
hostname(config-route-map)# exit
hostname(config)# access-list route access_list permit 192.168.1.1/32
hostname(config)# access-list route access_list permit 192.168.2.0/24
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

Configuring an IPv6 Route Access List

To configure an IPv6 route access-list, in the global configuration mode, use the following command:

ipv6 access-list route *name* [{**deny** | **permit**} {*X:X:X:X::X/M* [**exact-match**] | **any**}]

- *name* - Specifies the name of the route access-list and enters the configuration mode of the route access-list. The value range is 1 to 31 characters. If the name already exists, you will be directly redirected to the configuration mode of the route access-list.
- **deny** | **permit** - Specifies the action for the matched IPv6 address.
- *X:X:X:X::X/M* - Specifies the IPv6 prefix and prefix length to be matched.
- **exact-match** - Specifies to match the exact IPv6 address (including the netmask).
- **any** - Specifies to match any IPv6 address.

To delete the specified IPv6 route access-list, in the global configuration mode, use the following command:

no ipv6 access-list route *name* [{**deny** | **permit**} {*X:X:X:X::X/M* [**exact-match**] | **any**}]

If any IP address matching rule is specified, the command will only delete the rule from the route access-list, but will not delete the route access-list.

To add description to the IPv6 route access-list, in the global configuration mode, use the following command:

ipv6 access-list route *name* **description** *description*

- *name* – Specifies the name of the route access-list. The value range is 1 to 31 characters.
- *description* – Specifies the description of the route access-list. The value range is 1 to 31 characters.

To delete the description, in the global configuration mode, use the following command:

no ipv6 access-list route *name* **description**

AS Path Access List

The AS path is the sequence of AS numbers that route traverses before reaching the destination network. Before advertising a route to anther AS, BGP adds the local AS number into the AS_PATH attribute.

You can implement route filtering based on the AS path access list, which consists of two parts: a regular expression and the corresponding operation (permit or deny) to be performed upon successful matches. If the regular expression matches the AS path of the route, the system proceeds to execute the specified operation. Otherwise, the system performs the deny operation. You can configure at most 64 AS path access lists and each AS path access list can have at most 8 regular expressions configured.

Configuring an AS-path Access List

To configure the AS-path access list, use the following command in the global configuration mode:

ip as-path access-list *access-list-number* {**deny** | **permit**} *regular-expression*

- *access-list-number* – Specifies the number of the AS-path access list. The range is 1 to 500.
- **deny** | **permit** – Specifies the action that will be performed to the route that matches the AS-path access list.
- *regular-expression* – Specifies the regular expressions to match the AS path. StoneOS supports the Perl Compatible Regular Expressions (PCRE).

To delete the AS-path access list, use the following command in the global configuration mode:

no ip as-path access-list *access-list-number* [{**deny** | **permit**} *regular-expression*]

In the example below, you can configure an AS-path access list whose number is 1, refuse the route that has traversed AS 31, and allow other routes.

```
hostname(config)# ip as-path access-list 1 deny _31_
hostname(config)# ip as-path access-list 1 permit .*
hostname(config)#
```

Community List

A BGP community is a group of routes with the same characteristics, independent of their associated IP subnets and ASs. Besides custom community attributes, the system supports the following well-known BGP community attributes:

- No-export: Routes with this community attribute cannot be advertised to peers that are outside the AS.
- No-adverties: A route with this attribute cannot be advertised to any other BGP peers.

- Local-as: Routes with this community attribute can be advertised to other peers only in the local AS.
- Internet: By default, all routes belong to the Internet community. A route with this attribute can be advertised to all BGP peers.

Configuring BGP Communities

To configure the community list, use the following command in the global configuration mode:

ip community-list {**standard** *community-list-name* | *community-list-number*} {**deny** | **permit**} {[**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*]}

- **standard** *community-list-name* – Specifies the name of the community list. You can specify up to 31 characters.
- *community-list-number* - Specifies the number of the community list. The number is in the range of 1 to 99.
- **deny** | **permit** – Specifies the actions performed to the route that matched the list. deny means the route will be denied and permit means the route will be permitted.
- [**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*] – Specifies the communities path attributes. You can specify one or more attributes and use one space to separate them. The value of *community-number*is in the range of 1 to 4294967295.

To delete the community list, use the following command in the global configuration mode:

no ip community-list {**standard** *community-list-name* | *community-list-number*}

ECMP

Equal Cost Multi-Path Routing (ECMP) is a routing strategy where the next-hop packet forwarding to a single destination can occur over multiple best paths which tie for top place in routing metric calculations.

Configuring ECMP

By default the ECMP function is enabled, and allows up to 40 equal-cost routes for the purpose of load balancing. To enable or disable ECMP, in the VRouter configuration mode, use the following command:

ecmp enable *ecmp-route-num*

- *ecmp-route-num* - Specifies the maximum number of ECMP routes permitted in the system. The value range is 1 to 1000. The value of 1 indicates ECMP is disabled.

Configuring ECMP Route Selection

To configure the method for selecting an ECMP route, in the global configuration mode, use the following command:

ecmp-route-select {**by-5-tuple** | **by-src** | **by-src-and-dst**}

- **by-5-tuple** - Selects a route based on network quintuple (source IP address, destination IP address, source port, destination port and service type).
- **by-src** - Selects a route based on the source IP address.
- **by-src-and-dst** - Selects a route based on the source IP address and destination IP address. This is the default method.

Static Multicast Routing

Multicast refers to the communication method of transmitting data from one source to multiple destination nodes. The source that sends data is known as the multicast source, and the nodes that receive data form a multicast group. The destination address to which the multicast source sends data is known as a multicast address. Its range is 224.0.0.0 to 239.255.255.255 (Class D addresses).

Any host in the Internet can be used as a multicast source. Once the multicast source sends one copy of data to the multicast address, all the nodes in the group will receive the data. Information transmission by multicast can effectively save the network bandwidth. Increasing the number of

users accessing the network will not lead to a heavier burden on the host that is sending data, thus reducing network workload.

To transmit data from the multicast source to the members in the multicast group, you need to manually configure the following options for the multicast routing rule:

- Multicast source and multicast address: the source IP and destination IP of the multicast.
- Ingress and egress interface: the data that match the corresponding multicast source and multicast address flows in from the ingress interface specified in the multicast routing rule, and flows out from the specified egress interface.

Enabling/Disabling a Multicast Route

By default the multicast route is disabled. To enable or disable the multicast route, in the VRouter configuration mode, use the following commands:

- Enable: **ip multicast-routing**
- Disable: **no ip multicast-routing**

Configuring a Static Multicast Route

To create a static multicast route, in the VRouter configuration mode, use the following command:

ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

- *A.B.C.D A.B.C.D* - Specifies the multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address. The value range is 224.0.0.0 to 239.255.255.255.
- **iif** *interface-name* - Specifies an ingress interface. You can specify up to two ingress interfaces.
- **eif** *interface-name* - Specifies an egress interface. You can specify up to four egress interfaces.

To delete the specified static multicast route, in the VRouter configuration mode, use the following command:

no ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

Specifying an Ingress/Egress Interface

You can configure an ingress or egress interface for the existing static multicast route. Each multicast route can have up to two ingress interfaces, and up to 32 egress interfaces. The options of ingress and egress interface must be configured in the static multicast route configuration mode. To enter the static multicast route configuration mode, in the VRouter configuration mode, use the following command:

ip mroute *A.B.C.D A.B.C.D*

- *A.B.C.D A.B.C.D* - Specifies the multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.

To specify an ingress and egress interface for the existing static multicast routing entry, in the static multicast route configuration mode, use the following command:

- Specify an ingress interface: **iif** *interface-name*
- Specify an egress interface: **eif** *interface-name*

Repeat the above command to configure multiple ingress or egress interfaces.

Viewing Multicast Route Information

To view the multicast route information, in any mode, use the following command:

show ip mroute [*A.B.C.D A.B.C.D* | **static** | **summary**] [**vrouter** *vr-name*]

- **show ip mroute** - Shows all the multicast route information.
- *A.B.C.D A.B.C.D* - Shows the multicast route information of the specified multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.
- **static** - Shows the static multicast route information.

- **summary** - Shows the summary of multicast route.
- **vrouter** *vr-name* - Shows the multicast route information of the specified VRouter.

Viewing Multicast FIB Information

To view the multicast FIB information, in any mode, use the following command:

show mfib [*A.B.C.D A.B.C.D* | **summary**] [**vrouter** *vr-name*]

- **show mfib**- Shows all the multicast FIB information.
- *A.B.C.D A.B.C.D* - Shows the multicast FIB information of the specified multicast source and multicast address. The first *A.B.C.D* is the IP address of the multicast source, and the second *A.B.C.D* is the multicast address.
- **summary** - Shows the summary of multicast FIB.
- **vrouter** *vr-name* - Shows the multicast FIB information of the specified VRouter.

IGMP

Internet Group Message Protocol (IGMP) is used to establish and maintain multicast group membership between hosts and routers. A host reports its membership of a group to its local router over IGMP, and a router listens to reports from hosts and periodically sends out queries to check if any group member is alive. If no report is received from the member, the router side will determine there is no member in the multicast group.

The latest version of StoneOS supports IGMPv1 (defined in RFC1112) , IGMPv2 (defined in RFC2236) and IGMPv3 (defined in RFC3376). And it also supports IGMP Proxy (operating on the Application Layer) and IGMP Snooping (operating on the Link Layer).

IGMP Proxy

IGMP Proxy is designed to create multicast routing tables and forward multicast data by intercepting the IGMP packets between the hosts and routers. IGMP Proxy acts differently on the two interfaces of the Hillstone device:

On the upstream interface that connects to the multicast router, it acts as a host, responsible for responding to the queries from the router. When a new member is added to the multicast group, or when the last member exits, the proxy will proactively send a packet to report the member status on the upstream interface.

On the downstream interface that connects to the host, it acts as a router, responsible for the registration, query and deletion of group members.

To configure a IGMP proxy, take the following steps:

1. Enable multicast. For detailed operation, see Enabling/Disabling a Multicast Route.
2. Enable an IGMP proxy.
3. Configure the upstream interface to the host mode.
4. Configure the downstream interface to the router mode.
5. Configure a policy rule.

Enabling an IGMP Proxy

To enable or disable the IGMP proxy function, in the VRouter configuration mode, use the following commands:

- Enable: **ip igmp-proxy enable**
- Disable: **no ip igmp-proxy enable**

To enter the VRouter configuration mode, in the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* - Specifies a Vrouter. If the name exists, the system will directly enter the Vrouter configuration mode.

Configuring an IGMP Proxy Mode for an Interface

To configuring an IGMP proxy mode (either router mode or host mode) for an interface, in the interface configuration mode, use the following command:

ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*] [**v2** | **v3**]

- **router-mode** - Configures the IGMP proxy mode of the downstream interface to the router mode.
- **host-mode** - Configures the IGMP proxy mode of the upstream interface to the host mode.
- [*A.B.C.D*] - Specifies the multicast address. The IGMP proxy mode will only be applied to this address.
- **v2** – Specifies the protocol version of the IGMP message is IGMPv2. By default, the IGMPv2 protocol is used.
- **v3** – Specifies the protocol version of the IGMP message is IGMPv3.

To cancel the IGMP proxy mode for the specified interface, in the interface configuration mode, use the following command:

no ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

Viewing IGMP Proxy Information

To view the IGMP Proxy information, in any mode, use the following command:

show ip igmp-proxy [*A.B.C.D*] [**vrouter** *vrouter-name*]

- **show ip igmp-proxy** - Shows all the IGMP Proxy information in the system.
- [*A.B.C.D*] - Shows the IGMP Proxy information of the specified multicast address.
- [**vrouter** *vrouter-name*] - Shows the IGMP Proxy information of the specified VRouter.

IGMP Snooping

IGMP Snooping is designed to create multicast routing entries for a specific multicast address on a Layer 2 device by listening to the IGMP packets between hosts and routers. With IGMP Snooping enabled, the Hillstone device can forward multicast data based on the created multicast routing entries, efficiently reducing the cost of multicast communication. If IGMP Snooping is disabled, Hillstone device only advertises multicast data.

To configure IGMP Snooping, take the following steps:

1. Enable multicast. For detailed operation, see Enabling/Disabling a Multicast Route.
2. Enable IGMP Snooping.
3. Configure IGMP Snooping.
4. Configure a policy rule.

Enabling IGMP Snooping

To enable or disable the IGMP Snooping function, in the VSwitch configuration mode, use the following commands

- Enable: **ip igmp-snooping enable**
- Disable: **no ip igmp-snooping enable**

To create or enter the VSwitch configuration mode, in the global configuration mode, use the following command:

vswitch vswitch *Number*

- *Number* - Specifies the VSwitch's identifier. The value range may vary from different platforms. For example, the command vswitch vswitch2 will create a VSwitch named VSwitch2, as well as an interface named VSwitchif2. Besides the system will enter the configuration mode of VSwitch2. If the specified VSwitch exists, the system will directly enter the VSwitch configuration mode.

Configuring IGMP Snooping

To configuring IGMP Snooping, in the interface configuration mode, use the following command:

ip igmp-snooping {**router-mode** [*A.B.C.D*] | **host-mode** [*A.B.C.D*] | **disable** | **auto**}

- **router-mode** - Configures the IGMP Snooping mode of the downstream interface to the router mode.
- **host-mode** - Configures the IGMP Snooping mode of the upstream interface to the host mode.
- [*A.B.C.D*] - Specifies the multicast address.
- **disable** - Disables IGMP Snooping for the interface.
- **auto** - The system will determine the interface mode automatically based on the IGMP packet.

To cancel the IGMP Snooping mode, in the interface configuration mode, use the following command:

no ip igmp-snooping {**router-mode** *A.B.C.D* | **host-mode** *A.B.C.D*}

Dropping Unknown Multicast

By default dropping unknown multicast is disabled. With this function enabled, the device will drop the packets that are destined to unknown multicast groups, thus saving the bandwidth. To enable the function, in the VSwitch configuration mode, use the following command:

unknown-multicast drop

To disable the function, in the VSwitch configuration mode, use the following command:

no unknown-multicast drop

Viewing IGMP Snooping Information

To view the IGMP Snooping information, in any mode, use the following command:

show ip igmp-snooping [*A.B.C.D*] [**vswitch** *name*]

- **show ip igmp-snooping** - Shows all the IGMP Snooping information.
- [*A.B.C.D*] - Shows the IGMP Snooping information of the specified multicast address.
- [**vswitch** *name*] - Shows the IGMP Snooping information of the specified VSwitch.

BFD

BFD (Bidirectional Forwarding Detection) is a unified detection mechanism for the entire network, which is used to fast detect and monitor the forwarding and connection status of the link and the IP route. To enhance the network performance, the protocol neighbor must have the ability to detect the communication failures quickly. Thus, the backup communication can be established to restore the communication in time.

BFD creates sessions between two routers for monitoring the bidirectional forwarding path between these two routers, which provides services for the upper level protocol, for example, routing protocol. BFD does not have the discovering mechanism and upper level protocol will notify BFD to create sessions with specifies objects. If no BFD packets are received from the peer during the detection period after creating sessions, BFD will notify the upper-level service and the upper-level service will execute the corresponding operations.

In the current StoneOS, BFD can integrate with static route, OSPF route, and BGP route. Thus, StoneOS can realize the detection of the forwarding and connection status on the link that runs static route, OSPF route, and BGP route.

BFD Work Mode

Establishing a BFD session has two modes: active mode and passive mode. StoneOS now supports the active mode.

- Active mode: No matter whether BFD control packets are received or not from the peer before creating sessions, the BFD control packets will be sent actively.

- Passive mode: BFD control packets will not be sent before creating sessions until the control packets, which are sent from the peer, are received. During the process of initiating the sessions, one of the two sides must run in the active mode.

BFD has two detection modes that will work after creating sessions: asynchronous mode and inquiry mode. Two sides in the communication must be in the same mode.

- Asynchronous mode: Devices that works in the asynchronous mode send the BFD control packets periodically. If the peer does not receive the BFD control packets during the detection period, the session is considered as the down status.
- Inquiry mode: Assume that there is an independent method to confirm the connection status with the peer system. In this way, after creating the BFD session, the device will stop sending the BFD control packets periodically except for the requirements of verifying the connection apparently.

BFD Echo

The BFD Echo function makes the local device send the BFD Echo packets periodically and the peer device only returns the packets to the local device via the forwarding channel. You can use the Echo function to discover failures fast.

The Echo function can integrate with the detection methods. If you enable the Echo function in the asynchronous mode, the device will reduce the sending of the control packets. If you enable the Echo function in the inquiry mode, you can cancel the sending of BFD packets after the BFD session is established.



Notes: To use the Echo function, ensure the peer device can forward the Echo packets after you enable the Echo function in the local device.

Configuring BFD

Configuring BFD involved the following sections:

- Configuring the BFD detection methods
- Configuring the BFD session parameters
- Enabling/Disabling the Echo function
- Specifying the interval of receiving Echo packets
- Configuring the source IP address of the Echo packets

Configuring the BFD Detection Methods

There are two detection methods after creating the BFD session: asynchronous mode and the inquiry mode. Two sides in the communication must be in the same mode. By default, the detection mode of the BFD session is the asynchronous mode. You can change the mode according to your requirements. To use the inquiry mode, use the following command:

bfd demand enable

To change back to the asynchronous mode, use the following command:

no bfd demand enable

Configuring the BFD Session Parameters

After creating the BFD sessions, you can modify the minimum interval of receiving/sending BFD session packets and edit the multiple for calculating the timeout value. To configure the BFD session parameters, use the following command in the interface configuration mode:

bfd min-tx *min-tx-value* **min-rx** *min-rx-value* **detect-multiplier** *value*

- *min-tx-value* – Specifies the minimum interval of sending BFD packets. The unit is millisecond. The default value is 100 and it is in the range of 100 to 1000.
- *min-rx-value* – Specifies the minimum interval of receiving BFD packets. The unit is millisecond. The default value is 100 and the range is 100 to 1000.
- *value* – Specifies the multiple for calculating the timeout value. The detailed information of

To restore the value to the default one, use the following command in the interface configuration mode: **no bfd min-tx min-rx detect-multiplier**.



Notes:

- In the asynchronous mode, the system compares the value of the *min-tx-value* parameter of the local device with the value of the *min-rx-value* of the peer device, uses the bigger one times the value of the *value parameter* configured for the peer device, and uses the result as the timeout value.
- In the inquire mode with the Echo function enabled, the system compares the value of the *min-tx-value* parameter of the local device with the interval of receiving Echo packets configured for the peer device, uses the bigger one times the value of the *value* parameter configured for the local device, and uses the result as the timeout value.
- In the asynchronous mode with the Echo function enabled, the system compares the value of the *min-tx-value* parameter of the local device with the interval of receiving Echo packets configured for the peer device, uses the bigger one times the value of the *value* parameter configured for the peer device, and uses the result as the timeout value.

For more information about configuring the interval of receiving Echo packets, see Specifying the Interval of Receiving Echo Packets.

Enabling/Disabling the Echo Function

By default, the Echo function is disabled. To enable this function, use the following command in the interface configuration mode:

bfd echo enable

Use the following command in the interface configuration mode to disable the function:

no bfd echo enable

Specifying the Interval of Receiving Echo Packets

To specify the interval of receiving Echo packets, use the following command in the interface configuration mode:

bfd min-echo-rx *value*

- *value* – Specifies the interval of receiving BFD Echo packets. The unit is millisecond. The default value is 0 and the range is 100 to 1000.

To restore the value to the default one, use the following command in the interface configuration mode: **no bfd min-echo-rx**.

Configuring the Source IP Address of the Echo Packets

A large number of ICMP redirection packets sent from the peer leads to the network congestion. To avoid the network congestion, you can configure the source IP address of the Echo packets. To configure the source IP address, use the following command in the global configuration mode:

bfd echo-source-ip *echo-src-address*

- *echo-src-address* – Specifies the source IP addresses of the BFD Echo packets.

To delete the configured source IP address, use the following command in the global configuration mode: **no bfd echo-source-ip**.



Notes:

- You can specify a random source IP address of the Echo packets. Hillstone recommends you use an IP address which does not belong to the network segments where interfaces of the device locate.
- The destination IP address of the Echo packets that sent from the local device is the interface IP address of the local device.

Configuring BFD Multi-hop Detection

BFD sessions support one-hop detection and multi-hop detection. You can select the detection method according to the session networking.

- One-hop detection: BFD can detect the connectivity of the IP link between two directly-connected systems.
- Multi-hop detection: BFD can detect the link connectivity of any path between two devices.



Notes:

- In the current system, only BFD multi-hop session detection can integrate with the BGP route.
- BFD multi-hop session detection only supports the asynchronous mode, but not the query mode and echo function.

Creating a BFD Multi-hop Detection Template

The BFD multi-hop detection template is used to specify the encryption authentication mode of BFD control packets, the minimum interval and the detection time multiple for sending or receiving BFD multi-hop session packets. To create a BFD multi-hop detection template, in the global configuration mode, use the following command:

bfd template *template-name***multi-hop**

- *template-name* - Specifies the name of the BFD multi-hop detection template and enter the BFD multi-hop detection template configuration mode. If the specified name already exists, enter the BFD multi-hop detection template configuration mode directly.

To delete the specified BFD multi-hop detection template, in the global configuration mode, use the command **no bfd template***template-name*.

Specifying the Encrypted Authentication Mode of BFD Control Packets

As the number of network hops increases, BFD control packets may be tampered more easily. In BFD sessions, BFD control packets can be encrypted and authenticated. To specify the encrypted authentication mode of BFD control packets, in the BFD multi-hop detection template configuration mode, use the following commands:

authentication-type {**m-md5** | **m-sha1** | **md5** | **sha1** | **simple**} *key-id* {**plain***plain-string*}

- **m-md5** | **m-sha1** | **md5** | **sha1** | **simple** - Specifies the authentication algorithm: Meticulous MD5 algorithm (m-md5), Meticulous SHA1 algorithm (m-sha1), MD5 algorithm(md5), SHA1 algorithm (sha1) and simple authentication (simple).
- *key-id* – Specifies the authentication ID.
- **plain** *plain-string* – Specifies the key in the form of plain text.

To delete the specified encrypted authentication mode of BFD control packets, in the BFD multi-hop detection template configuration mode, use the command**no authentication-type**.

Configuring BFD Multi-hop Session Parameters.

After the BFD multi-hop session is established, you can modify the minimum interval and the detection time multiplier for sending or receiving BFD multi-hop session packets. To configure the BFD multi-hop session parameters, in the BFD multi-hop detection template configuration mode, use the following commands:

interval min-tx *min-tx-value***min-rx***min-rx-value* **detect-multiplier** *value*

- *min-tx-value* – Specifies the minimum interval for sending the BFD multi-hop session packets. The range is 100 to 1000 milliseconds, and the default value is 100 milliseconds.
- *min-rx-value* – Specifies the minimum interval for receiving the BFD multi-hop session packets. The range is 100 to 1000 milliseconds, and the default value is 100 milliseconds.
- **detect-multiplier***value* – Specifies the detection time multiplier to calculate the detection timeout time. The default value is 3, and the range is 3 to 50.

To restore to the default value, in the BFD multi-hop detection template configuration mode, use the command**no interval min-tx***min-rx* **detect-multiplier**.

Integrating BFD with Routing Protocols

BFD can integrate with following routing protocols:

- Integrating BFD with the static route
- Integrating BFD with the OSPF route
- Integrating BFD with the BGP route
- Integrating BFD with the IS-IS Route

Integrating BFD with the Static Route

The static route does not have the neighbor discovering mechanism. Thus, when BFD integrates with the static route, a failure detected by the BFD session indicates that the next hop is not reachable and this route will not be added to the routing table.

To integrate BFD with the static route and enable the BFD detection function for the specified next hop, use the following command in the VRoute configuration mode:

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – Specifies the network address of the static route. Hillstone devices support two formats: *A.B.C.D/M* or *A.B.C.D A.B.C.D*, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- *interface-name A.B.C.D* – Specifies the IP address of the next-hop interface.
- **bfd** – Enables the BFD detection function for the specified next hop.

To cancel the integration, use the following command in the VRouter configuration mode:

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

Integrating BFD with the OSPF Route

By integrating BFD with the OSPF route, the system realizes the quick link detection which has higher performance than the Hello detection mechanism of the OSPF protocol. With the integration, OSPF protocol improves its convergence performance.

To integrate BFD with the OSPF rout and enable the BFD detection function on the specified interfaces that corresponds to the OSPF route, use the following command in the interface configuration mode:

ip ospf bfd

To cancel the integration, use the following command in the interface configuration mode:

no ip ospf bfd

Integrating BFD with the BGP Route

To integrate BFD with the BGP route and enable the BFD detection function for the specified BGP neighbor, you can select the one-hop or multi-hop detection. In the BGP instance configuration mode, use the following command:

neighbor *A.B.C.D* **fall-over bfd** [**multi-hop** *bfd-template-name*]

- *A.B.C.D* – Specifies the IP address of the BGP peer.
- **multi-hop** *bfd-template-name* – When the multi-hop detection mode is used, specify the name of the BFD multi-hop detection template to bind this template. If this parameter is not specified, the single-hop detection mode will be used.

To cancel the integration, use the following command in the BGP instance configuration mode:

no neighbor *A.B.C.D* **fall-over bfd**

Integrating BFD with the IS-IS Route

By integrating BFD with the IS-IS route, and BFD works with IS-IS to more quickly detect the faults that occur on neighboring devices or links. In this manner, fast route convergence is implemented.

To integrate BFD with the IS-IS route and enable the BFD detection function on the specified interfaces that corresponds to the IS-IS route, use the following command in the interface configuration mode:

isis bfd

To cancel the integration, use the following command in the interface configuration mode:

no isis bfd

Viewing BFD Session Information

To view the BFD session information, use the following command in any mode:

show bfd session [**interface** *interface-name* | **neighbor***A.B.C.D* | **detail**]

- **interface** *interface-name* - Shows the information of the BFD sessions of the specified interface.
- *A.B.C.D* – Specifies ID of the neighbor router.
- **detail** – Shows the detailed information of the BFD sessions of all routers.

MPLS

MPLS is a technique which enables the forwarding of packets based on labels. A label is a fixed-length local identifier, encapsulated between the link layer and the network layer. It is used to identify the FEC (Forwarding Equivalence Class) to which a packet belongs, so that a group of packets can be forwarded in the same manner, for example, over the same path or with the same forwarding treatment. For packets carrying MPLS labels, forwarding is based on label lookup and replacement only, rather than on the destination IP address in traditional IP forwarding.

There are MPLS networks which contain LSRs (Label Switching Routers) as basic units. LSRs locating on the edge of an MPLS network are called LERs (Label Edge Routers) which interconnect with non-MPLS networks.

When an IP packet enters the MPLS network, the ingress LER parses the packet's header, encapsulates the packet with a label and then forwards it to the next hop. All subsequent MPLS nodes will do packet forwarding based on the label of the received packet without parsing the IP header, until the label is removed when the packet leaves the MPLS network.

In the MPLS network, when StoneOS device is deployed in Layer-2 security zone mode, it is capable of decapsulating the MPLS label to obtain the IP packet and then send the packet at to related service modules for security control. After that, the IP packet will be encapsulated with the previously removed labels and then transparently sent to other LSR.

StoneOS device can decapsulate at most five-layer MPLS labels. Packets encapsulating in more than 5-layer labels will be treated as non-IP packets and processed based on the configuration of the **l2-nonip-action** command.

MPLS packet security control is disabled by default. To enable this function, use the following command in the VSwitch configuration mode (enter the mode by using command **vswitch** **vswitch** *Number*):

mpls-tunnel-inspection-enable

To disable this function, use the following command in the VSwitch configuration mode:

no mpls-tunnel-inspection-enable

To enable MPLS debugging, use the following command in any mode:

debug dp mpls {**basic** | **error**}

- **basic** – Enables MPLS basic information debugging.
- **error** – Enables MPLS error information debugging.

To disable MPLS debugging, use the following command in any mode:

undebug dp mpls {**basic** | **error**}

- **basic** – Disables MPLS basic information debugging.
- **error** – Disables MPLS error information debugging.

Protocol Independent Multicast (PIM)

The Protocol Independent Multicast (PIM) indicates that static route or any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP, can provide the routing information for IP multicast. Multicast routing is not dependent on the unicast routing protocols, except that the multicast routing tables are generated by the unicast routing protocols.

According to different mechanisms, PIM is divided into the following two modes:

- Protocol Independent Multicast-Dense Mode (PIM-DM): applies to small-scale networks in which receivers are densely distributed.
- Protocol Independent Multicast-Sparse Mode (PIM-SM): applies to large-scale networks in which receivers are sparsely distributed.

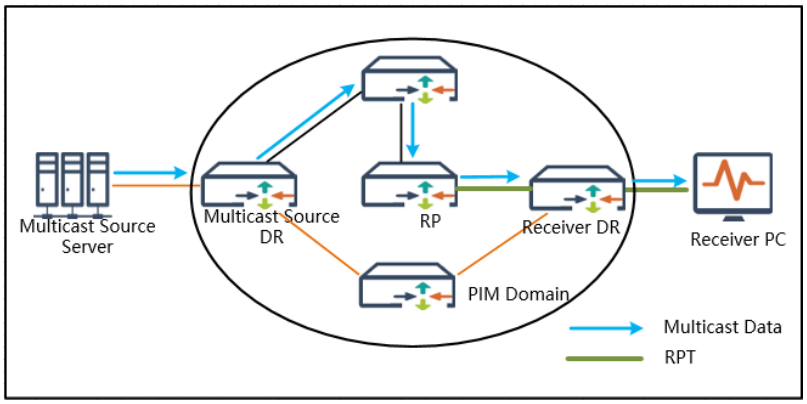
Currently, system only supports the PIM-SM mode.

Basic Principles of PIM-SM

PIM-SM can resolve P2MP data transmission problems in a large-scale network where users are sparsely distributed, so as to PIM-SM enable users to receive data on demand.

PIM-SM assumes that no host wants to receive multicast data. The PIM device forwards multicast data to the host only when a host requests multicast data explicitly.

PIM-SM sends the multicast information to the PIM device in the PIM domain through the configured RP (Rendezvous Point) and BSR (BootStrap Router), and then an RPT (Rendezvous Point Tree) will be built. Multicast data can be forwarded to the receiver along the RPT through the RP.



The key concepts of PIM-SM are as follows:

- **PIM Domain**: A network formed by PIM devices.
- **DR (Designated Router)**: There are two types of DR in a PIM network.

- **Multicast source DR**: A PIM device that is directly connected to the multicast source in a PIM-SM domain and is responsible for sending Register messages to the RP.
- **Receiver DR**: A PIM device that is directly connected to group members (receiver hosts) and is responsible for forwarding multicast data to the group members.
- **RP (Rendezvous Point)**: An RP is the core of a PIM-SM network, which can be divided into the static RP and dynamic RP. An RPT is a shared tree with an RP as the root and members of multicast group as the leaves in a PIM-SM network.
- **BSR (BootStrap Router)**: A BSR of a PIM-SM network, which is responsible for collecting and distributing RP information.
- **RPT (Rendezvous Point Tree)**: An RPT is a multicast distribution tree (MDT) with an RP as the root and members of multicast group as the leaves.
- **SPT (Shortest Path Tree)**: A shortest path tree (SPT) is a multicast distribution tree (MDT) with the multicast source as the root and members of multicast group as leaves.

Configuring PIM-SM

PIM-SM configurations include basic configurations and configurations of PIM-SM on different interfaces.

The basic configurations of PIM-SM include:

- Enabling/Disabling a Multicast Route (For details, see the Static Multicast Routing > Enabling/Disabling a Multicast Route section)
- Enabling/Disabling the PIM-SM
- Configuring a Candidate RP
- Configuring a Candidate BSR

- Configuring a Static RP
- Configuring the Switchover to SPT

The PIM-SM configurations for the interfaces include:

- Enabling/Disabling the PIM-SM for Interfaces
- Configuring the Priority of DR
- Specifying the Interval for Sending the Hello Packets
- Specifying the Interval for Sending IGMP General Query Messages.
- Specifying the IGMP General Query Timeout
- Specifying the Maximum Response Time for IGMP General Query
- Specifying the Non-direct Multicast Source Address
- Configuring the Multicast Router Interface to Join the Multicast Group
- Configuring the MSR Function



Notes: The PIM-SM function cannot be configured with the static multicast routing function or the IGMP Proxy function at the same time.

Basic Configurations

You can configure PIM-SM for different VRouter. The basic configurations of PIM-SM must be configured in the PIM-SM configuration mode. To enter the PIM-SM configuration mode, in the global configuration mode, use the following commands:

ip vrouter*vrouter-name* (entering the VRouter configuration mode)

router pim(entering the PIM-SM configuration mode)

Enabling/Disabling the PIM-SM

By default, the PIM-SM function is disabled. To enable or disable the PIM-SM function, in the PIM-SM configuration mode, use the following commands:

- Enable: **pim-sm enable**
- Disable: **no pim-sm enable**

Configuring a Candidate RP

Select PIM devices in the PIM-SM domain to configure as the candidate RP (Rendezvous Point), and then the RP will be elected from the candidates. Configure the candidate BSR at the same time, and then the BSR will be elected from the candidate BSR (BootStrap Router), which is responsible for collecting and distributing the RP information in the network.

To configure the candidate RP, in the PIM-SM configuration mode, use the following commands:

rp-candidate*interface-name* [**interval** *interval-time*] [**priority** *level*]

- *interface-name* – Specifies the interface where the candidate RP resides. The interface must be enabled with PIM-SM.
- *interval-time* – Specifies the interval for sending candidate RP messages. The range is 1 to 16383 seconds. The default value is 60 seconds.
- **priority** *level* – Specifies the priority (the smaller the value, the higher the priority). In the RP election, the candidate RP with the higher priority will be elected as the RP. The range is 0 to 255 and the default priority is 0.

To delete the configuration of candidate PR, in the PIM-SM configuration mode, use the following command:

no rp-candidate



Notes: When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is 224.0.0.0/4.

Configuring a Candidate BSR

In a PIM-SM domain, you need to configure one or more candidate BSR, and the BSR will be generated from the candidate BSR automatically. The BSR will collect and distribute the RP information.

To configure the candidate BSR, in the PIM-SM configuration mode, use the following commands:

bsr-candidate*interface-name* [**priority** *level*]

- *interface-name* – Specifies the interface where the candidate BSR resides. The interface must be enabled with PIM-SM.
- **priority** *level* – Specifies the priority (the higher the value, the higher the priority). If there is only one candidate BSR in the PIM-SM domain, it will be become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255, the default priority is 0.

To delete the configuration of candidate BSR, in the PIM-SM configuration mode, use the following command:

no bsr-candidate



Notes: When a dynamic RP is used, the candidate BSR and at least one candidate BSR must be configured in the PIM-SM domain.

Configuring a Static RP

When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP, which can save the bandwidth occupied by message exchange between the Candidate RP and the BSR. In the PIM-SM domain, the static RP configured on all the devices should be the same.

To specify the address of static RP, in the PIM-SM configuration mode, use the following commands:

rp-address*A.B.C.D* [*A.B.C.D/M*]

- *A.B.C.D* – Specifies the IP address of the interface where the static RP resides.
- *A.B.C.D/M* – Specifies the multicast address.

To delete the configured static RP address, in the PIM-SM configuration mode, use the following command:

no rp-address*A.B.C.D* [*A.B.C.D/M*]

Configuring the Switchover to SPT

Since the RPT (Rendezvous Point Tree) in the PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.

Figure: Before RPT switch to SPT

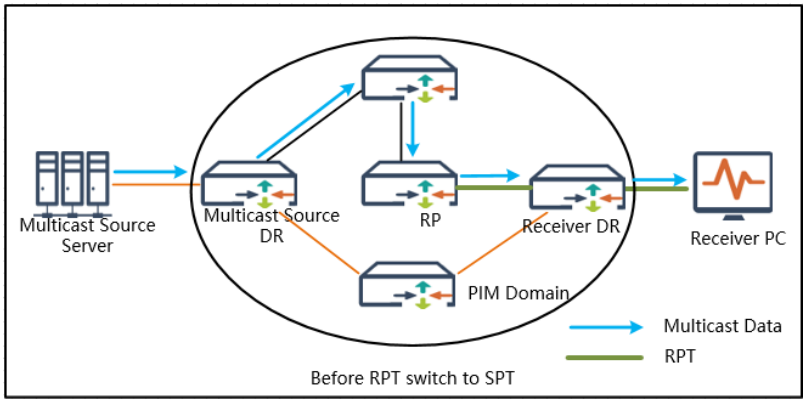
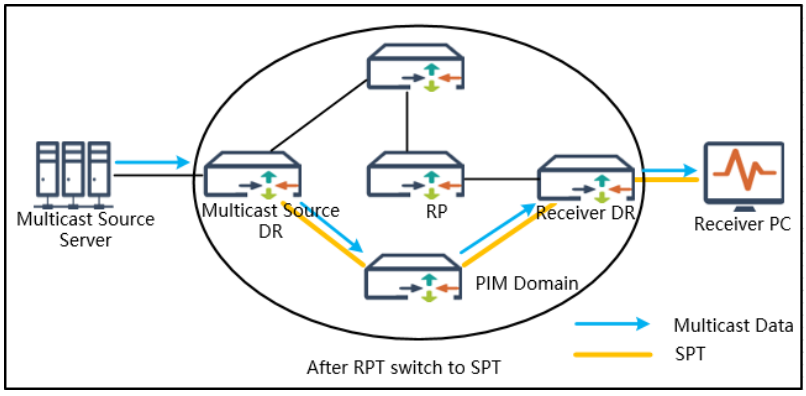


Figure: After RPT switch to SPT



To configure the switchover to SPT, in the PIM-SM configuration mode, use the following commands:

spt-threshold {0 | **infinity**}

- 0 – Enable the switchover from RPT to SPT. This is the default option.
- **infinity** – Disable the switchover to SPT.

To restore the switchover to SPT, in the PIM-SM configuration mode, use the following commands:

no spt-threshold

Configuring PIM-SM for Interfaces

The PIM-SM function for an interface must be configured in the interface configuration mode. The PIM-SM configurations for the interfaces include:

- Enabling/Disabling the PIM-SM for Interfaces
- Configuring the Priority of DR
- Specifying the Interval for Sending the Hello Packets
- Specifying the Interval for Sending IGMP General Query Messages.
- Specifying the IGMP General Query Timeout
- Specifying the Maximum Response Time for IGMP General Query
- Specifying the Non-direct Multicast Source Address
- Configuring the Multicast Router Interface to Join the Multicast Group
- Configuring the MSR Function

Enabling/Disabling the PIM-SM for Interfaces

By default, the PIM-SM function for interface is disabled. To enable or disable the PIM-SM function for interface, in the interface configuration mode, use the following commands:

- Enable PIM-SM on the specified interface:**ip pim sparse-mode**
- Disable PIM-SM on the specified interface:**no ip pim sparse-mode**



Notes: The PIM-SM function only can be enabled on the Layer 3 interface.

Configuring the Priority of DR

The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). To specify the priority of DR, in the interface configuration mode, use the following commands:

ip pim dr-priority *level*

- *level* – Specifies the priority of the DR (the higher the value, the higher the priority). The default value is 1. The range is 0 to 4294967294. All routers in the PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority of the routers is the same, the one with a large IP address will be selected.

To restore the default priority, in the interface configuration mode, use the command**no ip pim dr-priority**.

Specifying the Interval for Sending the Hello Packets

After the PIM-SM function is enabled on an interface, Hello packets will be sent periodically. You can specify the interval for sending Hello packets on the interface as needed. In the interface configuration mode, use the following command:

ip pim query-interval *interval*

- *interval* – Specifies the interval for sending Hello packets. The range is 1 to 65535, and the default interval is 30 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim query-interval**.

Specifying the Interval for Sending IGMP General Query Messages

The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain IGMP group membership of the interface. On the Hillstone device, after the PIM-SM function is enabled for the interface, the querier will send IGMP general query messages to learn about the entry and exit of multicast group members.

To specify the interval for sending IGMP general query messages, in the interface configuration mode, use the following command:

ip pim igmp-query-interval *interval*

- *interval* – Specifies the interval for sending IGMP general query messages. The range is 1 to 18000 seconds, and the default value is 60 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-interval**.

Specifying the IGMP General Query Timeout

If the multicast router in the network does not receive IGMP general query messages within the specified timeout period, multicast routers will elect a querier again.

To specify the IGMP general query timeout value, in the interface configuration mode, use the following commands:

ip pim igmp-query-timeout *timeout-value*

- *timeout-value* – Specifies the IGMP general query timeout value. The range is 30 to 300 seconds, and the default value is 120 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-timeout**.

Specifying the Maximum Response Time for IGMP General Query

You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the IGMP general query message twice and no response from

the receiver host within the specified maximum response time, system will delete the receiver in the multicast routing table.

To specify the maximum response time, in the interface configuration mode, use the following commands:

ip pim igmp-query-max-response-time*response-time*

- *response-time* – Specifies the maximum response time for IGMP general query. The range is 1 to 25 seconds, and the default value is 10 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-max-response-time**.

Specifying the Non-direct Multicast Source Address

The system cannot establish the neighbor relationship with a multicast source as the muticast source DR across different network segments, and the muticast source DR will discard multicast packets whose network segment is different from the ingress interface. Therefore, you can configure the non-direct multicast source address to ensure that the multicast source DR and multicast source multicast across network segments when unicast routing of the multicast source is reachable for all PIM devices within the multicast domain.

To specify the non-direct multicast source address, in interface configuration mode, use the following command:

ip pim non-direct multicast source*source-address/netmask*

- *source-address/netmask* – Specifies the multicast source address and subnet mask of the non-direct multicast source.

To delete the multicast source address of the non-direct multicast source, use the **no ip pim non-direct multicast source***source-address/netmask* command.



Notes:

- Only root-VSYS supports to configure the multicast source address of non-direct multicast source.
- You can configure at most 10 non-direct multicast source entries.

Configuring the MSR Function

The Multicast Service Reflection (MSR) function supports to process multicast data forwarded to the Vif interface by converting the source address and multicast group address of the original multicast stream into a new multicast stream. When multicast traffic matches the ingress interface and pre-reflection destination IP address in the MSR entry, it can be converted to the post-reflection destination IP address and source IP address in the MSR entry.

To configure a MSR entry, in Vif interface configuration mode, use the following command:

ip service reflect *interface-name* **destination** *dst-address-before* **to** *dst-address-after* **mask-len** *mask-length* **source** *source-address-after*

- *interface-name* - Specifies the ingress interface of the original multicast stream.
- *dst-address-before* - Specifies the multicast group address of the original multicast stream.
- *dst-address-after* - Specifies the post-reflection multicast group address.
- *mask-length* - Specifies the post-reflection subnet mask of the multicast group address. Valid values: 0 to 32.
- *source-address-after* - Specifies the post-reflection multicast source address, which needs to be in the same network segment as the IP address of the Vif interface.

To delete the specified MSR entry, in interface configuration mode, use the following command:

no ip service reflect *interface-name* **destination** *dst-address-before* **mask-len** *mask-length*

Notes:

- Only root VSYS supports the MSR function.
- When you use the MSR function, if unicast route performs route advertisement learning combined with the OSPF protocol, the OSPF network type on the Vif interface needs to be set to **point-to-point** by using the **ip ospf network point-to-point** command. This allows the neighbor device to learn non-host routes.
- You can configure at most 100 MSR entries. To edit an existing MSR entry, the *interface-name*, *dst-address-before*, and *mask-length* fields need to keep unchanged. Otherwise, a new MSR entry is created.
- X-series devices do not support this function.

Viewing PIM-SM Information

To view the BSR information, in any mode, use the following command:

show ip pim bsr-route [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BSR information of VRouter.

To view the PIM-SM interface information, in any mode, use the following command:

show ip pim interface [*interface-name*]

- *interface-name* - Shows the PIM information of the specified interface.

To view the PIM neighbor information, in any mode, use the following command:

show ip pim neighbor [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the PIM neighbor information of the specified VRouter.

To view the RP information, in any mode, use the following command:

show ip pim rp [**vrouter** *vrouter-name* | **mapping** [**vrouter** *vrouter-name*]]

- *vrouter-name* - Shows the RP information of the specified VRouter.
- **mapping** [**vrouter***vrouter-name*] - Shows all RP mapping information of the specified VRouter.

To view the RPF information, in any mode, use the following command:

show ip pim rpf*source-address* [**vrouter** *vrouter-name*]

- *source-address* – Shows the RPF information of the specified multicast source IP address.
- *vrouter-name* - Shows the RPF information of the multicast source IP address of the specified VRouter.

To view the IGMP multicast group information, in any mode, use the following command:

show ip pim igmp groups [*group-address* [**vrouter** *vrouter-name*]]

- *group-address* – Shows the IGMP multicast group information of the specified IP address.
- **vrouter** *vrouter-name* – Shows the IGMP multicast group information of the specified VRouter.

To view the IGMP interface information, in any mode, use the following command:

show ip pim igmp interfaces [*interface-name*]

- *interface-name* – Shows the IGMP information of the specified interface (the interface enabled with PIM-SM).

PIM-SSM

PIM-SM needs to maintain Rendezvous Points (RPs) to transmit multicast data. If receivers know the exact location of a multicast source and want to request multicast data directly from a multicast source, Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) can enable use hosts to rapidly join multicast groups. A shortest path tree (SPT) is set up between the multicast source and group members without maintaining an RP. The multicast data will be forwarded to receivers along the SPT.

Configuring PIM-SSM

The basic configurations of PIM-SSM include:

- Enabling/Disabling a Multicast Route (For the details, refer to **Static Multicast Routing** > **Enabling/Disling a Multicast Route**)
- Configuring the range of PIM-SSM multicast group address



Notes:

- PIM-SSM function is on the basis of the PIM-SM function. Configure PIM-SM mode first before configuring the PIM-SSM (For details, refer to **Protocol Independent Multicast** > **Configuring PIM-SM**).
- In HA environment, PIM-SSM only supports Active-Passive (A/P) mode.

Configuring Address Range of PIM-SSM Multicast Group

By default, the address range of PIM-SSM is 232.0.0.0/8. You can configure the address range of the PIM-SSM multicast group as needed, and the address range of PIM-SSM group should be the same within the network. When the address range of PIM-SSM multicast group is configured, the PIM-SSM function will also be enabled.

To configure the address range of the PIM-SSM multicast group, in the PIM-SM configuration mode, use the following command:

pim-ssm {**default** | *group-prefix/Mask* }

- **default** - Uses the default address range of PIM-SSM multicast group: 232.0.0.0/8.
- *group-prefix/Mask* - Specifies the address range of the certain PIM-SSM multicast group.

To delete the configured address range, in the PIM-SM configuration mode, use the following command:

no pim-ssm

Configuring IGMP Packets Filtering

You can filter IGMP packets received form the interfaces with PIM-SM/PIM-SSM function enabled to allow or deny multicast source or multicast group in the certain IGMP packets. By default, all IGMP packets will be allowed to receive by interfaces.

To make interface allow or deny multicast group in the IGMPv1/IGMPv2 packets, in the interface configuration mode, use the following command:

ip pim igmp {**permit** | **deny**} *group-prefix/Mask*

- **permit**- Allow interfaces to receive multicast group in the IGMPv1/IGMPv2 packets.
- **deny**- Make the interface deny receiving multicast group in the IGMPv1/IGMPv2 packets.
- *group-prefix/Mask*- Specify the address range of multicast group.

To restore to the default values, in the interface configuration mode, use the following command:

noip pim igmp {**permit** | **deny**}

To make interface allow or deny multicast source and multicast group in the IGMPv3 packets, in the interface configuration mode, use the following command:

ip pim igmpv3 {**permit** | **deny**} {**any** |*source-prefix/Mask*}{**any** |*group-prefix/Mask*}

- **permit**- Allow the interface to receive multicast source and multicast group in the IGMPv3 packets.
- **deny**- Make the interface deny receiving multicast source and multicast group in the IGMPv3 packets.
- **any** |*source-prefix/Mask*- Specify the address range of multicast source. **any** is for any multicast source address.
- **any** |*group-prefix/Mask* - Specify the address range of multicast group. **any** is for any multicast group address.

To restore to the default values, in the interface configuration mode, use the following command:

noip pim igmpv3 {**permit** | **deny**}

Adding Multicast Router Interface to Multicast Group

In a multicast environment, multicast receivers indicate their interest of receiving multicast data by sending an IGMP report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. However, if the routers do not connect to multicast receivers or the connected multicast receivers cannot send an IGMP report, data from the source fails to reach the routers. To solve this issue, you can add the interface of multicast routers to the multicast group by configuring join-group. The interface can be added to a specified multicast group based on the IGMPv2 protocol or IGMPv3 protocol.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv2, run the following command in the interface configuration mode:

ip pim igmp join-group*group-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv2 protocol.

In the interface configuration mode, run the **no ip pim igmp join-group***group-address* command to remove the interface from the specified multicast group.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv3, run the following command in the interface configuration mode:

ip pim igmpv3 join-group*group-addresssource-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv3 protocol.
- *source-address* - Specifies the IP address of multicast source data traffic that the interface receives.

In the interface configuration mode, run the **no ip pim igmp join-group***group-addresssource-address* command to remove the interface from the specified multicast group.



Notes:

- Only layer-3 interfaces can be added to the multicast group.
- To add an interface to the multicast group, the following requirements need to be met:
  - The PIM-SM function is enabled for the interface. For more information, refer to Enabling/Disabling the PIM-SM for Interfaces.
  - The device where the interface resides is receiver DR and has the highest priority. For more information about how to configure the priority of DR, refer to Configuring the Priority of DR.
  - The PIM-SM function is also enabled for the upstream device of the device where the interface resides.

MLD

Multicast Listener Discovery (MLD) is a protocol that manages IPv6 multicast members. The MLD protocol sets up and maintains memberships between IPv6 hosts and their directly connected multicast routers by exchanging MLD messages between them.

MLD has two versions: MLDv1 defined in RFC2710 and MLDv2 defined in RFC3810.



Notes: The system supports only MLDv1.

MLDv1

MLDv1 implements IPv6 multicast listener management based on the query and response mechanism.

MLDv1 defines the following messages:

- General Query: A querier sends General Query messages to all hosts and routers on the local network segment to discover which host groups have members on the network segment.
- Multicast Address Specific Query: A querier sends Multicast Address Specific Query messages to members in a specified multicast group on the shared network segment to check whether the group has members.
- Multicast Listener Report message: Hosts send Multicast Listener Report messages to a querier to request to join a multicast group or respond to General Query messages.
- Multicast Listener Done: A host sends a Multicast Listener Done message to notify the querier on the local network segment that it has left a group.

MLDv2

Based on MLDv1, MLDv2 allows member hosts to specify whether to accept messages from certain multicast sources.

MLDv2 messages consist of query messages and member report messages. MLDv2 does not define a specialized member leave message. The member leaves are communicated by using a specific type of report messages.

Configuring IPv6 PIM-SM

IPv6 PIM-SM configurations include basic configurations and configurations of PIM-SM on different interfaces.

The basic configurations of IPv6 PIM-SM include:

- Enabling/Disabling a Multicast Route (For more information, see Configuring IPv6 Routing.)
- Enabling/Disabling the IPv6 PIM-SM
- Configuring a Candidate RP
- Configuring a Candidate BSR

- Configuring a Static RP
- Configuring the Switchover to SPT

The IPv6 PIM-SM configurations for the interfaces include:

- Enabling/Disabling the IPv6 PIM-SM for Interfaces
- Configuring the Priority of DR
- Specifying the Interval for Sending the Hello Packets
- Specifying the Interval for Sending MLD General Query Messages.
- Specifying the MLD General Query Timeout
- Specifying the Maximum Response Time for MLD General Query

Basic Configurations of IPv6 PIM-SM

You can configure IPv6 PIM-SM for different VRouter. The basic configurations of IPv6 PIM-SM must be configured in the IPv6 PIM-SM configuration mode. To enter the IPv6 PIM-SM configuration mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* （entering the VRouter configuration mode）

ipv6 multicast-routing（enabling IPv6 multicast routing）

ipv6 router pim（entering the IPv6 PIM-SM configuration mode）

Enabling/Disabling the IPv6 PIM-SM

By default, the IPv6 PIM-SM function is disabled. To enable or disable the IPv6 PIM-SM function, in the IPv6 PIM-SM configuration mode, use the following commands:

- Enable: **pim-sm enable**
- Disable: **no pim-sm enable**

Configuring a Candidate RP

Select PIM devices in the IPv6 PIM-SM domain to configure as the candidate RP (Rendezvous Point), and then the RP will be elected from the candidates. Configure the candidate BSR at the same time, and then the BSR will be elected from the candidate BSR (BootStrap Router), which is responsible for collecting and distributing the RP information in the network.

To configure the candidate RP, in the IPv6 PIM-SM configuration mode, use the following commands:

rp-candidate *ipv6-address* [**interval** *interval-time*] [**priority** *level*]

- *ipv6-address* – Specifies the IPv6 address of the candidate RP interface. The address cannot be the link-local address. The interface must be enabled with IPv6 PIM-SM.
- *interval-time* – Specifies the interval for sending candidate RP messages. The range is 1 to 16383 seconds. The default value is 60 seconds.
- **priority** *level* – Specifies the priority (the smaller the value, the higher the priority). In the RP election, the candidate RP with the higher priority will be elected as the RP. The range is 1 to 192 and the default priority is 192.

To delete the configuration of candidate PR, in the IPv6 PIM-SM configuration mode, use the following command:

no rp-candidate



Notes: When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is FF00::/8.

Configuring a Candidate BSR

In a PIM-SM domain, you need to configure one or more candidate BSR, and the BSR will be generated from the candidate BSR automatically. The BSR will collect and distribute the RP information.

To configure the candidate BSR, in the IPv6 PIM-SM configuration mode, use the following commands:

bsr-candidate *ipv6-address* [**priority** *level*]

- *ipv6-address* – Specifies the IPv6 address of the candidate BSR interface. The address cannot be the link-local address. The interface must be enabled with IPv6 PIM-SM.
- **priority** *level* – Specifies the priority (the higher the value, the higher the priority). If there is only one candidate BSR in the PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255, the default priority is 0.

To delete the configuration of candidate BSR, in the IPv6 PIM-SM configuration mode, use the following command:

no bsr-candidate



Notes: When a dynamic RP is used, the candidate RP and at least one candidate BSR must be configured in the IPv6 PIM-SM domain.

Configuring a Static RP

When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP, which can save the bandwidth occupied by message exchange between the Candidate RP and the BSR. In the IPv6 PIM-SM domain, the static RP configured on all the devices should be the same.

To specify the address of static RP, in the IPv6 PIM-SM configuration mode, use the following commands:

rp-address *ipv6-rp-address* [*ipv6_multicast_addr/length*]

- *ipv6-rp-address* – Specifies the IP address of the interface where the static RP resides. The address cannot be the link-local address.
- *ipv6_multicast_addr/length* – Specifies the multicast address.

To delete the configured static RP address, in the IPv6 PIM-SM configuration mode, use the following command:

no rp-address *ipv6-rp-address*[*ipv6_multicast_addr/length*]

Configuring the Switchover to SPT

Since the RPT (Rendezvous Point Tree) in the IPv6 PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.

Figure: Before RPT switch to SPT

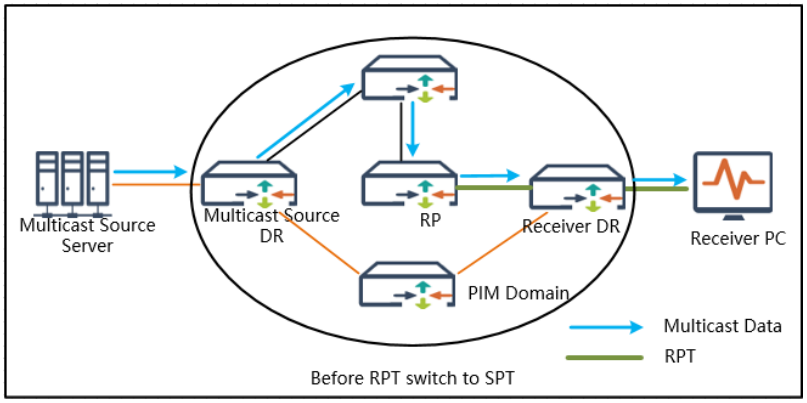
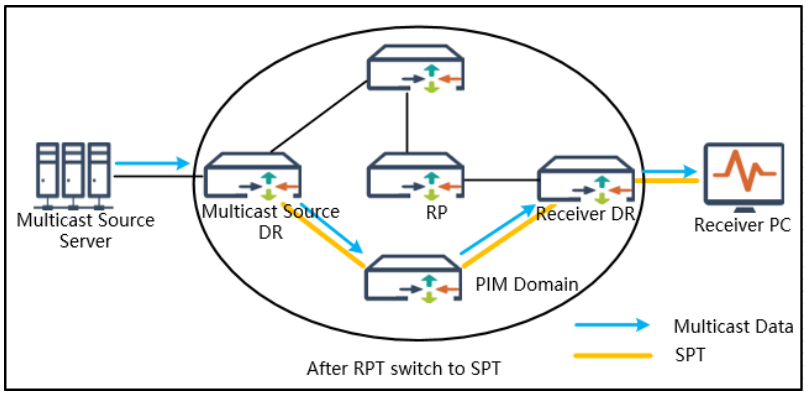


Figure: After RPT switch to SPT



To disable the switchover to SPT, in the IPv6 PIM-SM configuration mode, use the following commands:

spt-threshold infinity

To restore the switchover to SPT, in the IPv6 PIM-SM configuration mode, use the following commands:

no spt-threshold infinity

Configuring IPv6 PIM-SM for Interfaces

The IPv6 PIM-SM function for an interface must be configured in the interface configuration mode. The IPv6 PIM-SM configurations for the interfaces include:

- Enabling/Disabling the IPv6 PIM-SM for Interfaces
- Configuring the Priority of DR
- Specifying the Interval for Sending the Hello Packets
- Specifying the Interval for Sending MLD General Query Messages
- Specifying the MLD General Query Timeout
- Specifying the Maximum Response Time for MLD General Query

Enabling/Disabling the IPv6 PIM-SM for Interfaces

By default, the IPv6 PIM-SM function for interface is disabled. To enable or disable the IPv6 PIM-SM function for interface, in the interface configuration mode, use the following commands:

- Enable PIM-SM on the specified interface: **ipv6 pim sparse-mode**
- Disable PIM-SM on the specified interface: **no ipv6 pim sparse-mode**



Notes: The IPv6 PIM-SM function can be enabled only on the Layer 3 interface.

Configuring the Priority of DR

The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). To specify the priority of DR, in the interface configuration mode, use the following commands:

ipv6 pim dr-priority *level*

- *level* – Specifies the priority of the DR (the higher the value, the higher the priority). The default value is 1. The range is 0 to 4294967294. All routers in the IPv6 PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority of the routers is the same, the one with a large IP address will be selected.

To restore the default priority, in the interface configuration mode, use the command **no ipv6 pim dr-priority**.

Specifying the Interval for Sending the Hello Packets

After the IPv6 PIM-SM function is enabled on an interface, Hello packets will be sent periodically. You can specify the interval for sending Hello packets on the interface as needed. In the interface configuration mode, use the following command:

ipv6 pim hello-interval *interval*

- *interval* – Specifies the interval for sending Hello packets. The range is 1 to 3600, and the default interval is 30 seconds.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 pim hello-interval**.

Specifying the Interval for Sending MLD General Query Messages

The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain MLD group membership of the interface. On the Hillstone device, after the IPv6 PIM-SM function is enabled for the interface, the querier will send MLD general query messages to learn about the entry and exit of multicast group members.

To specify the interval for sending MLD general query messages, in the interface configuration mode, use the following command:

ipv6 pim mld query-interval *interval*

- *interval* – Specifies the interval for sending MLD general query messages. The range is 1 to 1800 seconds, and the default value is 125 seconds.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 pim mld query-interval**.

Specifying the MLD General Query Timeout

If the multicast router in the network does not receive MLD general query messages within the specified timeout period, multicast routers will elect a querier again.

To specify the MLD general query timeout value, in the interface configuration mode, use the following commands:

ipv6 pim mld query-timeout *timeout-value*

- *timeout-value* – Specifies the MLD general query timeout value. The range is 3 to 3620 seconds, and the default value is 260 seconds.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 pim mld query-timeout**.

Specifying the Maximum Response Time for MLD General Query

You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the MLD general query message twice and no response from the receiver host within the specified maximum response time, system will delete the receiver in the multicast routing table.

To specify the maximum response time, in the interface configuration mode, use the following commands:

ipv6 pim mld query-max-response-time *response-time*

- *response-time* – Specifies the maximum response time for MLD general query. The range is 1 to 32 seconds, and the default value is 10 seconds.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 pim mld query-max-response-time**.

Viewing IPv6 PIM-SM Information

To view the BSR information, in any mode, use the following command:

show ipv6 pim bsr-router[**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BSR information of VRouter.

To view the IPv6 PIM-SM interface information, in any mode, use the following command:

show ipv6 pim interface [*interface-name*]

- *interface-name* - Shows the PIM information of the specified interface.

To view the IPv6 PIM neighbor information, in any mode, use the following command:

show ipv6 pim neighbor [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the IPv6 PIM neighbor information of the specified VRouter.

To view the RP information, in any mode, use the following command:

show ipv6 pim rp [**vrouter** *vrouter-name* | **mapping** [**vrouter** *vrouter-name*]]

- *vrouter-name* - Shows the RP information of the specified VRouter.
- **mapping** [**vrouter***vrouter-name*] - Shows all RP mapping information of the specified VRouter.

To view the RPF information, in any mode, use the following command:

show ipv6 pim rpf*source-address* [**vrouter** *vrouter-name*]

- *source-address* – Shows the RPF information of the specified multicast source IP address.
- *vrouter-name* - Shows the RPF information of the multicast source IP address of the specified VRouter.

To view the MLD multicast group information, in any mode, use the following command:

show ipv6 pim mld groups [*group-address* [**vrouter** *vrouter-name*]]

- *group-address* – Shows the MLD multicast group information of the specified IP address.
- **vrouter** *vrouter-name* – Shows the MLD multicast group information of the specified VRouter.

To view the MLD interface information, in any mode, use the following command:

show ipv6 pim mld interfaces [*interface-name*]

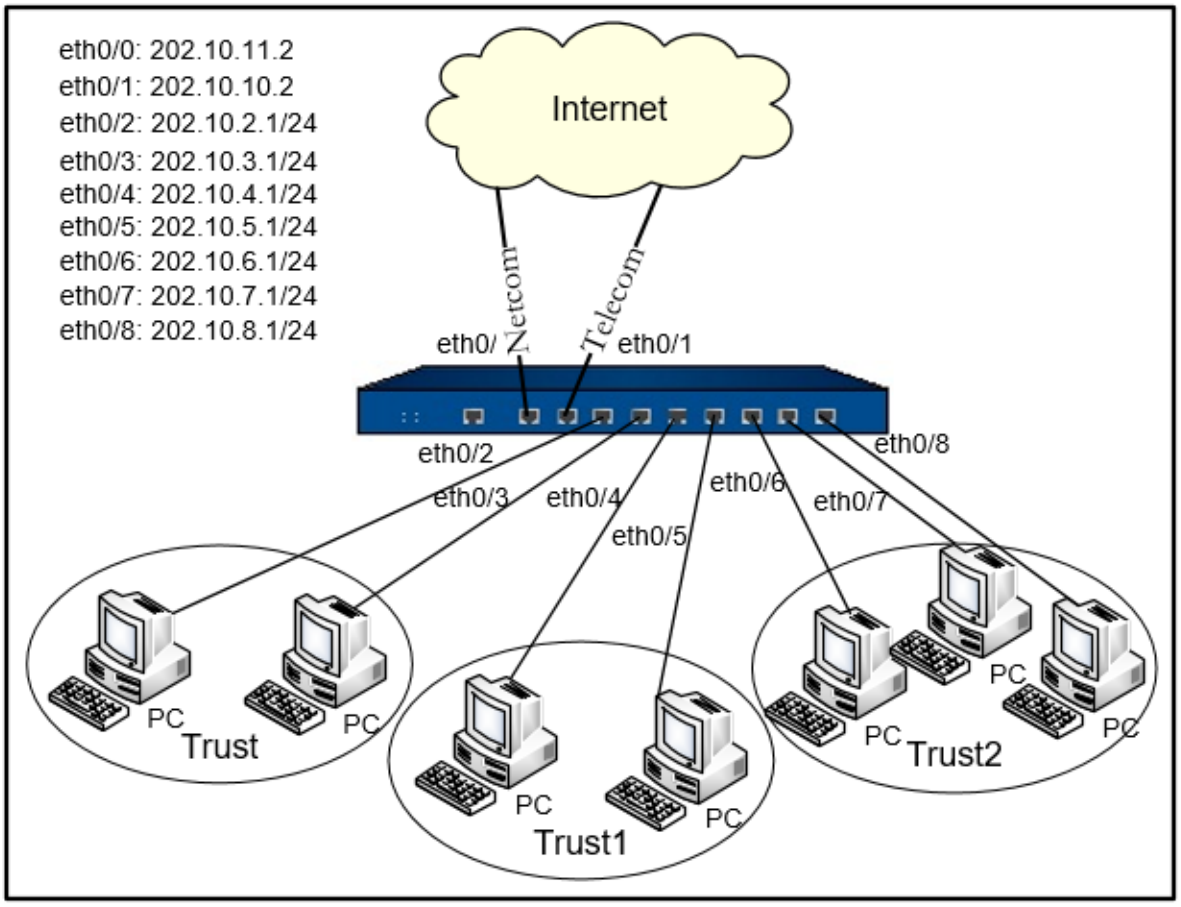
- *interface-name* – Shows the MLD information of the specified interface (the interface enabled with IPv6 PIM-SM).

Examples of Configuring Routes

This section describes several route-related configuration examples, including an enabling/disabling static route query configuration example, multi-VR configuration examples, a static multicast route configuration example, an IGMP Proxy configuration example and an inbound LLB configuration example.

Example of Configuring Static Route Query

The interface ethernet0/0 and ethernet0/1 of the device connect to ISP Netcom and Telecom respectively; the traffic from Trust and Trust1 in the Intranet goes to Netcom, and other traffic goes to Telecom. The network topology is shown below:



As shown above, etherent0/0 and ethernet0/1 belong to the untrust zone, and their IPs are 202.10.11.2 and 202.10.10.2 respectively; etherent0/2 and ethernet0/3 belong to the Trust zone, and their IPs are 202.10.2.1/24 and 202.10.3.1/24 respectively; etherent0/4 and ethernet0/5 belong to the Trust1 zone, and their IPs are 202.10.4.1/24 and 202.10.5.1/24 respectively; etherent0/6, ethernet0/7 and etherent0/8 belong to the Trust2 zone, and their IPs 202.10.6.1/24, 202.10.7.1/24 and 202.10.8.1/24 respectively.

Configuration Steps

Configurations of the security zones and interfaces are omitted. Only the configuration example of routes is as follows:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 202.10.10.2(the traffic from this segment goes to Telecom by default)
```

```
hostname(config-vrouter)# ip route source 202.10.2.1/24 202.10.11.2(the traffic from this segment goes to Netcom by default)
hostname(config-vrouter)# ip route source 202.10.3.1/24 202.10.11.2(the traffic from this segment goes to Netcom by default)
hostname(config-vrouter)# ip route source 202.10.4.1/24 202.10.11.2(the traffic from this segment goes to Netcom by default)
hostname(config-vrouter)# ip route source 202.10.5.1/24 202.10.11.2(the traffic from this segment goes to Netcom by default)
```

In the above source routing configuration, the traffic from the Trust and Trust1 zone will go to Netcom, while the traffic from other zones will go to Telecom. If the Netcom line fails for any reason, users in the Trust and Trust1 zones will not be able to access the Internet. In such a case only when all the above 4 source routes are deleted will the traffic be completely migrated to the Telecom line. If there are too many relevant source routes, the workload of deleting routes and then adding routes after troubleshooting will be very heavy; besides the trivial work also possibly leads to errors. The Hillstone' s solution is: when any line fails, disable the source route query, and then users in the Trust and Trust1 zones will use the default route and be able to access the Internet through the Telecom line. Use the following command:

```
hostname(config)# route disable sbr
```

After troubleshooting, to re-enable the source route query function, use the following command:

```
hostname(config)# hostname(config)# route enable sbr
```

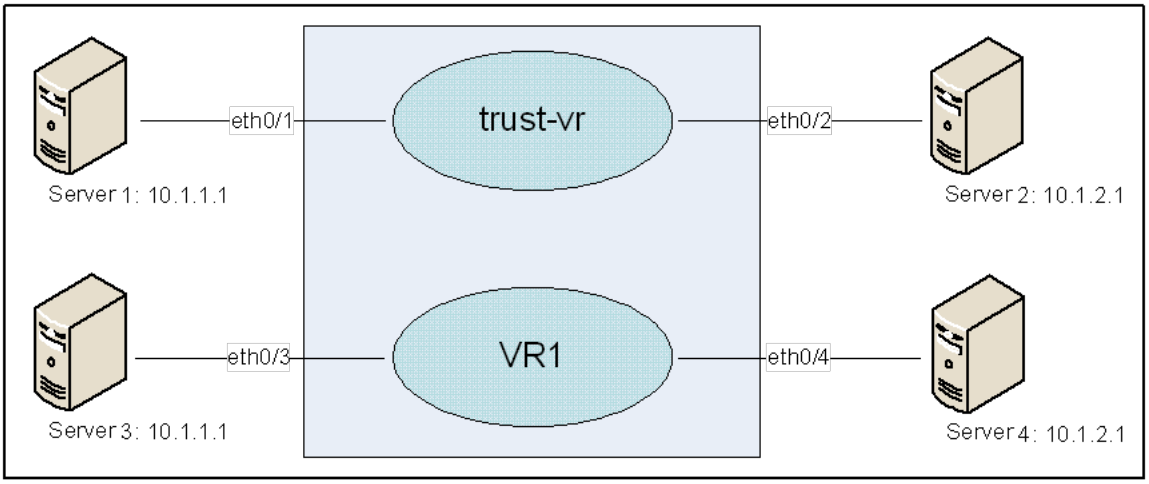
Example of Configuring Multi-VR

This section describes two multi-VR configuration examples, including:

- Independent multi-VR forwarding
- Inter-VR forwarding

Independent Multi-VR Forwarding

There are overlapped IP addresses in Trust-vr and VR1, but the data transmission of the two VRs should be independent, and should not affect each other. The network topology is shown below:



There are two VRs in the system: trust-vr and VR1. ethernet0/1 belongs to zone1, ethernet0/2 belongs to zone2, both zone1 and zone2 belong to trust-vr; ethernet0/3 belongs to zone3, ethernet0/4 belongs to zone4, belong zone3 and zone4 belong to VR1. The IP address of ethernet0/1 and ethernet0/3 is overlapped; the IP address of ethernet0/2 and ethernet0/4 is overlapped as well.

Configuration Steps

Step 1: Enable multi-VR on the device:

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
hostname# reboot
System reboot, are you sure? y/[n]: y
```

Step 2: After rebooting, create VR1:

```
hostname(config)# ip vrouter VR1
```

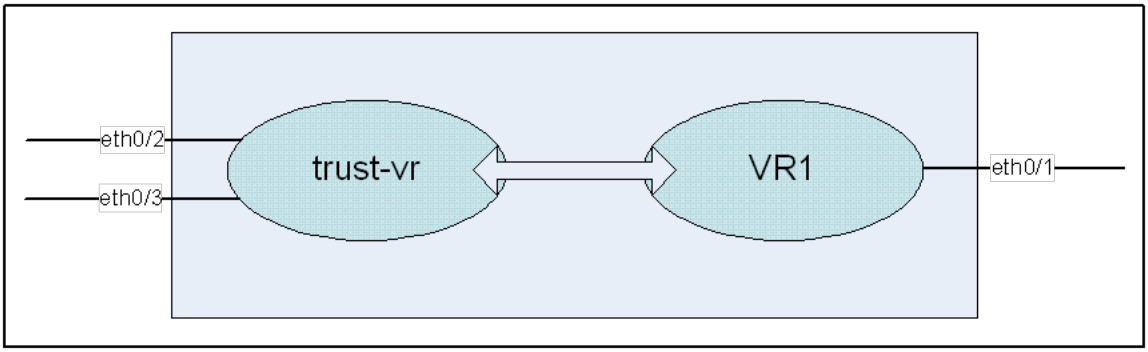
Step 3: Configure interfaces and security zones (by default zone1 and zone2 belong to trust-vr):

```
hostname(config)# zone zone1
```

```
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
hostname(config-zone-zone2)# exit
hostname(config)# zone zone3
hostname(config-zone-zone3)# vrouter VR1
hostname(config-zone-zone3)# exit
hostname(config)# zone zone4
hostname(config-zone-zone4)# vrouter VR1
hostname(config-zone-zone4)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 10.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.2.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone3
hostname(config-if-eth0/3)# ip address 10.1.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone zone3
hostname(config-if-eth0/4)# ip address 10.1.2.1/24
hostname(config-if-eth0/4)# exit
hostname(config)#
```

Inter-VR Forwarding

There are two VRs in the system: trust-vr and VR1. The goal is to allow trust-vr forwarding data through VR1. The network topology is shown below:



There are two VRs in the system: trust-vr and VR1. ethernet0/1 belongs to zone1, and zone1 belongs to VR1; ethernet0/2 and ethernet0/3 belong to zone2, and zone2 belongs to trust-vr. The following configuration example allows trust-vr to forward data through VR1.

Configuration Steps

Step 1: Enable multi-VR on the device:

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
hostname# reboot
System reboot, are you sure? y/[n]: y
```

Step 2: After rebooting, create VR1:

```
hostname(config)# ip vrouter VR1
```

Step 3: Configure interfaces and security zones (by default zone2 belongs to trust-vr):

```
hostname(config)# zone zone1
hostname(config-zone-zone1)# vrouter VR1
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
```

```
hostname(config-zone-zone2)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone2
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 4: Configure an inter-VR forwarding route:

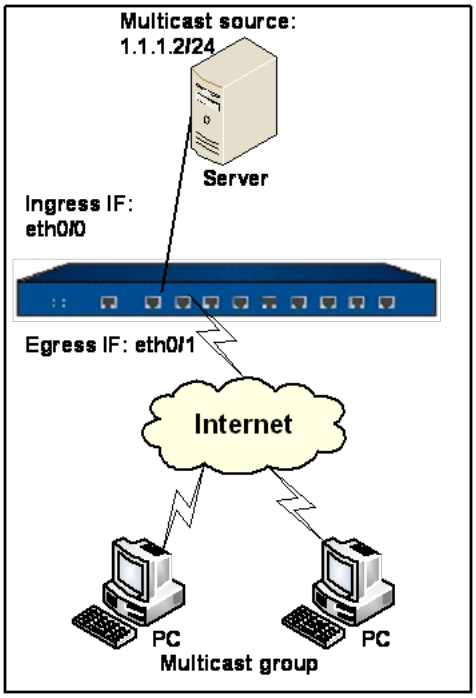
```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 vrouter VR1
hostname(config-vrouter)# exit
hostname(config)# ip vrouter VR1
hostname(config-vrouter)# ip route 10.1.1.0/24 vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.2.0/24 vrouter trust-vr
hostname(config-vrouter)# exit
hostname(config)#
```

Example of Configuring Static Multicast Route

This section describes a static multicast route configuration example.

Requirement

The multicast source sends data to multicast group. The multicast address is 224.91.91.2. Interface ethernet0/0, the ingress interface of the multicast data, belongs to the trust zone; ethernet0/1, the egress interface of the multicast data, belongs to the untrust zone. The goal is to configure a static multicast route so that the multicast data can be properly transmitted to the client PC that belongs to the multicast group. The network topology is shown below:



Configuration Steps

Step 1: Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.1.1.1/24
```

```
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Enable and configure a multicast route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# ip mroute 1.1.1.2 224.91.91.2 iif ethernet0/0 eif eth-
ernet0/1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
```

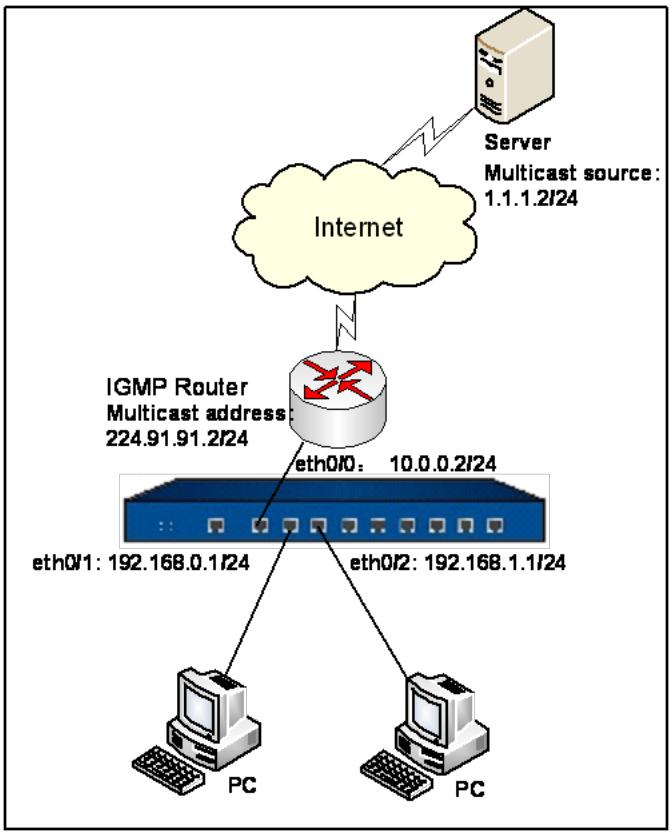
```
hostname(config)#
```

Example of Configuring IGMP Proxy

This section describes an IGMP Proxy configuration example.

Requirement

The multicast source sends data to the multicast group. The multicast address is 224.91.91.2. Interface ethernet0/0 is the upstream interface; ethernet0/1 and ethernet0/2 are the downstream interfaces. Configure an IGMP Proxy so that the multicast data can be properly forwarded to the client PC that belongs to the multicast group. The network topology is shown below:



Configuration Steps

Step 1: Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 10.0.0.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.0.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 192.168.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 2: Enable a multicast route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Enable and configure an IGMP Proxy:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip igmp-proxy enable
hostname(config-vrouter)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-proxy host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-proxy router-mode
```

```
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-proxy router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Example of Configuring IGMP Snooping

This section describes an IGMP Snooping configuration example.

Requirement

The multicast source sends data to the multicast group. The multicast address is 224.91.91.2. The device is working in the transparent mode. Interface ethernet0/0 is the upstream interface; ethernet0/1 and ethernet0/2 are the downstream interfaces. The goal is to configure IGMP snooping so that the multicast data can be properly forwarded to the client PC that belongs to the multicast group.

Configuration Steps

Step 1: Configure interfaces and security zones:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-untrust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone l2-trust
hostname(config-if-eth0/2)# exit
hostname(config)# interface vswitchif1
hostname(config-if-vsw1)# ip address 192.30.1.100 255.255.255.0
hostname(config-if-vsw1)# exit
hostname(config)#
```

Step 2: Enable a multicast route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
```

```
hostname(config)#
```

Step 3: Enable and configure IGMP Snooping:

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ip igmp-snooping enable
hostname(config-vswitch)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-snooping host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-snooping router-mode
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-snooping router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone l2-untrust
hostname(config-policy-rule)# dst-zone l2-trust
```

```
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

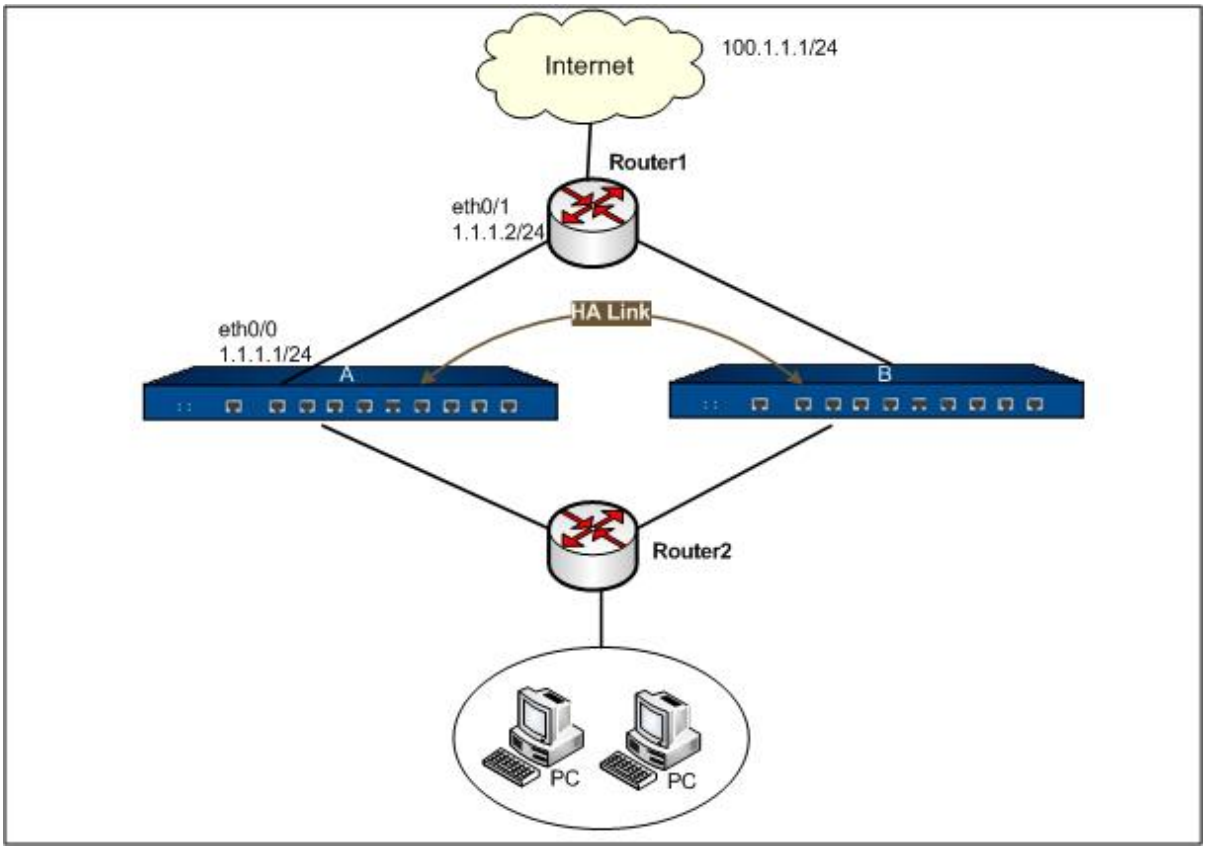
Example of Configuring BFD

This section lists three examples of configuring BFD as follows:

- Integrating BFD with the static route
- Integrating BFD with the OSPF route
- Integrating BFD with the BGP route

Requirement

The redundant link consists of two Hillstone devices and two routers. The BFD detection function is enabled between the routers and the Hillstone devices. The reachable network segment of Router1 is 100.1.1.1/24. The following examples individually integrate BFD with the static route, the OSPF route, and the BGP route between the Router1 and the device A. The network topology is shown in the figure below:



Configuration Steps

Integrating BFD with the Static Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A. The default detection method is asynchronous:

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# bfd min-tx 100 min-rx 100 detect-multiplier 3
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 3: Configure the device A to integrate BFD with the static route Router1:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 100.1.1.1/24 ethernet0/0 1.1.1.2 bfd
hostname(config-vrouter)# exit
hostname(config)#
```

Step 4: Configure the interface of Router1 and the BFD functions. The IP address of the interface is 1.1.1.2/24.

Integrating BFD with the OSPF Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A, specify the detection method as the inquiry method, enable the Echo function, and integrate BFD with the OSPF route:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
hostname(config-if-eth0/0)# ip ospf bfd
hostname(config)#
```

Step 3: Configure the OSPF route on the device A:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# network 1.1.1.1/24 area 0
hostname(config-router)# exit
hostname(config)#
```

Step 4: Configure the interface of Route1, BFD functions, and OSPF route. The IP address of the interface is 1.1.1.2/24. Use the inquiry method, enable the Echo function, and ensure the Echo packets can be forwarded.

Integrating BFD with the BGP Route

Step 1: Configure interfaces of the device A:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure the BFD session parameters on the interface of the device A, specify the detection method as the inquiry method and enable the Echo function.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 3: Configure the BGP protocol on the device A and integrate BFD with BGP:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router bgp 100
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# neighbor 1.1.1.2 fall-over bfd
hostname(config-router)# network 1.1.1.1/24
hostname(config-router)# exit
hostname(config)#
```

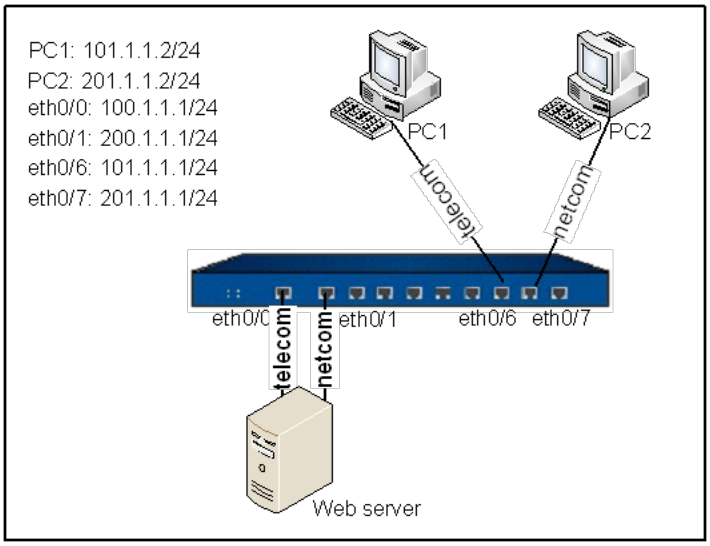
Step 4: Configure the interface of Route1, BFD functions, and BGP route. The IP address of the interface is 1.1.1.2/24. Use the inquiry method, enable the Echo function, and ensure the Echo packets can be forwarded.

Example of Configuring LLB

This section describes an inbound LLB configuration example.

Requirement

Ethernet0/6 and ethernet0/7 are connected to telecom and netcom links respectively. With inbound LLB enabled, the device will return the IP address defined in the ISP static address named telecom after receiving a DNS request from netcom users, and will return the IP address defined in the ISP static address named telecom after receiving a DNS request from telecom users. The network topology is shown below:



Configuration Steps

Configurations of interfaces are omitted. Only the configurations of ISP information and inbound LLB are provided.

Step 1: Configure ISP information:

```
hostname(config)# isp-network telecom
hostname(config-isp)# 101.1.1.0/24
hostname(config-isp)# exit
hostname(config)# isp-network netcom
hostname(config-isp)# 201.1.1.0/24
hostname(config-isp)# exit
```

Step 2: Enable SmartDNS and configure SmartDNS rules:

```
hostname(config)# llb inbound smartdns enable
hostname(config)# llb inbound smartdns test
hostname(config-llb-smartdns)# domain www.test.com
hostname(config-llb-smartdns)# ip 100.1.1.2 isp telecom interface ethernet0/0 weight
10
hostname(config-llb-smartdns)# ip 200.1.1.2 isp netcom interface ethernet0/0 weight
```

```
10
hostname(config-llb-smartdns)# exit
```

Step 3: Confirm the above configurations have taken effect by command show:

```
hostname(config)# show isp-network all
ISP telecom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
101.1.1.0/24
ISP netcom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
201.1.1.0/24
hostname(config)# show llb inbound smart test
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active;
I: inactive
==========================================================-
==========
----------------------------------------------------------
name: test
domain count: 1
rule count: 2
status: enable
domains: www.test.com;
ip addresses:
```

```
-------------------------------------------------------------------
ID IP ISP IF PROX TRACK W S
1 100.1.1.2 telecom ethernet0/0 D 10 A
3 200.1.1.2 netcom ethernet0/1 D 10 A
=================================================================
================
```

When PC1 requests www.test.com, the device will return the IP address for telecom link (100.1.1.2); when PC2 requests www.test.com, the device will return the IP address for netcom link (200.1.1.2).

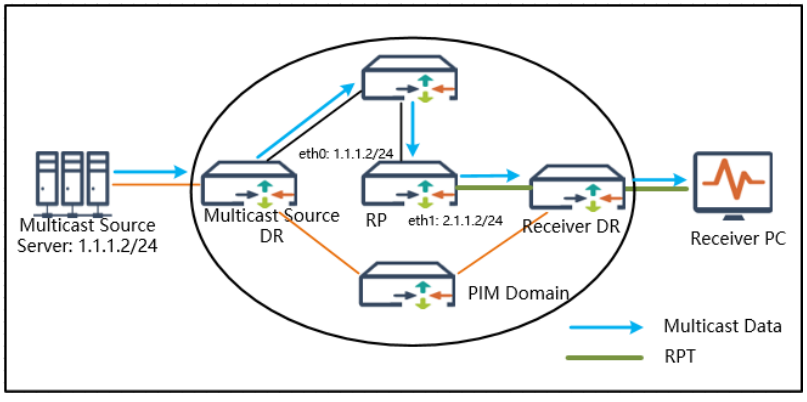
Example of Configuring PIM-SM

This section describes a PIM-SM configuration example.

Requirement

The multicast source sends data to the multicast group. The multicast address is 224.91.91.2. The receiver PC receives multicast data in the multicast mode, and the PIM domain adopts the SM mode. Assume that the device is the candidate RP, the interface loopback1 is used as the interface for electing RP, the interface ethernet0/0 is the upstream interface, and the interface ethernet0/1 is the downstream interface. After PIM-SM is configured, multicast data can be forwarded to the receiver PC. The network topology is shown below:

Figure : Network Topology of Configuring PIM-SM



Configuration Steps

Step 1: Enable a multicast route.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

Step 2: Enable and configure PIM-SM.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter))# router pim
hostname(config-vrouter)# pim-sm enable
hostname(config-vrouter)# rp-candidate loopback1
hostname(config-vrouter)# bsr-candidate loopback1
hostname(config-vrouter))# exit
hostname(config)#
```

Step 3: Configure the interface and enable the PIM-SM for the interface.

```
hostname(config)# interface loopback1
hostname(config-if-loo1))# zone trust
hostname(config-if-loo1)# ip address 2.2.2.2/24
hostname(config-if-loo1)# ip pim sparse-mode
hostname(config-if-loo1))# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.2/24
hostname(config-if-eth0/0)# ip pim sparse-mode
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# ip pim sparse-mode
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Chapter 4 System Management

This section contains the following contents:

- "Naming Rules" on Page 626
- "Configuring a Host Name" on Page 627
- "Configuring System Admin Users" on Page 629
- "Creating a Trusted Host" on Page 656
- "Configuring NetBIOS Name Resolution" on Page 659
- "Management of System User" on Page 661
- "Configuring a MGT Interface" on Page 680
- "Configuring a Storage Device" on Page 688
- "Managing Configuration Files" on Page 694
- "System Maintenance and Debugging" on Page 719
- "Rebooting the System" on Page 725
- "Upgrading StoneOS" on Page 727
- "SCM HA" on Page 751
- "Device HA Switchover When Switch Module failed" on Page 752
- "License Management" on Page 753
- "Simple Network Management Protocol (SNMP)" on Page 781
- "Network Configuration Protocol (NETCONF)" on Page 799
- "HSM Agent" on Page 802

- "Network Time Protocol (NTP)" on Page 806
- "Configuring Schedule" on Page 815
- "Configuring a Track Object" on Page 818
- "Configuring a Threshold" on Page 829
- "Monitor Alarm" on Page 831
- "CPU Cache Error Monitor" on Page 834
- "The Maximum Concurrent Sessions" on Page 835
- "Connecting to Hillstone Cloud Service Platform" on Page 848
- "Configuring Tab Title at WebUI Login" on Page 628
- "Configuring the system language" on Page 719
- "Configuring the RESTful API Interface to Upload Files" on Page 864
- "Clearing Alarm Status of Indicators" on Page 864
- "Specifying the Device as an SSH/Telnet Client" on Page 865
- "Switching the Working Mode of SIOM Module" on Page 867
- "Specifying the Maximum Retry Time for Configuration Deployment" on Page 868
- "Enabling/Disabling the Function of IP Fragmented Packets Reassembling in the IOM/SIOM Module" on Page 869

Naming Rules

When you name an object, follow the conventions below:

- Hillstone recommends you to not use the following special characters: comma (,), single quotation marks (‘ ‘), quotation marks (“”), tab, space, semicolons (;), backslash (\), slash (/), angle brackets (<>), and other special characters (&, #). It is recommend that you should use figures (0-9) and letters (a-z, A-Z) in the name.
- If an object name has space in it, you need to enclose the entire name in quotation marks when you use CLI, but this does not apply to WebUI operations.

Configuring a Host Name

A host name distinguishes one device from another. The default host name is the platform model.

To edit a host name, in the global configuration mode, use the following command:

hostname *host-name*

- *host-name* – Specifies the host name of the Hillstone device. You can specify up to 63 characters. After executing the command, the command prompt will be changed to the specified host name.

To restore to default value, in global configuration mode, use the command **no hostname**.

For example, the following commands change the host name to hillstone:

```
hostname# configure
hostname(config)# hostname hillstone
hillstone(config)#
```

Configuring the Displayable Length of the Host Name

You can configure the length of the host name that can be displayed by the system. The part of the host name exceeding the configured length will be displayed as "~" . To configure the displayable length of the host name, in the global configuration mode, use the following command:

hostname-display-length *length*

- *length* – Specifies the host name that can be displayed by the system. The length range is 1 to 63 characters. The default value is 16 characters, that is, when the length of the host name exceeds 16 characters, the exceeding part will be displayed as "~".

To restore to the default value, in the global configuration mode, use the following command:

no hostname-display-length

Viewing the Displayable Length of the Host Name

To view the displayable length of the host name, in any mode, use the following command:

show hostname-display-length

Configuring Tab Title at WebUI Login

At WebUI login, the browser tab title is "Hillstone Networks".

You can modify this title by configuring it as any one of the device's host name, model number and management address, or as a combination of any two or three items of them. The configuration will take effect at next-time WebUI login.

To configure the browser tab title at WebUI login, in the global configuration mode, use the following command:

webui-title-display-mode [**hostname**] [**platform**] [**manage-address**]

- **hostname** - Specifies the device's host name as the tab title.
- **platform**- Specifies the device' model number as the tab title.
- **manage-address** - Specifies the device' management address as the tab title.

If this command is executed with none of these items specified, or the tab title configuration is deleted, the default tab title will be displayed. If multiple items are specified, the sequence of the items is not limited. The sequence of the items displayed in the actual tab title is consistent with the configuration sequence.

To delete the tab title configuration, in the global configuration mode, use the following command:

no webui-title-display-mode

To view the tab title configuration, in any mode, use the following command:

show webui-title-display-mode

Configuring System Admin Users

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles.

By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: can write, execute and write the system. Administrator role can manage all functions of the device, view configurations and execute commands like import, export and save etc. under configuration mode.
- **admin-read-only**: can write and execute, view configurations, and execute export command under configuration mode.
- **operator**: can write, execute and write the system. Operator can modify settings others than administrator privileges, reboot the system, restore factory default and upgrade StoneOS, view configurations, but operators cannot view log messages, and execute some commands.
- **auditor**: can manage log messages, including view, export and clear logs. The table lists admin user's permissions.

Operation	Permissions			
	Administrator	Administrator-read-only	Operator	Auditor
Configure (including save configuration)	√	χ	√	χ
Managing admin users	√	χ	χ	χ
Restore factory default	√	χ	χ	χ
Delete configuration file	√	χ	√	χ

Operation	Permissions			
	Administrator	Administrator-read-only	Operator	Auditor
Roll back configuration	√	χ	√	χ
Reboot	√	χ	χ	χ
View configuration information	√	√	√	χ
View log information	√	√	χ	√
Modify current admin password	√	√	√	√
Command import	√	χ	√(except upgrading StoneOS)	χ
Command export	√	√	χ	√
Command clear	√	√	√	√
Command ping/traceroute	√	√	√	χ
Command debug	√	√	√	χ
Command exec	√	√	√	√
Command terminal width	√	√	√	√

- The system has a default administrator “hillstone”. This default administrator can be edited.
- Except administrator, other roles cannot edit properties of a system admin user, but only its own password.
- Auditor can manage one or more log messages, but an auditor’s log types are defined by users of administrator role.

The property settings of a system administrator are:

- Creating administrator roles
- Specifying administrator role's privileges
- Specifying administrator role's description
- Creating an admin user
- Assigning a role
- Configuring password
- Configuring accesses for admin users
- Configuring Single Sign-on (SSO)
- Configuring two-factor authentication for admin users logging in to the WebUI
- Configuring an API token for an admin user
- Configuring log types for auditors
- Specifying login limit
- Configuring Login Options for the Default Administrator
- Viewing Admin roles
- Viewing admin users
- VSYS admin users

Creating Administrator Roles

To create a new administrator role, use the following command in the global configuration mode:

admin role *role-name*

- *role-name* – Specifies the name of the administrator role. The length varies from 4 characters to 95 characters. After executing this command, the system will create the administrator role

and enter the administrator role configuration mode. If the name already exists, it will enter the administrator role configuration mode directly.

To delete an administrator role, use the **no admin role** *role-name* command.

Specifying Administrator Role's Privileges

To specify the administrator role's privileges of CLI, use the following command in the administrator role configuration mode:

cli-privilege all {**rw** | **none**}

- **rw** | **none** – **rw** represents the administrator role has the read-write privilege to all CLI commands. **none** represents the administrator role does not have privilege of CLI and cannot use CLI.

Specifying Administrator Role's Description

To specify administrator role's description, use the following command in the administrator role configuration mode:

description *description*

- *description* – Specify the description for the administrator role. You can specify up to 255 characters.

Use the **no description** command to delete the description.

Creating an Admin User

To create an admin user and enters its configuration mode, under global configuration mode, use the following command:

admin user *user-name*

- *user-name* - Specifying a name for the admin user. The length is from 4 to 31 characters. This command not only creates the admin user, also enters the user's configuration mode; if the admin user exists, it enters its configuration mode directly.

To delete an admin user, under global configuration mode, use the command **no admin user** *user-name*.

When you are under an admin user's mode, you can edit its role, password, access methods and log types (for auditor roles).

Assigning a Role

To assign a role for an admin user, in the user's configuration mode, use the following command:

role {**admin** | **operator** |**auditor** |**admin-read-only**}

- **admin** - Specifying the role of this user as an Administrator.
- **operator** - Specifying the role of this user as an Operator.
- **auditor** - Specifying the role of this user as an Auditor.
- **admin-read-only** - Specifying the role of this user as an Administrator-read-only.

Configuring Password

Password is required for an admin account. To define a password, in the admin user's configuration mode, use the following command:

password *password*

- *password* – Specify a password for admin user. The length is from 4 to 31 characters.

To cancel a password, under the admin user's configuration mode, use the command **no password**.

If you login as an operation, auditor or administrator-read-only, you can edit your own password under any mode:

exec admin user password update *password*

- *password* – Enter the new password. The length is from 4 to 31.



Notes: If you use an Administrator account, you have the privilege to edit the password of every user.

Configuring Password Policy for Admin Users

Password policy defines admin user's password complexity. The password complexity controls the total length of the password, the length of each element, and the validity period of the password. A password can be a combination of elements from the following types:

- Capital letters A to Z.
- Lowercase letters a to z.
- Figures 0 to 9.
- Other visible characters such as semicolon, slash(only support DBC case).

You must enter the password policy mode before you can change the complexity requirement. Use the command **password-policy** to enter password policy configuration mode.

You can set the password complexity if the default-settings can not fit the security requirement. You must enable password complexity checking before setting the password complexity.

To enable or disable password complexity checking, in password policy configuration mode, use the following command:

admin complexity {**enable** | **disable**}

- **enable** | **disable** – Enable or disable password complexity checking. By default, the password complexity checking is disabled. After the feature is enabled, the default complexity requires that the password must contain all the four types of formats: two uppercase letters, two lowercase letters, two figures and two other visible characters (e.g.@).

To define the length of password elements, in password policy configuration mode, use the following command:

admin {**capital-letters** | **non-alphanumeric-letters** | **numeric-characters** | **small-letters**} *value*

- **capital-letters** *value* – Specify the length of capital letters in password. The default value is 2 and the range is 0 to 16.
- **non-alphanumeric-letters** *value* – Specify the length of visible characters except letters and figures in password. The default value is 2 and the range is 0 to 16.
- **numeric-characters** *value* – Specify the length of figures in password. The default value is 2 and the range is 0 to 16.
- **small-letters** *value* – Specify the length of lowercase letters in password. The default value is 2 and the range is 0 to 16.

To define the minimum length of password for the admin users, in password policy configuration mode, use the following command:

admin min-length *length-value*

- **min-length** *length-value* – Specify the minimum length of the password. The default value is 4, and the range is 4 to 16. After password complexity checking is enabled, the default value is 8(two uppercase letters, two lowercase letters, two figures and two other visible characters), and the range is 8 to 16.



Notes: You can define the minimum length of the password in order to strengthen the security whether the password complexity checking is enabled or not.

The validity period of the password is used to limit the time that you use password. When you log in, if the entered password has expired, the system will prompt to reset the password. After pressing Enter, please enter the new password again. If the new password does not meet the password complexity requirements or the new passwords for the two times are not consistent, you need to re-input. Given that continuous input for three times does not meet the requirement of the password, you can not connect to the device. You are still required to set a new password when logging in again. The new password can be the same as the old one.

To define the validity period of the password for the admin users, in password policy configuration mode, use the following command:

admin password-expiration *value*

- **password-expiration** *value* – Specifies the validity period of the password. The unit is day. The range is 0 to 365. The default value is 0, which indicates that there is no restriction on validity period of the password.

In the password policy configuration mode, use the command **no admin complexity** to resume the default setting of password complexity checking.

To enable or disable the History Password Check function, in the password policy configuration mode, use the following command:

admin history-password-check {**enable** | **disable**}

- **enable | disable** – Enable or disable the History Password Check function. By default, this function is disabled.

With the History Password Check function enabled, when you change your password, the system verifies whether the new password is the same as the historical password. The new password cannot be the same as the specified numbers of historical passwords. To configure the History Password Check function, in the password policy configuration mode, use the following command:

admin history-password-records*count*

- *count* - Specifies the number of historical passwords to be verified. The value rage is from 3 to 8. The default value is 5, indicating that the new password cannot be the same as the last five historical passwords.

Viewing Password Policy for Admin Users

To view password policy for admin users, in any mode, use the command:

show password-policy

Configuring the Function of Resetting the Administrator Password by Security Question

The function of resetting the administrator password by security question enables you to change passwords through security question. You can easily reset the password without knowing the previous password. If this function is configured and enabled, when you enter the wrong username or password for three consecutive times through the console port, the system will prompt you to reset the password by the security question.

To configure the security question, in the global configuration mode, use the following commands:

admin reset-password question {**custom***value* | **predefined** {**question1** | **question2** | **question3**}}

- **question custom** *value* – Specifies the user-defined question, which can only include letters, numbers, and special characters (excluding "). Chinese characters cannot be included in the security question. When you enter a string, add double quotations to the value. The value range is 1 to 256 characters.
- **question predefined question1** – Specifies predefined question 1 as the security question. Question1 is "What is your aspiration?" .
- **question predefined question2** – Specifies predefined question 2 as the security question. Question2 is "What is your most impressed day?".
- **question predefined question3** – Specifies predefined question 3 as the security question. Question3 is "What do you like best?".

To configure the security answer, in the global configuration mode, use the following command:

admin reset-password answer *value*

- **answer** *value* – Specifies the security answer, which can only include letters, numbers, and special characters (excluding "). Chinese characters cannot be included in the security question. When you enter a string, add double quotations to the value. The value range is 1 to 256 characters.

To enable/disable the function of resetting the administrator password by security question, in the global configuration mode, use the following commands:

admin reset-password {enable | disable}

- **enable** − Enables the function of resetting the administrator password by the security question. To enable the function, you need to configure the security question and its answer first.
- **disable** − Disables the function of resetting the administrator password by the security question.

To delete the security question and its answer, in the global configuration mode, use the following commands:

no admin reset-password {question | answer}

- **question** − Deletes the security question and its answer at the same time. To perform this operation, you need to disable the function of resetting the administrator password by security question first.
- **answer** − Deletes the security answer only. To perform this operation, you need to disable the function of resetting the administrator password by security question first.

To view the information about the function of resetting the administrator password by security question, including the enabled/disabled status of the function, the content of the security question, and the security answer, in any mode, use the following command:

show admin reset-password

Configuring Accesses for Admin Users

By default, a newly created admin user does not have its access opened to visit the device. To add accesses for an admin user, in the user's configuration mode, use the following command:

access {console | http | https | ssh | telnet | netconf | any}

- **console** − Allows the admin user to use Console port to access the device.
- **http** − Allows the admin user to use HTTP to access the device.

- **https** – Allows the admin user to use HTTPS to access the device.
- **ssh** – Allows the admin user to use SSH to access the device.
- **telnet** – Allows the admin user to use TELNET to access the device.
- **netconf** – Allows the admin user to use NETCONF to access the device.
- **any** – Allows the admin user to use any of the above methods to access the device.

Use this command to add access for admin user.

To cancel the specified access, in the user's configuration mode, use the command **no access** {**console** | **http** | **https** | **ssh** | **telnet** | **netconf** | **any**}.



Notes: When the "Telnet" or "HTTP" login type is enabled, the system will prompt the protocols are not secure.

Configuring Single Sign-on (SSO)

Single Sign-on (SSO) is supported only by virtual product -CloudEdge. This function is disabled by default and can be enabled as required. By enabling this function and specifying the SSO scheme of a third-party platform on CloudEdge, you can access CloudEdge without authentication after logging in to that third-party platform. The system supports three SSO schemes:

- By specifying the SSO scheme as CAS_QIMING, you can log in to the CloudEdge without authentication after logging in to the Venustech CSMP
- By specifying the SSO scheme as CTYUN, you can log in to the CloudEdge without authentication after logging in to the e Cloud.
- By specifying the SSO scheme as 360-YUNZHEN, you can log in to the CloudEdge without authentication after logging in to the 360 CSMP.

Enabling/Disabling SSO

To enable or disable the SSO function, in the global configuration mode, use the command:

Enable: **admin sso-login enable**

Disable: **admin sso-login disable**



Notes: When configuring SSO, the system time of the third-party platform and the CloudEdge must be consistent. The time difference of this two parties cannot exceed 10 minutes, otherwise the SSO will fail.

After enabling the SSO function, you need to specify one of the following SSO schemes of a third-party platform: CAS_ QIMING, CTYUN and 360_YUNZHEN.

Specifying the SSO scheme as CAS_QIMING

To specify the SSO scheme as CAS_QIMING, in the global configuration mode, use the command:

admin sso-login type cas-qiming

After specifying the SSO scheme as CAS_QIMING, you need to specify the Service Ticket check URL and the virtual router where the third-party SSO passes.

- To specify the Service Ticket check URL , in the CAS_QIMING SSO mode, use the following command:

  ticket-check-url *url*

- To specify the virtual router where the third-party SSO passes, in the SSO mode, use the following command:

  vrouter *vrouter-name*

Specifying the SSO Scheme as CTYUN

To specify the SSO Scheme as CTYUN, in the global configuration mode, use the following command:

admin sso-login type ctyun

Viewing/Deleting the Token Information of CTYUN

This function can be used only in CTYUN SSO. The system allows you to view or delete the Token information of the administrator. Token information is used for authentication during SSO.

To view the administrator's Token information, in the global configuration mode, use the command:

show admin sso-token type ctyun

To delete the administrator's Token information, in the global configuration mode, use the command:

exec admin sso-token-del type ctyun owner *username*

- *username* – Specifies the username of the administrator whose Token information needs to be deleted.

Specifying the SSO Scheme as 360_YUNZHEN

To specify the SSO scheme as 360_YUNZHEN, in the global configuration mode, use the command:

admin sso-login type 360-yunzhen

Viewing the Token Information of 360_YUNZHEN

This function can be used only in 360_YUNZHEN SSO. The system allows you to view the Token information of the administrator. Token information is used for authentication during SSO.

To view the administrator's Token information, in the global configuration mode, use the command:

show admin sso-info type 360-yunzhen

Viewing the SSO Information

To view the SSO infomation , in any mode ,use the following command:

show http

Configuring Two-factor Authentication for Admin Users Logging in to the WebUI

An administrator can log in to the WebUI by using SMS/Email two-factor authentication.

Enabling SMS/Email Two-factor Authentication

To configure SMS/Email two-factor authentication, in global configuration mode, use the following command:

admin {**sms-auth** [**gateway** *provider-name* | **modem**] | **email-auth** [**smtp** *smtp-name*] | **verification-timeout** *timeout* | **auth-sender** *sender-name*}

- **sms-auth** – Enables the SMS authentication. After the SMS authentication is enabled, the administrator who does not configure the mobile number will be unable to log in to the device.
- **gateway***provider-name* – Sets the method of the SMS authentication to SMS gateway.
- **modem** – Sets the method of the SMS authentication to SMS modem.
- **email-auth** – Enables the Email authentication. After the Email authentication is enabled, the administrator who does not configure the email address will be unable to log in to the device.
- **smtp***smtp-name* – Specifies the mail server.
- **verification-timeout***timeout* – Specifies the validity period of SMS/email verification codes. Valid values: 1 to 30 minutes. Default value: 5 minutes. You cannot log in to the device if you do not enter the verification code within the validity period.
- **auth-sender***sender-name* – Specifies the sender name, which can be 1 to 64 characters. The name will be displayed in the text message/email.

In global configuration mode, use the **no admin sms-auth** command to disable the SMS authentication.

In global configuration mode, use the **no admin email-auth** command to disable the Email authentication.



Notes: You cannot enable the SMS/Email authentication and SSO from a third-party platform at the same time.

Configuring the Mobile Number for an Administrator

After the SMS authentication is enabled, an administrator is required to pass a multi-factor authentication by using a verification code. The administrator who does not configure the mobile number will be unable to log in to the WebUI of the device. To configure the mobile number, in administrator configuration mode, use the following command:

phone *phone-number*

- *phone-number* – Specifies the mobile number of the administrator.

Configuring the Email Address for an Administrator

After the Email authentication is enabled, an administrator is required to pass a multi-factor authentication by using an email verification code. The administrator who does not configure the email address will be unable to log in to the WebUI of the device. To configure the email address, in administrator configuration mode, use the following command:

email *email*

- *email* – Specifies the email address of the administrator.

Configuring an API Token for an Administrator

After you enable the SMS/Email authentication, the administrator can only use the API token authentication when logging in to the device by using RESTful API. You can create an API token for a specified administrator and update, renew, clear, enable, and disable the API token.

Creating an API Token

To create an API token, in administrator configuration mode, use the following command:

api-token create – By default, the newly created API token is enabled.

Changing the Validity Period of the API Token

To change the validity period of the API token, in administrator configuration mode, use the following command:

api-token expiration*expiration-time*

- *expiration-time* – Changes the validity period of the API token. Valid values: 0 to 365 days. Default value: 60 days. The value 0 indicates that the API token is valid for a long term.

Updating the API Token

After an administrator updates the API token, the original API token immediately becomes invalid. The validity period of the newly generated API token will be recalculated. To update the API token, in administrator mode, use the following command:

api-token update

Renewing the API Token

An administrator can renew the API token in the enabled or expired state. The value of the API token does not change after the renewal. The validity period of the API token will be recalculated.

api-token renewal

Enabling the API Token

An administrator can enable the API token. The validity period of the API token will be recalculated. For example, if the original validity period is 30 days, the validity period will become 30 days again after you enable this API token. To enable the API token, in administrator configuration mode, use the following command:

api-token enable

Disabling the API Token

An administrator can disable the API token. If needed, the administrator can use this API token again by using the **enable** command. To disable the API token, in administrator configuration mode, use the following command:

api-token disable

Deleting the API Token

An administrator can delete the API token. To do this, use the following command:

api-token delete

Viewing API Token

You can use the show command in any mode to view the API token of a specified administrator:

show admin api-token *user-name*

Example:

```
hostname(config)# show admin api-token test
=============================================================
====
API Token: (Displays the API token value, which is used to log in to RESTful API) ewoJInR5cCI6CSJKV1QiLAoJImFsZyI6CSJTSEEyNTYiCn0-
=.ewoJInVzZXJuYW1l-
IjoJInRl-
c3QiLAoJInZzeXN-
faWQiOgk-
wCn0-
=.$020100rE$cmWWDXrSBhBtQvY+Pco1mSf-
fmhmICNk7NKAhxeS08wX/Kb08=
Begin Time: 2022-11-17 21:08:42(Displays the point in time when the API token takes effect)
Expiration: 60 days(Displays the validity period of the API token)
Time To Expiration: 60 days(Displays the remaining days of the API token)
Current status: normal(Displays the current status of the API token. The value normal indicates that the API token is enabled.)
=============================================================
```

```
====
```

Configuring Log Types for Auditors

An admin user of auditor role is only allowed to view, export and clear log messages. The log types that can be visited by auditor is also defined by Administrator. To specify the log types, under auditor's configuration mode, use the command:

log {config | event | nbr | threat | sandbox | network | operation | iot-monitor | share-access-detect | endpoint-tag| session | nat | urlfilter| pbr| dlp | cf| nbc | traffic | ips}

- **config** – Specifies that the auditor can manage configuration logs.
- **event** – Specifies that the auditor can manage event logs.
- **nbr** – Specifies that the auditor can manage NBR logs.
- **network** – Specifies that the auditor can manage network logs.
- **iot-monitor** – Specifies that the auditor can manage IoT monitor logs.
- **threat** – Specifies that the auditor can manage threat logs.
- **sandbox** – Specifies that the auditor can manage sandbox logs.
- **share-access-detect** – Specifies that the auditor can manage share access logs.
- **operation** – Specifies that the auditor can manage operation logs.
- **endpoint-tag** – Specifies that the auditor can manage endpoint tag logs.
- **session** – Specifies that the auditor can manage session logs.
- **nat** – Specifies that the auditor can manage NAT logs.
- **urlfilter** – Specifies that the auditor can manage URL filter logs.
- **pbr** – Specifies that the auditor can manage PBR logs.
- **dlp** – Specifies that the auditor can manage DLP logs.

- **cf** – Specifies that the auditor can manage CF logs.
- **nbc** - Specifies that the auditor can manage NBC logs.
- **traffic** - Specifies that the auditor can manage IPS logs.
- **ips** - Specifies that the auditor can manage IPS logs.

Repeat this command to spcify more than one log types.

To cancel access to a log type, use the command **no log** {**config** | **event** | **nbr** | **threat** | **sandbox** | **network** | **operation** | **iot-monitor** | **share-access-detect** | **endpoint-tag** | **session** | **nat** | **url-filter** | **pbr**| **dlp** | **cf**| **nbc** | **traffic** | **ips**}.

Specifying Login Limit

If an admin user failes to enter correct password for the specified times, the IP or user account will be disallowed to login again within the specified duration.

To specify a lockout duration of IP, under global configuration mode, use the following command:

admin lockout-duration *time*

- **lockout-duration** *time* – Specifying lockout duration. The unit is minute. The length is 1 to 65525. The default value is 2.

Use the command **no admin lockout-duration** to resume to the default value.

To specify a lockout duration of user account, under global configuration mode, use the following command:

admin lockout-duration-user *time*

- **lockout-duration-user** *time* – Specifying lockout duration. The unit is minute. The length is 1 to 65525. The default value is 2.

Use the command **no admin lockout-duration-user**to resume to the default value.

To specify the maximum login failure time of IP, under the global configuration mode, use the command:

admin max-login-failure *times*

- **max-login-failure** *times* – Specify the maximum error password times. The default value is 3, and the range is 1 to 256.

Use the command **no admin max-login-failure** to resume to the default failure time.

To specify the maximum login failure time of user account, under the global configuration mode, use the command:

admin max-login-failure-user *times*

- **max-login-failure-user** *times* – Specify the maximum error password times. The default value is 3, and the range is 1 to 5.

Use the command **no admin max-login-failure-user** to resume to the default failure time.



Notes: This command is available only for admin user of administrator role.

Configuring the Maximum Number of Admin Users

You can configure the maximum number of admin users. After configuring, the admin users that you can create at most will be the specified number. You can adjust it as needed. If the maximum is adjusted, only you restart device can the specified value take effect. To configure the maximum number of admin users, in the global configuration mode, use the following commands:

capacity management max-administrative-users*capacity-num*

- *capacity-num* - Specify the maximum number of admin users, ranging from 1 to 128.

Use the command **no capacity management max-administrative-users** to resume to the default value . The default value verifies on different pflatform.



Notes: This command is a local configuration command and does not support HA synchronization. In HA environment, if the maximum number of admin users set on the master device is different from that on the backup device, the HA status may be normal, while system will prompt an alarm regularly.

Configuring Login Options for the Default Administrator

System has a default administrator "hillstone" and a default password "hillstone". However, there is a risk that the default username and password may be cracked. To avoid that risk, when you logs in with the default username and password for the first time, the system will prompt to change the default password. Then, you can log in again with the new password.

```
Administrator is logging in with default account and password:
Please change your password:
new password: ******  (Enter the new password)
Please input the new password again
new password: ******  (Enter the new password again)
```



Notes: In the HA Active-Passive (A/P) mode, the backup device does not support this function, and you can log in with the default username and password.

Enabling Telnet/HTTP Login Type for the Default Administrator

By default, The Telnet and HTTP login types for the default administrator "hillstone" are disabled. To enable the Telnet or HTTP login type for the default administrator, refer to Configuring Accesses for Admin Users.

Viewing Admin roles

To show admin roles: **show admin role** [*role-name*]

Viewing Admin Users

To view admin users, under any mode, use the command:

- To show admin users: **show admin user**
- To show details of an admin user: **show admin user** *user-name*
- To show lockout duration: **show admin lockout-duration**

- To show maximum login failure time: **show admin max-login-failure**
- To show the SMS and Email authentication configuration of admin users: **show admin multiple-factor-auth**

Example:

```
hostname(config)# show admin multiple-factor-auth
=============================================================
Multiple-factor-auth status: sms(Displays the status of two-factor authentication. The value sms indicates that the SMS authentication is enabled and the value email indicates that the Email authentication is enabled.)
Sender name: (Displays the sender name of the text message/email)
Verify code timeout: 5 (minutes) (Displays the validity period of SMS/e-mail verification codes)
SMS config: (Displays the configuration of the SMS authentication)
-----------------------------------------
SMS agent: gateway(Displays the method of the SMS authentication)
SMS service provider: 11(Displays the service provider of the SMS gateway)
Email config: (Displays the configuration of the email authentication)
-----------------------------------------
Email server name: (Displays the name of the mail server)
=============================================================
```

VSYS Admin Users

The admin users of each VSYS are independent from other VSYS. VSYS admin users also have different roles of Administrator, Administrator-ready-only, operator and auditor. Their roles and previleges are the same with normal admin users.

When creating VSYS administrators, you must follow the requirements listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into non-root VSYS.
- After logging into root VSYS, the root administrators can switch to non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after the successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in the format of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The table lists VSYS admin user’s permissions.

Operation	Permissions							
	Root VSYS Administrator	Root VSYS Administrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Administrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including save configuration)	√	χ	√	χ	√	χ	√	χ
Managing admin users	√	χ	χ	χ	√	χ	χ	χ

Operation	Permissions							
	Root VSYS Admin-isrator	Root VSYS Admin-isrator-read-only	Root VSYS Oper-ator	Root VSYS Aud-itor	Non-root VSYS Admin-isrator	Non-root VSYS Admin-isrator-read-only	Non-root VSYS Oper-ator	Non-root VSYS Aud-itor
Restore fact-ory default	√	χ	χ	χ	χ	χ	χ	χ
Delete con-figuration file	√	χ	√	χ	√	χ	√	χ
Roll back configuration	√	χ	√	χ	√	χ	√	χ
Reboot	√	χ	√	χ	χ	χ	χ	χ
View con-figuration information	√	√	√	χ	View info in current VSYS	View info in current VSYS	View info in current VSYS	χ
View log information	√	√	χ	√	√	√	χ	√
Modify cur-rent admin password	√	√	√	√	√	√	√	√
Command import	√	χ	√	χ	√	χ	√	χ
Command export	√	√	√	√	√	√	√	√

Operation	Permissions							
	Root VSYS Admin-isrator	Root VSYS Admin-isrator-read-only	Root VSYS Oper-ator	Root VSYS Aud-itor	Non-root VSYS Admin-isrator	Non-root VSYS Admin-isrator-read-only	Non-root VSYS Oper-ator	Non-root VSYS Aud-itor
Command clear	√	√	√	√	√	√	√	√
Command ping/tracero-ute	√	√	√	χ	√	√	√	χ
Command debug	√	√	√	χ	χ	χ	χ	χ
Command exec	√	√	√	√	√	√	√	√
Command terminal width	√	√	√	√	√	√	√	χ

Logging in to the Device by Using the API Token

The administrator can use the user name and password or API token authentication when logging in to the device by using RESTful API. You can create an API token for a specified administrator and update, renew, clear, enable, and disable the API token.

Notes: After you enable the SMS or Email authentication, the administrator can only use the API token authentication when logging in to the device by using RESTful API.

Creating an API Token

To create an API token, in administrator configuration mode, use the following command:

api-token create – By default, the newly created API token is enabled.

Changing the Validity Period of the API Token

To change the validity period of the API token, in administrator configuration mode, use the following command:

api-token expiration *expiration-time*

- *expiration-time* – Changes the validity period of the API token. Valid values: 0 to 365 days. Default value: 60 days. The value 0 indicates that the API token is valid for a long term.

Updating the API Token

The administrator can update the API token value as required. After the API token is updated, the original API token immediately becomes invalid. The newly generated API token recalculates the expiration time based on the current time and validity period. To update the API token, in administrator mode, use the following command:

api-token update

Renewing the API Token

An administrator can renew the API token in the enabled or expired state. The value of the API token does not change after the renewal. The API token recalculates the expiration time based on the current time and validity period. For example, if the validity period of the administrator "test" is 10 days, the current date November 17, 2022, and the expiration date November 25, 2022, the expiration date will be renewed to November 27, 2022 after the renewal.

api-token renewal

Enabling the API Token

An administrator can enable the API token. The validity period of the API token will be recalculated. For example, if the original validity period is 30 days, the validity period will become 30

days again after you enable this API token. To enable the API token, in administrator configuration mode, use the following command:

api-token enable

Disabling the API Token

An administrator can disable the API token. If needed, the administrator can use this API token again by using the **api-token enable** command. To disable the API token, in administrator configuration mode, use the following command:

api-token disable

Deleting the API Token

An administrator can delete the API token. To do this, use the following command:

api-token delete

Viewing API Token

You can use the show command in any mode to view the API token of a specified administrator:

show admin api-token *user-name*

Example:

```
hostname(config)# show admin api-token test
================================================================
====
API Token: (Displays the API token value, which is used to log in to RESTful
API) ewoJInR5cCI6CSJKV1QiLAoJImFsZyI6CSJTSEEyNTYiCn0-
=.ewoJInVzZXJuYW1l-
IjoJInRl-
c3QiLAoJInZzeXN-
faWQiOgk-
wCn0-
=.$020100rE$cmWWDXrSBhBtQvY+Pco1mSf-
fmhmICNk7NKAhxeS08wX/Kb08=
```

```
Begin Time: 2022-11-17 21:08:42(Displays the point in time when the API token takes effect)
Expiration: 60 days(Displays the validity period of the API token)
Time To Expiration: 60 days(Displays the remaining days of the API token)
Current status: normal(Displays the current status of the API token. The value normal indicates that the API token is enabled.)
------------------------------------------------------------
```

Creating a Trusted Host

Hillstone device allows only trusted hosts to manage the system. Trusted hosts are recognized by their IP address range, or MAC address/range. If the host address is in the specified range, the host is a trusted host.

By default, the address range of the trusted host is 0.0.0.0/0, which means all hosts are trusted. Therefore, you are suggested to configure a proper address range and delete the default range afterward.



Notes: When you cannot access the device from a particular host, check the IP settings of the trusted host.

To set the IP range for the trusted host, in the global configuration mode, use the following command:

admin host {**range** *A.B.C.D A.B.C.D* | *A.B.C.D netmask* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet** | **netconf** | **any** }

- **range***A.B.C.D A.B.C.D* | *A.B.C.D netmask* | *A.B.C.D/M* | **any** – Specifies the IP range of the trusted host, such as 1.1.1.1 255.255.0.0. **any** means any IP address.
- **http** | **https** | **ssh** | **telnet** | **netconf** | **any** – Specifies the login type of the trusted host. **any** menas any type of HTTP, HTTPS, SSH, Telnet and NETCONF.

To set the IP range and MAC address/range, in the global configuration mode, use the following command:

admin host {**range** *A.B.C.D A.B.C.D | A.B.C.D netmask | A.B.C.D/M* | **any**} **mac-host** { **range** *H.H.H H.H.H | H.H.H* | **any**} {**http** | **https** | **ssh** | **telnet** | **netconf** | **any** }

- range *A.B.C.D A.B.C.D* | *A.B.C.D netmask* | *A.B.C.D/M* | any – Specifies the IP range of the trusted host, such as 1.1.1.1 255.255.0.0. any means any IP address.
- **range** *H.H.H H.H.H | H.H.H* | **any**} – Specifies the MAC address or range of the trusted host, such as 1111.1111.1111 2222.2222.2222. any means any MAC address.
- http | https | ssh | telnet | netconf | any – Specifies the login type of the trusted host. any menas any type of HTTP, HTTPS, SSH, Telnet and NETCONF.

You can repeat the above commands to set more range of the trusted hosts. At most 128 range can be set in the system.

Use the command no admin host {range *A.B.C.D A.B.C.D* | *A.B.C.D netmask* | *A.B.C.D/M* | *any*} to disable the specified IP range.

Use the command no admin host {range *A.B.C.D A.B.C.D* | *A.B.C.D netmask* | *A.B.C.D/M* | *any*} **mac-host**{ **range** *H.H.H H.H.H | H.H.H*| *any*} to disable the specified IP range and MAC address/range.

When IP range is used to match the trusted hosts, use the command no admin host {range*A.B.C.D A.B.C.D* | *A.B.C.D/M* | any} {http | https | ssh | telnet | netconf | any } to disable the specified login type.

When IP range and MAC address/range are used to match the trusted hosts, use the command no admin host {range *A.B.C.D A.B.C.D* | *A.B.C.D/M* | any} **mac-host**{ **range** *H.H.H H.H.H | H.H.H* | *H.H.H*| *any*} {http | https | ssh | telnet | netconf | any } to disable the specified login type.

Creating an IPv6 Trusted Host

Trusted hosts are recognized by their IP addresses. If the host IP address is in the specified IPv6 range, the host is a trusted host.

To set the IP range for the trusted host, in the global configuration mode, use the following command:

admin ipv6-host {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} [**mac-host** {*H.H.H* | **range***H.H.H H.H.H* | **any**}] {**http** | **https** | **ssh** | **telnet**| **netconf** | **any** }

- *X:X:X:X::X/M* | **range** *X:X:X:X::X X:X:X:X::X* | **any** - Specifies the start IP and end IP of trusted hosts, for example, "1.1.1.1 255.255.0.0". any means you can access the device from any host.
- **mac-host** {*H.H.H* | **range***H.H.H H.H.H* | **any**} – Specifies the MAC address range of trusted hosts. any means you can access the device from any host. After you specify the range, the address type is IPv6&MAC. If not specified, the address type of trusted hosts is IPv6.
- **http** | **https** | **ssh** | **telnet** | **netconf** | **any** - Specifies the protocol you can use to access the device from a trusted host. **any** means all the four protocols are enabled.

You can specify up to 128 trusted IP ranges.

To cancel configuring a trusted host whose address type is IPv6, use the command **no admin ipv6-host** {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**}.

To cancel configuring a trusted host whose address type is IPv6&MAC, use the command **no admin ipv6-host** {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} **mac-host** {*H.H.H* | **range***H.H.H H.H.H* | **any**}.

To disable access to the device from IPv6 trusted hosts over the specified protocol, use the command **no admin ipv6-host** {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} {**http** | **https** | **ssh** | **telnet** | **netconf**}. If only one login type is configured, you can delete this login type only by deleting the trusted hosts.

To disable access to the device from IPv6&MAC trusted hosts over the specified protocol, use the command **no admin ipv6-host** {*X:X:X:X::X/M* | **range***X:X:X:X::X X:X:X:X::X* | **any**} **mac-host** {*H.H.H* | **range***H.H.H H.H.H* | **any**} {**http** | **https** | **ssh** | **telnet** | **netconf**}. If only one login type is configured, you can delete this login type only by deleting the trusted hosts.

Viewing Trusted Host IP

To view information on configured trusted IP range, in any mode, use the following command:

show admin host

Example:

```
hostname(config)# show admin host
=================================================================
==================================
Addr Addr Type Login type
(Trusted Host Address / Address Type: IPv4, IPv4&MAC,
IPv6, or IPv6&MAC / Login type)
-----------------------------------------------------------------
----------------------------------
0.0.0.0/0 IPv4 Telnet SSH HTTP HTTPS
::/0 IPv6 SSH HTTPS
1000::1/23 1111.1111.1111 IPv6&MAC SSH HTTPS
1000::1/23 IPv6 HTTPS NETCONF
=================================================================
==================================
```

Configuring NetBIOS Name Resolution

The feature of NetBIOS name resolution enables the system to get all registered NetBIOS names of computers in the managed network, and store them in the cache, so that it can provide IP address-NetBIOS name resolution service for functional modules.

So far, NetBIOS name resolution is only used by the traffic logging feature to display the host name in its logs. Therefore, you should enable the NetBIOS name resolution if you want to view host names in traffic logs. For information about how to configure traffic log, see "Displaying Hostname/Username in the Traffic Logs" of "Logs".

To configure NetBIOS name resolution, take the following steps:

1. Enable the NetBIOS host name resolution service for the specified zone (the zone should not the one being connected to WAN).
2. StoneOS automatically looks up NetBIOS names for IP addresses in the stat-sets.

This process may take a while and the results are stored in the NetBIOS cache table. The table is updated regularly by the system.



Notes: The computer's host name cannot be searched unless it is enabled with NetBIOS.

Enabling NetBIOS Name Resolution

To enable NetBIOS name resolution for a zone, in the zone configuration mode, use the following command:

nbt-cache enable

To disable NetBIOS name resolution, use the following command:

no nbt-cache enable



Tip: To enter a zone configuration mode, use the command zone zone-name**zone** *zone-name*.

Resolving an IP to NetBIOS Name

To resolve an IP address of a host to its NetBIOS host name and MAC address, in the global configuration mode, use the following command:

nbtstat ip2name *ip-address* [**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address to be resolved.
- **vrouter** *vrouter-name* - Specifies the VR of the host. If this parameter is not defined, StoneOS uses the default VR (trust-vr).

Clearing NetBIOS Cache

To clear NetBIOS cache, in the global configuration mode, use the following command:

clear nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address and NetBIOS cache data related to this IP address are cleared by the system. If this parameter is not defined, all NetBIOS cache data are cleared.
- **vrouter** *vrouter-name* - Specifies the VR and NetBIOS cache data related to this VR are cleared by the system. If this parameter is not specified, all NetBIOS cache data are cleared.

Viewing NetBIOS Cache

To view NetBIOS cache data (including IP address, host name, MAC address and VR), in any mode, use the following command:

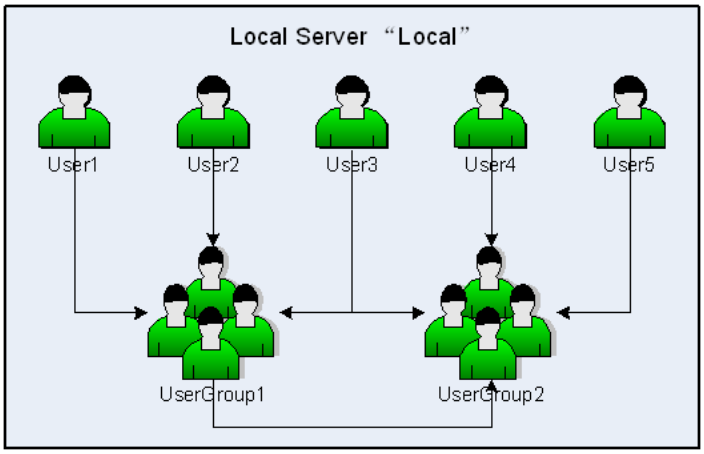
show nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

- *ip-address* - Shows NetBIOS cache data related to the specified IP address. If this parameter is not defined, all NetBIOS cache data are displayed.
- **vrouter** *vrouter-name* - Shows NetBIOS data of the specified VR. If this parameter is not defined, all NetBIOS cache data are displayed.

Management of System User

In StoneOS, user refers to the user who uses the functions and services provided by the Hillstone device, or who is authenticated or managed by the device. The authenticated users consist of local user and external user. The local users are created by administrators. They belong to different local authentication servers, and are stored in system's configuration files. The external users are stored in external servers, such as AD server or LDAP server. StoneOS supports user group to facilitate user management. Users belonging to one local authentication server can be allocated to different user groups, while one single user can belong to different user groups simultaneously; similarly, user groups belonging to one local authentication server can be allocated to different user groups, while one single user group can belong to different user groups simultaneously. The following dia-

gram takes the default AAA server Local as an example and shows the relationship between users and user groups:



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or exclusively use some bandwidth. In StoneOS, users and privileges are not directly associated. Instead, they are associated by roles. The mappings between roles and users are defined by role mapping rules. When a role is assigned with some services, its mapped users receive the corresponding services as well. StoneOS supports the AND, NOT or OR logical calculation of roles.If a role is used by different modules, the user will be mapped to the result role generated by the specified operation. The system supports the role blacklist function. You can control whether a user can be successfully authenticated to log in by adding the role the user maps to in the role blacklist. During login authentication, if the role information obtained by the user via role mapping is in the role blacklist, the user cannot access the network.

Hillstone device supports the following role-based functions:

- Role-based policy: Access control over users according to their roles.
- Role-based QoS: Bandwidth control over users according to their roles.
- Role-based stat-set: Collects statistics on bandwidth, sessions and new sessions based on roles.
- Role-based session limit: Implements session limits for specific users.

- SSL VPN role-based host security check: Resource access control over users according to roles.
- Role-based PBR: Implements routing for users of different types.
- Role-based SSL VPN/ZTNA/WebAuth/L2TP/802.1X/IPSec VPN (UserGroup) access control: With the role blacklist function, only specific users can have access to the network.

Configuring Users

User configurations include static user binding configuration and authenticated user configuration.

Binding an IP/MAC Address to a User

To bind an IP address or MAC address to a user, in the global configuration mode, use the following command:

user-binding *aaa-server-name user-name* {**ip** {*ipv4-address* | *ipv6-address*} [**auth-check-only** | **vrouter** *vr-name*] | **mac** *mac-address*}

- *aaa-server-name* - Specifies the name of the user's AAA server.
- *user-name* - Specifies the user name.
- **ip** {*ipv4-address* | *ipv6-address*} - Specifies the IP address, including IPv4 address and IPv6 address.
- **auth-check-only** - If this parameter is configured, the system checks if the user IP address conforms with the bound IP of this user. If it conforms, the user is allowed to enter authentication stage.
- **vrouter** *vr-name* - Specifies the VR of the designated IP/MAC address. The default value is the default VR (trust-vr).
- **mac** *mac-address* - Specifies the MAC address.

To remove the binding of IP/MAC and user, in the global configuration mode, use the following command:

no user-binding *aaa-server-name user-name* {**ip** {*ipv4-address* | *ipv6-address*} [**auth-check-only**] | **mac** *mac-address*} [**vrouter** *vr-name*]

Configuring Users in the Local AAA Servers

You can configure users/user groups to a local AAA server. To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**

user *user-name*

To create a local user, in the local AAA server configuration mode, use the following command:

- *user-name* - Specifies the user name. You can specify up to 63 characters.

This command creates a user and leads you into its configuration mode; if the user name exists, you will directly enter the user configuration mode. To delete the specified user, in the AAA server configuration mode, use the following command:

no user *user-name*

Configurations of a local user include:

- Basic settings: password, expiration, description and user group configuration.
- Dial-up VPN settings: IKE ID configuration.
- PnPVPN settings: DNS server, WINS server, IP/netmask/gateway/tunnel routing of DHCP address pool and tunnel routes. For detailed information, see "Configuring User's Network" of "VPN".

Configuring Password

To specify a password, in the user configuration mode, use the following command:

password [**irreversible-cipher**] *password*

- irreversible-cipher - Specifies method to encrypt the user's password as the irreversible encryption algorithm.If this parameter is not specified, the encryption mode is reversible encryption.
  - In reversible encryption algorithm, system will use the reversible encryption algorithm AES to encrypt the user password. In some authentication scenarios, system can decrypt the password for authentication.
  - In irreversible encryption algorithm,system will use the SHA irreversible encryption algorithm to encrypt user passwords. The passwords cannot be decrypted. In this case, the user can not authenticate through CHAP (Challenge Handshake Authentication Protocol, which is used in L2TP VPN and 802.1X).
- *password* - Specifies the user password. You can specify up to 31 characters.

To delete a password, in the user configuration mode, use the following command:

no password

Specifying a User Expiration Date

An expired user cannot pass the authentication, so it becomes an invalid user. By default, all users have no expiration date set.

To specify the expiration date and time for a user, in the user configuration mode, use the following command:

expire *Month/day/year HH:MM*

- *Month/day/year HH:MM* - Specifies the date and time in the format of month/date/year hour:minute. For example, expire 02/12/2010 12:00 indicates that the user is invalid since 12:00, February 12nd, 2010.

To cancel the expiration date configuration, in the user configuration mode, use the following command:

no expire

Describing a User

To give some description for a user, in the user configuration mode, use the following command:

desc *string*

- *string* - Specifies description at a maximum of 31 characters.

To delete the description, in the user configuration mode, use the following command:

no desc

Specifying an IKE ID

The Dial-up VPN users need IKE IDs. To specify an IKE ID, in the user configuration mode, use the following command:

ike_id {**fqdn** *string* | **asn1dn** *string* | **key-id** *string* }

- **fqdn** *string* - Uses IKE ID of the FQDN (Fully Qualified Domain Name) type. *string* is the ID content.
- **asn1dn** *string*- Uses IKE ID of the Asn 1dn type, which is only applicable to the user with a certificate. *string* is the ID content.
- **key-id** *string* – Specifies the ID that uses the type of the Key ID. This type can only be used in the XAUTH function.

To delete the IKE ID of a user, in the user configuration mode, use the following command:

no ike_id

Specifying a User Group

You can categorize users into a group according to your need. One user is allowed to be in multiple groups.

To specify a group for a user, in the user configuration mode, use the following command:

group *user-group-name*

- *user-group-name* - Specifies the name of an existing group in the system. You can specify up to 127 characters.

Repeat this command to define more user groups for a user. Note: If a user is added to more than 256 groups, only the first 256 group associations will take effect based on the association sequence. This principle also applies when the group associations are configured on an external authentication server.

To cancel a user-user group relationship, in the user configuration mode, use the following command:

no group *user-group-name*



Tip: For more information about user group settings, see Configuring a User Group.

Viewing User/User Group Information

To view the information of user/user group, in any mode, use the following commands:

- Show all users:

  show user

- Show a specific user:

  show user aaa-server *server-name* [**name** *user-name*]

- Show the IP/MAC and user bindings:

  show user-binding aaa-server *server-name*

- Show user groups:

  show user-group aaa-server *server-name*

Configuring a User Group

You can configure users or user groups on a local AAA server. To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name*

type local.

To create a local user group, in the local AAA server configuration mode, use the following command:

user-group *user-group-name*

- *user-group-name* - Specifies a name for the user group.

This command creates the user group and leads you into the user group configuration mode; if the user group of the specified name exists, you will enter the user group configuration mode directly.

To delete the specified user group, use the following command:

no user-group *user-group-name*

To add a member (either a user or another user group) to the user group, in the user group configuration mode, use the following command:

member {**user** *user-name* | **group** *user-group-name*}

- *user-name* - Specifies the user name.
- *user-group-name* - Specifies the user group name. A user group can include up to five nested layers, but a group cannot add itself as a member.

Repeat this command to add more members to a group.

To delete a member from a user group, in the user group configuration mode, use the following command:

no member {**user** *user-name* | **group** *user-group-name*}

User Going Offline Alarm

The system supports the Going Offline Alarm function of User, which can be used to monitor the offline status of users. When the number of users going offline exceeds the specified threshold within a specified period of time, the system generates a corresponding event log for alarm. In addition, the system can send the alarm to related personnel by using SNMP Trap host, sms, or email in a timely manner. This facilitates subsequent response and handling.

To configure the Going Offline Alarm function of User, take the following steps:

1. Creating a User Going Offline Alarm Profile.

2. Configuring an L2TP VPN Instance to Reference a User Going Offline Alarm Profile.

Notes:

- The system can create at most 4 user going offline alarm profiles.
- At most one alarm message can be sent to a specified trap host/email address/mobile number within a minute.

Creating a User Going Offline Alarm Profile

To create a user going offline alarm profile, in global configuration mode, use the following command:

user-logout-alarm profile*profile_name*

- *profile_name* – Specifies the name of the user going offline alarm profile. After the command is executed, the system generates a user going offline profile with the specified name and enters the user going offline alarm configuration mode. If the specified name already exists, the system directly enters the user going offline alarm configuration mode. Valid values: 1 to 31 characters. You can create at most 4 user going offline alarm profiles.

To delete a specified user going offline alarm profile, in global configuration mode, use the following command:

no user-logout-alarm profile *profile_name*

Configuring User Going Offline Alarm Threshold

The system allows you to configure the threshold of user going offline alarm. When the number of times that users go offline exceeds the threshold within a specified period of time, an alarm is generated. If not configured, an alarm is generated when 50 times of users going offline occur within 60 seconds.

To configure the user going offline alarm threshold, in user going offline alarm configuration mode, use the following command:

logout-threshold *times* **interval** *time-value*

- *times* – Specifies the times threshold of user going offline. Valid values: 10 to 500. Default value: 50.
- **interval** *time-value* – Specifies the time threshold of user going offline. Valid values: 10 to 300 seconds. Default value: 60 seconds.

To restore the threshold of user going offline alarm to defaults, in user going offline alarm configuration mode, use the following command:

no logout-threshold

Configuring a User Going Offline Alarm Mode

After a user going offline alarm message is generated, the system can send the alarm message to related personnel by using SNMP Trap host, sms, or email in a timely manner. This facilitates subsequent response and handling.



Notes: At most one alarm message can be sent to a specified trap host/email address/mobile number within a minute.

The configuration of user going offline alarm includes:

- Enabling/Disabling the SNMP Trap Alarm Function
- Enabling/Disabling the SMS Alarm Function
- Specifying the SMS Alarm Type
- Specifying the SMS Gateway
- Specifying the Mobile Number Used for Receiving Text Messages
- Enabling/Disabling the Email Alarm Function

- Specifying the Email Server
- Specifying the Email Address Used for Receiving Alarm Emails

Enabling/Disabling the SNMP Trap Alarm Function

The system supports the SNMP Trap Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm trap message to the configured trap host.

To enable/disable the SNMP Trap Alarm function, in user going offline alarm configuration mode, use the following command:

snmp-trap {**enable** | **disable**}

- **enable** – Enable the SNMP Trap Alarm function.
- **disable** – Disable the SNMP Trap Alarm function.



Notes: Before you use the SNMP Trap Alarm function, you need to configure the trap host. For more information, see Configuring Recipient of SNMP Trap.

Enabling/Disabling the SMS Alarm Function

The system supports the SMS Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm text message to the specified mobile number.

To enable/disable the SMS Alarm function, in user going offline alarm configuration mode, use the following command:

sms {**enable** | **disable**}

- **enable** – Enable the SMS Alarm function.
- **disable** – Disable the SMS Alarm function.

Specifying the SMS Alarm Type

When you use text message as an alarm, the system allows you to specify the SMS alarm type. After the system generates an alarm, it will automatically send an alarm text message to the

specified mobile number by using SMS modem or SMS gateway. If not specified, the SMS alarm type is SMS gateway.

To configure the SMS alarm type, in user going offline alarm configuration mode, use the following command:

sms type {**modem** | **service-provider**}

- **modem** – Sets the SMS alarm type to SMS modem. Note: CloudEdge does not support this parameter.
- **service-provider** – Sets the SMS alarm type to SMS gateway.

To restore the SMS alarm type to defaults, in user going offline alarm configuration mode, use the following command:

no sms type



Notes: CloudEdge does not allow you to set the SMS alarm type to SMS modem, so the **no sms type** command cannot take effect.

Specifying the SMS Gateway

When you set the SMS alarm type to SMS gateway, you also need to specify a configured SMS gateway.

To specify the SMS gateway, in user going offline alarm configuration mode, use the following command:

sms service-provider*provider_name*

- *provider_name* – Specifies the configured SMS gateway.

To delete the SMS gateway, in user going offline alarm configuration mode, use the following command:

no sms service-provider



Notes: Before you use the SMS Alarm function, you need to configure the SMS gateway. For more information, see Specifying Instance of SMS Gateway.

Specifying the Mobile Number Used for Receiving Text Messages

To specify the mobile number used for receiving alarm text messages, in user going offline alarm configuration mode, use the following command:

phone *phone_number*

- *phone_number* – Specifies the mobile number used for receiving text messages, which needs to be 6 to 15 characters in length.

You can repeat the command above to specify multiple mobile numbers. At most 3 mobile numbers can be specified.

To delete the specified mobile number, in user going offline alarm configuration mode, use the following command:

no phone *phone_number*

Enabling/Disabling the Email Alarm Function

The system supports the Email Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm notification to a specified email address.

To enable/disable the Email Alarm function, in user going offline alarm configuration mode, use the following command:

email {**enable** | **disable**}

- **enable** – Enable the Email Alarm function.
- **disable** – Disable the Email Alarm function.

Specifying the Email Server

When you use email as an alarm, you also need to specify a configured email server.

To specify the email server, in user going offline alarm configuration mode, use the following command:

smtp-server*server_name*

- *server_name* – Specifies the configured email server.

To delete the specified email server, in user going offline alarm configuration mode, use the following command:

no smtp-server



Notes: Before you use the Email Alarm function, you need to configure the email server. For more information, see Configuring a SMTP Server Instance.

Specifying the Email Address Used for Receiving Alarm Emails

To specify the email address used for receiving alarm emails, in user going offline alarm configuration mode, use the following command:

email *email_address*

- *email_address* – Specifies the email address used for receiving alarm emails, which needs to be 1 to 127 characters in length.

You can repeat the command above to specify multiple email addresses. At most 3 email addresses can be specified.

To delete the specified email address, in user going offline alarm configuration mode, use the following command:

no email *email_address*

Viewing a User Going Offline Alarm Profile

To view a created user going offline alarm profile, including the profile name, alarm threshold, and alarm mode, in any mode, use the following command:

show user-logout-alarm profile [*profile_name*]

- *profile_name* – Specifies the name of the user going offline alarm profile. If not specified, all created user going offline alarm profiles are displayed.

Configuring a Role

Role configurations include:

- Creating a role
- Creating a role mapping rule
- Configuring a role combination
- Configuring a Role Blacklist

Creating a Role

To create a role, in the global configuration mode, use the following command:

role *role-name*

- *role-name* - Specifies a name for the role. You can specify up to 31 characters.

To delete a role, in the global configuration mode, use the following command:

no role *role-name*

Creating a Role Mapping Rule

Role mapping rule defines the mapping relationship between a role and user/user group. StoneOS supports up to 64 role mapping rules, and each rule has a maximum number of 256 entries.

When the authentication for SSL VPN is set to USB Key certificate authentication ("User-name/Password + USB Key Certificate" or "USB Key only"), the system can map a role for the user according to the CN, OU or DN field of the USB Key certificate. For more information about USB Key authentication, see "Authentication With USB Key Certificate" of "VPN".

To enter the role mapping rule configuration mode, in the global configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* - Specifies a name for the role mapping rule. You can specify up to 31 characters. This command creates a rule and leads you in the role mapping rule configuration mode; if this rule exists, you will enter its configuration mode directly.

To delete the specified role mapping rule, in the global configuration mode, use the following command:

no role-mapping-rule *rule-name*

To configure a role mapping rule, in the role mapping rule configuration mode, use the following command:

To configure a role mapping rule, in the role mapping rule configuration mode, use the following command:

match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*| **user-attribute** *user-attribute-name* | **certificate-dn** *dn-field*} **role** *role-name*

- **any** | **user***user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*| **user-attribute** *user-attribute-name* | **certificate-dn** *dn-field* - Specifies the user, user group, certificate name, organization unit, user attributes or distinguished name for the mapping. **any** refers to any user, user group, certificate name, organization unit, user attributes or distinguished name in the system.
- **role** *role-name* - Specifies a role to be mapped in this rule.

Repeat this command to add more mapping rules.

To delete the specified mapping rule, in the role mapping rule configuration mode, use the following command:

no match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*| **user-attribute** *user-attribute-name* | **certificate-dn***dn-field*} **role** *role-name*

Configuring a User Attribute Instance

To configure a user attribute instance, you need to enter the configuration mode of the user attribute instance. In the global configuration mode, use the following command:

role-mapping-source user-attribute *user-attribute-name* **protocol-type** {**radius** | **ad/ldap**}

- *user-attribute-name* - Specifies the name of the user attribute instance.
- **protocol-type** {**radius** | **ad/ldap**} - Specifies the protocol type, which can be RADIUS (**radius**) or AD/LDAP (**ad/ldap**).

After this command is performed, the system creates a user attribute instance with the specified name and protocol type and enters the configuration mode of the user attribute instance. If the specified user attribute instance name exists, you will directly enter the configuration mode of the user attribute instance.



Notes: The system supports up to 64 user attributes instances.

In the global mode, use the **no role-mapping-source user-attribute** *user-attribute-name* command to cancel the configured user attribute instance.

Configuring Filters

To configure filters for the user attribute instance, in the configuration mode of the user attribute instance, use the following command:

attribute *attribute-value* {**contain** | **end-with** | **equal-to** | **greater-than** | **less-than** | **same-as** | **start-with**} *value*

- *attribute-value* - Specifies the name of the user attribute. The name can be user-defined or common names of user attributes.
- **contain** | **end-with** | **equal-to** | **greater-than** | **less-than** | **same-as** | **start-with** - Specifies the mapping operation, which can be contain, end-with, equal-to, greater-than, less-than, same-as,

or start-with.

- *value* - Specifies the mapping value of the user attribute.



Notes:

- Each user attribute instance supports up to 8 filers.
- When protocol type is specified as RADIUS, the mapping operation associated with string-typed user attributes can only be contain, start-with, end-with, or same-as. The mapping operation associated with number-typed user attributes can only be equal-to, greater-than, or less-than.
- When the mapping operation is contain, start-with, end-with, or same-as, the mapping value can be strings or numbers. When the mapping operation is equal-to, greater-than, or less-than, the mapping value can only be numbers.

In the configuration mode of the user attribute instance, use the following command to delete configured filters of the user attribute instance:

no attribute *attribute-value* {**contain** | **end-with** | **equal-to** | **greater-than** | **less-than** | **same-as** | **start-with**} *value*

Configuring the Matching Policy

To configure the matching policy of the user attribute instance, in the configuration mode of the user attribute instance, use the following command:

match {**once** | **all**}

- **once** | **all** - Specifies the matching policy of the user attribute instance: Once or All. **once** – The user is matched to the role mapped to the user attribute instance when the user hits any filter configured in the user attribute instance. **all** - The user is matched to the role mapped to the user attribute instance only when the user hits all filters configured in the user attribute instance.

In the configuration mode of the user attribute instance, use the **no match** command to cancel the specified matching policy of the user attribute instance.

Configuring a Role Combination

Roles can be grouped using logical calculation into a role combination. To configure a role combination, in the global configuration mode, use the following command:

role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

- [**not**] *r1* - Specifies the first role in this combination. **not** means excluded; *r1* refers to the name of an existing role. For example, "not testrole1" means all roles other than testrole1.
- **and** | **or** - Specifies the logical operator.
- [**not**] *r2* - Specifies the second role in this combination. *r2* refers to the name of an existing role.
- **role** *r3* - Specifies the calculated result. *r3* refers to the name of the result.

To delete the specified role combination, in the global configuration mode, use the following command:

no role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

Configuring a Role Blacklist

The system supports the role blacklist function. You can control whether a user can be successfully authenticated to log in by adding the role the user maps to in the role blacklist. During login authentication, if the role information obtained by the user via role mapping is in the role blacklist, the user cannot access the network.

To configure a role blacklist, in the global configuration mode, use the following command:

role-black-list *role-name*

- *role-name* - Specifies the name of the role to be added to the role blacklist. The value range is from 1 to 31 characters.

Note: You can only add existing role names to the role blacklist. To create a new role, in the global configuration mode, use the **role** *role-name* command.

In the global configuration mode, use the **no role-black-list** *role-name* command to delete a role name from the role blacklist.

Viewing Role Information

To view role related information, use the following commands:

- Show role information: **show role**
- Show role mapping rule information: **show role-mapping-rule** [*rule-name*]
- Show role combination information: **show role-expression**
- To view information about the role blacklist: **show role-black-list**

Configuring a MGT Interface

You can login to the Hillstone device over Console port, Telnet, SSH, or WebUI and configure their timeout settings, port number and PKI trust domain of HTTPS.

If you fail to login to the device three times in one minute over Telnet, SSH, HTTP or HTTPS, your login attempts will be refused in two minutes.

Configuring a Console MGT Port

This section describes how to configure the baud rate and timeout value of the console port.

Configuring the Baud Rate

To configure the baud Rate of console port, in any mode, use the following command:

exec console baudrate {9600 | 19200 | 38400 | 57600 | 115200}

- 9600 | 19200 | 38400 | 57600 | 115200 - Specifies the baud rate. The unit is bps.

Note: For A2200, A1800, A1600, X10800, X9180, K2680, and K2380, the default value is 9600bps. For other model devices, the default value is 115200bps.



Notes: When you login to the device, the baud rate of your console terminal should conform to the console baud rate specified here.

Configuring Timeout

If there is no configuration performed by the logged-in administrator until timeout, the system will disconnect the connection.

To configure the console timeout value, in the global configuration mode, use the following command:

console timeout *timeout-value*

- *timeout-value* - Specifies console timeout value. The value range is 0 to 60 minutes; the value of 0 means no time limit. The default value is 10.

To restore to the default value of console timeout, in the global configuration mode, use the following command:

no console timeout

Configuring a Telnet MGT Interface

When you login to the device over Telnet, your Telnet port should conform with the device Telnet port specified here. If an established Telnet connection does not send Telnet request until timeout, it will be disconnected.

To configure the Telnet timeout value, in the global configuration mode, use the following command:

telnet timeout *timeout-value*

- *timeout-value* - Specifies the Telnet timeout value. The range is 1 to 60 minutes. The default value is 10.

To restore to the Telnet default timeout value, in the global configuration mode, use the following command:

no telnet timeout

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

telnet max-session *max-session*

- *max-session* – Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

To restore the session numbers to the default value, in the global configuration mode, use the following command:

no telnet max-session

To specify the port number of Telnet, in the global configuration mode, use the following command:

telnet port *port-number*

- *port-number* - Specifies Telnet port number. The range is 1 to 65535. The default value is 23.

To restore to the default value, in the global configuration mode, use the following command:

no telnet port

Telnet maximum login number defines how many times you can try to login to the device over Telnet. If you fail more than the maximum times, your Telnet login attempts will be refused.

To specify the Telnet maximum login number, in the global configuration mode, use the following command:

telnet authorization-try-count *count-number*

- *count-number* - Specifies the maximum login number. The value range is 1 to 10 times. The default value is 3.

To restore to the default value, in the global configuration mode, use the following command:

no telnet authorization-try-count

Configuring a SSH MGT Interface

This section describes how to configure SSH timeout value, port number and connection interval.

SSH timeout value defines the maximum idle time of a SSH connection. If an established SSH connection does not send any SSH request until timeout, it will be disconnected.

To configure the SSH timeout value, in the global configuration mode, use the following command:

ssh timeout *timeout-value*

- *timeout-value* - Specifies the SSH maximum idle time. The value range is 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the following command:

no ssh timeout

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

ssh max-session *max-session*

- *max-session* – Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

To restore the session numbers to the default value, in the global configuration mode, use the following command:

no ssh max-session *max-session*

To set up the SSH port number, in the global configuration mode, use the following command:

ssh port *port-number*

- *port-number* - Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.

To restore to the default SSH port number, in the global configuration mode, use the following command:

no ssh port

SSH connection interval specifies the frequency of receiving SSH requests. When an SSH connection is established, the device receives the next SSH connection request at an interval of the time specified here.

ssh connection-interval *interval-time*

- *interval-time* - Specifies an interval time. The value range is 2 to 3600 seconds. The default value is 2.

To restore to the default value, in the global configuration mode, use the following command:

no ssh connection-interval

Configuring a WebUI MGT Interface

This section describes how to configure parameters of WebUI (HTTP or HTTPS) access.

To define the WebUI timeout value, in the global configuration mode, use the following command:

web timeout *timeout-value*

- *timeout-value* - Specifies the WebUI timeout value. The value range is 1 to 1440 minutes. The default value is 10.

To restore to the default WebUI timeout value, in the global configuration mode, use the following command:

no web timeout

To specify the HTTP port number, in the global configuration mode, use the following command:

http port *port-number*

- *port-number* - Specifies the port number of HTTP. When visiting WebUI over HTTP, the browser’s HTTP port must be the same as the port number specified here. The value range is 1 to 65535. The default value is 80.

To restore to the default HTTP port number, in the global configuration mode, use the following command:

no http port

To configure the anti-XSS service, in the global configuration mode, use the following command:

http anti-xss { disable | enable | mode {normal| strict}}

- **disable | enable** – Disables/Enables the anti-XSS service. By default, this service is enabled.
- **mode {normal| strict}** – Specifies the mode of the anti-XSS service, including the character matching mode and the regular expression mode.

In the global configuration mode, use the following command to restore the configurations to the default.

no http anti-xss { disable | enable | mode {normal| strict}}

Click-jacking is a visual deception means. The attacker uses an invisible iframe to cover a web page and induces the end user to perform operations on the web page. The end user will click on the invisible iframe page without knowing it. To prevent the attacker's page from being embedded in the WebUI page of the firewall, you can enable the anti-click-jacking function, which will add an "X-Frame-Options sameorigin" field to the response to make sure all WebUI pages of the firewall are from the same domain name. By default, the anti-click-jacking function is enabled.

To disable the anti-click-jacking function, in the global configuration mode, use the following command:

http anti-click-jacking disable

To enable the anti-click-jacking function, in the global configuration mode, use the following command:

http anti-click-jacking enable

Content Security Policy (CSP) can control what resources user agents can load for a given page to prevent cross-site scripting attacks, which improves security.

To configure a content security policy, in global configuration mode, use the following command:

http content-security-policy {script-src-self | none}

- **script-src-self** - Specifies to match the current zone, which allows inline script styles and dynamic creation of scripts from strings.
- **none** - Do not match any content.

Users can access the device via HTTPS or GM HTTPS:

- HTTPS: The system communicates with the client (browser) based on the TLS/SSL protocol;
- GM HTTPS: The system communicates with the client (GM browser) based on the GM TLS/SSL protocol. In the SSL authentication process, two certificates are used, including the signature certificate and the encryption certificate.

To enable or disable GM HTTPS, in the global configuration mode, use the following command:

https ssl-protocol-gm {**enable** | **disable**}

- **enable** | **disable** - Enables or disables GM HTTPS.

To specify the HTTPS port number, in the global configuration mode, use the following command:

https port *port-number*

- *port-number* - Specifies the HTTPS port number. When visiting WebUI over HTTPS, the browser's HTTPS port number must be the same as the port number specified here. The value range is 1 to 65535. The default value is 443.

To restore to the default HTTPS port number, in the global configuration mode, use the following command:

no https port

To specify the PKI trust domain for HTTPS access, or specify the PKI trust domain of signature certificate for GM HTTPS access, in the global configuration mode, use the following command:

https trust-domain *trust-domain-name*

- *trust-domain-name* - Specifies the name of the configured PKI trust domain. When users access the device via HTTPS, in the SSL authentication process, the HTTPS server uses the certificate stored in the specified PKI trust domain. When users access the device via GM HTTPS, in the GMSSL authentication process, the HTTPS server uses the certificate stored in the specified PKI trust domain as the signature certificate. By default, the system uses the below default PKI trust domain: trust_domain_default.

To restore the default PKI trust domain, in the global configuration mode, use the following command:

no https trust-domain

GM HTTPS applies two certificates. Therefore, when GM HTTPS is enabled, you should specify the PKI trust domain of the encryption certificate. To specify the PKI trust domain of the encryption certificate, in the global configuration mode, use the following command:

https trust-domain-enc *trust-domain-name*

- *trust-domain-name* - Specifies the name of the configured PKI trust domain. When users access the device via GM HTTPS, in the GMSSL authentication process, the HTTPS server uses the certificate stored in the specified PKI trust domain as the encryption certificate. By default, the system uses the below default PKI trust domain: trust_domain_default.

To restore to the default encryption trust domain for GM HTTPS access, in the global configuration mode, use the following command:

no https trust-domain-enc

Viewing MGT Interface Configuration Information

To view management interface configuration information, in any mode, use the following commands:

- Show console port configuration information: **show console**
- Show Telnet configuration information: **show telnet**

- Show SSH configuration information: **show ssh**
- Show Web configuration information: **show http**

Configuring a Storage Device

Hillstone network behavior control feature allows you to keep full records of user network behaviors. The logs are stored in a local database in form of a database file.

The storage device that can accommodate local database can be an SD card, USB disk or the storage expansion module provided by Hillstone.

Formatting a Storage Device

If a storage device cannot function, or its file system is not supported by StoneOS, or it has not been formatted yet, you can execute formatting command to repair it, change its file system or format it.

To format a storage device, in any mode, use the following command:

exec format [**sd0** | **usb0** | **usb1** | **storage***X*]

- **sd0** - Formats the SD card in the SD slot.
- **usb0** | **usb1** - Formats the USB disk inserted to the device's USB port.
- **storage***X* - Formats the storage expansion module in the specified slot. X is the slot number and its value range varies from platform types.



Notes: Formatting a storage device erases all the data in it. You should back up your files.

Removing a Storage Device

If you pull out the storage device with force, unsaved data may be lost. To ensure data integrity, you should use the command below to safely remove the device.

To safely remove a storage device, in any mode, use the following command:

exec detach [sd0 | usb0 | usb1 | storage*X*]

- sd0 - Removes the SD card from the SD slot.
- usb0 | usb1 - Removes the USB disk from the specified USB port.
- storage*X* - Removes the storage expansion module from the specified slot.

Upgrading Database Data

After you upgrade the system to a new version, both the earlier and new versions of data, such as logs, monitoring data, and reports, exist in the database. Due to the format inconsistency between these two versions of data, you may not be able to view the earlier version of data. To ensure that system features can be displayed and used properly, you need to upgrade the earlier version of data in the database to the data in the format that complies with the new version. If you do not need the earlier version of data, delete it.

To upgrade database data, in any mode, use the following command:

exec database data {upgrade | delete}

- upgrade - Upgrade earlier version of data whose format is inconsistent with that of new version of data. If the system is downgraded to a lower version, the upgrade status of data in the database is Upgrade not started. In this case, you can use this command to downgrade database data to data in the format that complies with the new version.
- delete - Delete earlier version of data whose format is inconsistent with that of new version of data.

Viewing Upgrade Status of Database Data

The upgrade statuses of database data include "Upgrade not started", "Upgrading", and "No database files need to be upgraded". To view the upgrade status of database data, in any mode, use the following command:

show mysql data operate

An example command output is shown as follows:

```
hostname#show mysql data operate
Mysql database progress:
==========================================
State Percentage
------------------------------------------------------------------
Upgrade not started.
==========================================
```

Configuring Storage Management

The system provides storage management functions to help you manage system storage space by limiting the disk space occupied by each function. In addition, system allocates fixed storage space for packet loss statistics, long-term monitor, reports, and logs of each module. For devices with hard disks installed, you can configure a custom storage size. When the data storage space of each function reaches or exceeds the configured thresholds, logs are generated to generate alarms. The configuration of the storage management page varies depending on whether the device contains hard disks.



Notes:

- The storage management function is available only for:
  - SG-6000 A-Series devices (except SG-6000-A200/A200W/A200G4B)
  - SG-6000 K-Series devices
  - SG-6000 A-Series devices X8180/X20803/X20812
  - CloudEdge
- It is recommended that the sum of custom storage space configurations do not exceed the total threshold. Otherwise, some data stores may fail to reach the preset threshold.

Configuring Threshold Alarm

When the system storage ratio or storage space reaches the specified threshold, the system will perform the specified action to control the system storage.

To configure the threshold of alarm, in the global configuration mode, use the following command:

storage threshold percent *percent-value*

- *percent-value* – Specify the threshold of alarm. The storage ratio ranges from 0.01% to 90%.

Specifying the Action to Handle Logs Exceeding the Storage Threshold

When reached the specified threshold, the system will perform the specified action, including override the earliest data and stop recording data.

To configure the action, in the global configuration mode, use the following command:

storage threshold log {**automatically-overwirte** | **stop-overwrite**}

- **automatically-overwirte** - The system will delete earliest logs. For SG-6000 K-Series devices installed with hard disks, if you need to back up the deleted logs, enable the FTP function to transfer the deleted logs to the FTP server. See Configuring a Syslog Server
- **stop-overwrite** - The system will stop storing new logs.

Configuring the Calculated Mode of the Storage Threshold

To configure the calculated mode of the storage threshold, in the global configuration mode, use the following command:

storage thresholdlog mode {**global** | **by-log-type**}

- **global** - The storage threshold is calculated based on the total storage space.
- **by-log** - The storage threshold is calculated based on the separate storage space of each module log.

Note: For devices without hard disks, the storage threshold is calculated **by-log-type**by default, and the storage space for logs and reports is a fixed value.

Enabling/Disabling Threshold Alarm

When the system storage ratio or storage space reaches the specified threshold, the system will record a log message.

To enable/disable the threshold of alarm, in the global configuration mode, use the following command:

Enable: **storage threshold alert-log enable**

Disable: **storage threshold alert-log disable**

Configuring Total Log Storage Threshold

For devices with hard disks installed, you can configure the total storage threshold for all types of logs. For a device without hard disks, the log storage threshold is default value and cannot be configured.

To configure the total log storage threshold, in the global configuration mode, use the following command:

storage threshold log percent *percent-value*

- *percent-value* – Specify the total log storage threshold. The storage ratio ranges from 0.01% to 90%.

Note: The total log storage threshold can take effect only when the calculated mode is set to **global**(use the command **storage thresholdlog mode global**).

Configuring the Log Storage Threshold for Each Type

For devices with hard disks installed, you can configure custom log storage threshold of the specified module as required. For a device without hard disks, the log storage thresholds are default values(event log 7%, configuration log 6%, and network log 6%) and cannot be configured.

To configure the log storage threshold for each type, in the global configuration mode, use the following command:

storage threshold log {**configuration** | **endpoint-tag** | **event** | **network** | **sandbox** | **threat** | **traffic** {**session** | **nat**} } *percent-value*

- {**configuration** | **endpoint-tag**| **event** | **network** | **sandbox** | **threat** | **traffic** {**session** | **nat**} } *percent-value* - Specify the disk space size of the log.

Note: The the log storage threshold for each type can take effect only when the calculated mode is set to **by-log-type**(use the command **storage threshold log mode by-log-type**).

Configuring Storage Threshold of Report

For devices with hard disks installed, you can customize the disk space size for the report file as needed. For a device without hard disks, the system allocates a default disk space size for the report file and cannot be configured.

To configure the storage space of report, in the global configuration mode, use the following command:

storage threshold log report *percent-value*

- **report** *percent-value* - Specify the disk space size of the report file.

Note: For devices without hard disks, the storage space for reports is a fixed value.

Configuring Long-term Monitor Storage Size

For devices with hard disks installed, you can customize the storage size of statistical data for the Long-term Monitor function as needed. For a device without hard disks, the statistical data for the Long-term Monitor function cannot be stored.

The long-term monitor function is available only for:

- SG-6000 A-Series devices (except A1605/A1805/A2205) installed with hard disks.
- SG-6000 K-Series devices installed with hard disks .

To configure the storage size of statistical data for the Long-term Monitor function, run the following command in the global configuration mode:

storage threshold statistics-long-term *percent-value*

- *percent-value* - Configure the storage size of statistical data for the Long-term Monitor function. Valid values: 0.01% to 90%. Default value: 10%.

Configuring a Packet Loss Storage Size

For A-Series devices (except A1605/A1805/A2205) with hard disks installed, you can customize a storage size for packet loss statistics as needed. For a A-Series device without hard disks, the packet loss statistics cannot be stored.

To configure a storage size for packet loss statistics, run the following command in the global configuration mode:

storage threshold module-drop-counter *percent-value*

- *percent-value* - Specifies the storage size for packet loss statistics. Valid values: 0.1%-90%. Default value: 2%. If the storage usage exceeds the threshold, earlier statistical data is deleted.

Viewing the Configuration of Storage Threshold

To view the configuration of storage threshold , maximum storage space and utilization, in any mode, use the following command:

show storage threshold

Managing Configuration Files

All information of system configuration, such as its initial and current configuration information, is stored in the configuration files. You can use command lines or visit the WebUI to view all sorts of system configurations. The information is stored and displayed in the format of command line.

Managing Configuration Information

This section describes how to view, import, export and save the configuration information.



Notes: Passwords of local users will not be exported when you export configuration information.

Viewing Configuration Information

Initial configuration information, stored in the configuration file, is used to configure the system parameters when the device is powered on. If no proper initial configuration information is found, the device uses default parameters to initialize the system. Similarly, the parameter settings the system is using now are called current configuration information.

StoneOS saves ten versions of initial configuration information. The latest one is used by the system as its startup configuration information when it starts up; the other versions are backup files. The last saved configuration information is marked as "Startup" and the nine backup versions are marked by number from 0 to 8 based on their saved time.



Notes: If you have rolled back to a specified saved initial configuration, the configuration information is marked as "Startup".

To view the current startup configuration information, in any mode, use the following command:

show configuration [**startup**]

To view the backup startup configuration information, in any mode, use the following command:

show configuration backup *number*

- *number* - Specifies the number of the configuration information.

To view the current configuration information, in any mode, use the following command:

show configuration

Comparing the Differences Between Current Configuration and Current/Backup Startup Configuration

You can compare the differences between the current configuration and the current startup configuration (startup configuration file) of the device to decide whether to save the current configuration to the startup configuration file and a new backup configuration file. Alternatively, when you prepare to use a backup startup configuration (backup configuration file) as the configuration file of the next startup, you can first compare the current configuration with the specified backup configuration file. To do this, use the following command:

show configuration difference {**startup** | **backup***number*} [**current-line***current-line-number* | **saved-line***saved-line-number*]

- **startup** – Specifies to compare the differences between the current configuration and current startup configuration of the device.
- **backup***number* – Specifies to compare the differences between the current configuration and a backup startup configuration of the device.
- **current-line***current-line-number* – Specifies to compare the differences starting from the *current-line-number* line of the current configuration and the first line of the startup/backup configuration file. If not specified, the comparison starts from the first line of both the current configuration and the startup/backup configuration file.
- **saved-line***saved-line-number* – Specifies to compare the differences starting from the first line of the current configuration and the *saved-line-number* line of the startup/backup configuration file. If not specified, the comparison starts from the first line of both the current configuration and the startup/backup configuration file.

Example:

```
hostname#show configuration difference startup current-line 3 (Compare the differences starting from the third line of the current configuration and the first line of the startup configuration file)
  --- current.config(- indicates the content that only belongs to the current configuration)
  +++ startup.config(+ indicates the content that only belongs to the startup/backup configuration file)
  @@ -1,5 +1,9 @@(Starting from the third line and going down 5 lines in the current configuration, there are differences when compared with the content from the first line in the startup configuration file, going down 9
```

```
lines.)
-# global configuration version: 194(-indicates the con-
tent that only belongs to the current configuration)
-# configuration sequence number: 383
+# Generated by autosave at 2023-09-11 15:54:37(+ indic-
ates the content that only belongs to the startup con-
figuration file)
+# Size is 11876 bytes
+# Software Version 5.5 SG6000-MX_MAIN-7x-V6-r0828.bin
2023/08/28 21:01:28
+
+# global configuration version: 192
+# configuration sequence number: 381
# PREVIOUS CONFIGERATION START(If no - or + exists, the
content of these two configuration files is the same.)
sandbox cloud-server-check enable
# END OF PREVIOUS CONFIGERATION
```

To view the current interface configuration information, in any mode, use the following command:

show configuration interface [*interface-name* | **last** *number*]

- *interface-name* – Specifies the interface name of the configuration information need to displayed.
- **last** *number* – Specifies the interface entry number of configuration information need to be displayed. System will display the interface configuration information from the last specified value entry to the end entry.

To view the current configuration information, in any mode, use the following command:

show configuration record

To view the current configuration information the system is using, in any mode, use the following command:

show configuration running

To view the current address book configuration information the system is using, in any mode, use the following command:

show configuration [**ipv4** | **ipv6**] **address** [**last** *number* | *address-name*]

- [**ipv4** | **ipv6**] - Specifies to display the configuration information of the IPv4 (**ipv4**) or IPv6 (**ipv6**) address entries, including the address entry name, type (pre-defined or user-defined) and address members. If not specified, it will display the configuration information of all IPv4 and IPv6 address entries.
- **last** *number* – Specifies the address entry number of the configuration information need to be displayed. System will display the address configuration information from the last specified value entry to the end entry, including the address entry name, type (pre-defined or user-defined) and address members.
- *address-name* - Specifies to display the configuration information of the address entry with the specified name, including the address entry name, type (pre-defined or user-defined) and address members.

To view the current policy configuration information the system is using, in any mode, use the following command:

show configuration policy [**last** *number*]

- *last number* – Specifies the policy entry number of the configuration information need to be displayed. System will display the policy configuration information from the last specified value entry to the end entry.

To view the current routing configuration information the system is using, in any mode, use the following command:

show configuration vrouter [**last** *number*]

- **last** *number* – Specifies the routing entry number of the configuration information need to be displayed. System will display the routing configuration information from the last specified value entry to the end entry.

Output the current configuration information using the XML format, in any mode, use the following command:

show configuration xml

Rolling Back to Previous Configurations

To roll back to the previous configuration, there are two ways:

In the execution mode, use the following command to roll back to the previous configuration. StoneOS saves the latest ten versions of system configurations as initial configuration files for you to use in system initiation. When the system restarts, the specified configuration will be used.

rollback configuration backup *number*

- *number* - Specifies the number of initial configuration file.

In the configuration rollback mode, use the following command to roll back to the previous configuration and exit the configuration rollback mode. The configuration will be valid without restarting the device.

exec configuration rollback



Notes: In the execution mode, you should use **exec configuration start** command to enter the rollback mode.

For example:

```
hostname# exec configuration start  (Enter the configuration rollback mode)
hostname[TRN]# configure  (Enter the global configuration mode)
…… (Execute any configuration, and the configuration will be valid immediately)
```

```
hostname[TRN](config)# exec configuration rollback (Roll back the con-
figuration and exit the configuration rollback mode)
hostname#
```

Exiting the Configuration Rollback Mode

To exit the configuration rollback mode directly, you can use the following two ways:

In the configuration rollback mode, use the following command to exit the configuration rollback mode directly.

exec configuration commit

For example:

```
hostname# exec configuration start (Enter the configuration rollback
mode)
hostname[TRN]# configure (Enter the global configuration mode)
..... (Execute any configuration, and the configuration
will be valid immediately)
hostname[TRN](config)# exec configuration commit (Exit the con-
figuration rollback mode directly)
hostname#
```

In the configuration rollback mode, use the command **exit**to exit the terminal directly.



Tip:

- When different users log in the device meanwhile, only the user who enters the configuration rollback mode first can do further configuration, and the later users cannot.
- When a user log in the device through different access methods, the user of a certain access method enters in the configuration rollback mode first can do further configuration, and the later users of other access methods



cannot. The user of other access methods can force the user of that access method to exit the configuration rollback mode through command.

Configuring the Action

When exiting the configuration rollback mode by using command **exit**, system wil exit the configuration rollback mode directly by default. To roll back to the previous configuration and exit the configuration rollback mode, in the global configuration mode, take the following command:

cli-exit-action rollback

To restore to the default value, in the global configuration mode, take the following command:

cli-exit-action commit

Deleting a Configuration File

To delete a configuration file from the system, in the configuration mode, use the following command:

delete configuration {**startup** | **backup** *number*}

- **startup** - Deletes the current configuration file.
- **backup** *number* - Deletes the specified backup configuration file.

Saving Configuration Information

When the current configurations are saved, they become the initial configuration information used by the system as next start-up configurations.

To save the current configurations, in any mode, use the following command:

save [*string*]

- *string* - Give some description for the saved configuration. If you leave this parameter blank, the former configurations will be replaced.

Backing up Configuration File Automatically

You can configure the function of back up the configuration file automatically, the device will check the configuration file regularly, when the configuration file changes, the system will update the configuration files to a FTP server , a TFTP server, a SFTP server or a FTPS server.



Notes: For any device platform, the maximum number of system configuration files that can be backed up is 5.

To back up configuration file to a FTP server automatically, in the global configuration mode, use the following command:

configuration auto-backup ftp *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*] [**cpu-threshold***threshold-value*]

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies the user name and password accessing FTP server.
- **vrouter** *vrouter-name* – Specifies the VRouter name.
- **path** *path* - Specifies the path of transferring the configuration files.
- **interval** *time-value* – Specifies the update interval. The value range is 1 to 7*24 hours. The default value is 1 hour.If this parameter is not specified, the system will check the configuration file hourly, and back up the changed configuration files to FTP server when configurations are changed.
- **cpu-threshold***threshold-value* - Specifies the CPU threshold for automatic backup of configuration files to the FTP server. Valid values: 1 to 99. By default, no limit is specified. After specifying the threshold, when the CPU utilization exceeds the threshold, configuration files will not be sent to the FTP server during that cycle. The system will wait until the next cycle to send configuration files again.

In the global configuration mode, use **no configuration auto-backup ftp** command to cancel the settings of backing up configuration file to a FTP server automatically.

To back up configuration file to a TFTP server automatically, in the global configuration mode, use the following command:

configuration auto-backup tftp *ip-address* [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

In the global configuration mode, use **no configuration auto-backup tftp** command to cancel the settings of backing up configuration file to a TFTP server automatically.

To back up configuration file to a SFTP server automatically, in the global configuration mode, use the following command:

configuration auto-backup sftp*ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

In the global configuration mode, use **no configuration auto-backup sftp** command to cancel the settings of backing up configuration file to a SFTP server automatically.

To back up configuration file to a FTPS server automatically, in the global configuration mode, use the following command:

configuration auto-backup ftps *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

In the global configuration mode, use **no configuration auto-backup ftps** command to cancel the settings of backing up configuration file to a FTPS server automatically.

Viewing backing up configuration file automatically Information

To view backing up configuration file automatically Information, in any mode, use the following command:

show configuration auto-backup

Exporting Configuration Information

Current and backup configurations can be exported to external destinations, including FTP server, TFTP server, a SFTP server or a FTPS server and USB flash disk.

To export system configurations to an FTP server, in the execution mode, use the following command:

export configuration {**startup** [**config-filetype zip** [**zip-password** *zip-password*]] | **backup** *number*| **all-vsys**} **to ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] [*file-name*]

- **startup** | **backup** *number* | **all-vsys** - Exports the current startup configurations, the specified backup configurations or the current startup configurations of VSYS.
- **config-filetype zip** [**zip-password** *zip-password*] - When exporting the current startup configurations, the system supports encrypted and unencrypted ZIP files. *zip-password* specifies the compression password of the ZIP file.
- *ip-address* - Specifies the IP address of FTP server.
- *vrouter-name* - Exports the configuration information of the specified VRouter.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *file-name* - Specifies the name for the file.

To export configurations to a TFTP server, in the execution mode, use the following command:

export configuration {**startup** [**config-filetype zip** [**zip-password** *zip-password*]] | **backup** *number* | **all-vsys**} **to tftp server** *ip-address* [**vrouter** *vrouter-name*] [*file-name*]

To export configurations to a SFTP server, in the execution mode, use the following command:

export configuration {**startup** [**config-filetype zip** [**zip-password** *zip-password*]] | **backup** *number* | **all-vsys**} **to sftp server** *ip-address* [**vrouter** *vrouter-name*] [**user***user-name* **password** *password*] [*file-name*]

To export configurations to a FTPS server, in the execution mode, use the following command:

export configuration {**startup** [**config-filetype zip** [**zip-password** *zip-password*]] | **backup** *number* | **all-vsys**} **to ftps server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] [*file-name*]

To export system configurations to USB flash disk, in the execution mode, use the following command:

export configuration {**startup** [**config-filetype zip** [**zip-password** *zip-password*]] | **backup** *number* | **all-vsys**} **to** {**usb0** | **usb1**} [**vrouter vrouter-name**] [*file-name*]

Importing Configuration Information

Configuration files can be imported into the system from the FTP server, TFTP server, SFTP server, FTPS server or USB flash disk inserted to the device USB port.

To import configurations from an FTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from ftp server** *ip-address* **user** *user-name* **password** *password* [**vrouter** *vrouter-name*] *file-name*

- **all-vsys** – Imports configuration information of all VSYS.
- **config-filetype zip** [**zip-password** *zip-password*] - Specifies the imported file type as being ZIP. If the file is encrypted, enter the compression password.
- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *vrouter-name* - Exports configuration information for the specified VRouter.
- *file-name* - Specifies a name for the configuration file.

To import configurations from a TFTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from tftp server** *ip-address* [**vrouter** *vrouter-name*] *file-name*

To import configurations from a SFTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from sftp server** *ip-address* [**vrouter** *vrouter-name*] [**user***user-name***password***password*] [*file-name*]

To import configurations from a FTPS server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from sftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] [*file-name*]

To import configurations from a USB flash disk, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from** {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

Enabling /Disabling Importing Configuration in USB Automatically

By default, when the device system starts, it will import the configuration files in USB automatically, that is, replace all existing configuration files in the device, including predefined configuration files and incremental configuration files (added on the basis of predefined configuration) , you can disable this function by command, and then the configuration file will not be imported automatically. To disable or enable this function, in global configuration mode, use the following command:

- Disable: **configuration load-by-usb disable**
- Enable: **configuration load-by-usb enable**

Take note of the following items when configuration files in the USB flash drive are automatically imported:

- The imported predefined configuration file name is in the **sn_XXX.config** format, in which "sn" indicates the serial number of the device and "XXX" indicates the custom fields. "XXX" can be up to 128 bytes and can contain letters, numbers, and underscores. After the configuration file is imported, the imported logs will be recorded in the root directory of the USB flash drive. If multiple configuration files with the same device SN number exist in the USB flash drive, you can change the format of configuration file name to **sn_timestamp.config** or **sn_timestamp_XXX.config**. This way, the system will import the configuration file with the

latest timestamp as the system boot file. The timestamp is in the **YYYYMMDDHHMMSS** format, in which Y indicates year, M indicates month, D indicates day, H indicates hour in 24-hour clock time, M indicates minute, and S indicates second, such as 20220521143030.

- The imported incremental configuration file name is in the **sn-inject_XXX.config** format, in which "sn" indicates the serial number of the device and "XXX" indicates the custom fields. "XXX" can be up to 128 bytes and can contain letters, numbers, and underscores. After the configuration file is imported, the imported logs will be recorded in the root directory of the USB flash drive. If multiple configuration files with the same device SN number exist in the USB flash drive, you can change the format of configuration file name to **sn-inject_timestamp.-config** or **sn-inject_timestamp_XXX.config**. This way, the system will import the configuration file with the latest timestamp as the system boot file. The timestamp is in the **YYYYMMDDHHMMSS** format, in which Y indicates year, M indicates month, D indicates day, H indicates hour in 24-hour clock time, M indicates minute, and S indicates second, such as 20220521143030.
- The automatically imported configuration file needs to be encoded in UTF-8 and the file size cannot exceed 16 MB.
- The automatically imported configuration file needs to be stored in the root directory of the USB flash drive.

Restoring Factory Defaults

You can either press the CLR button on the device or use the command in this section to reset the device and restore factory defaults.

To reset the device and restore factory defaults, in any mode, use the command **unset all**. See the following example:

```
hostname# unset all
Remove all the configuration(back to factory default), are you sure? y/[n]:  (type y to reset the device and restore factory defaults; type n or press Enter to go back to the execution mode.)
```



Notes: Use this command with caution. It clears all configurations on the device.

Switching the Working Mode of Fiber-optic Interfaces

The fiber-optic interfaces of the device itself and the interface expansion modules consist of four types which are QSFP28, QSFP+, SFP+, and SFP. Their default working modes are 100G, 40G, 10G, and 1G (1000M). The application of the four fiber-optic interfaces is as follows.

- **QSFP28 port**: The QSFP28 port cannot be inserted with the optical fiber-to-copper module. By default, it is in 100G working mode and can be switched to 40G working mode to connect with a 40G interface. To switch it to the 40G working mode, in the interface configuration mode, run the command: **channel-speed 40000**.
- **QSFP+ port**: The QSFP+ port cannot be inserted with the optical fiber-to-copper module. By default, it is in 40G working mode. It can be split into four 10G interfaces to connect with other 10G interfaces. In this condition, QSFP+ port still cannot be inserted with the optical fiber-to-copper module. The IOC-A-2QSFP+ of A-Series Firewall cannot be switched to the lower-speed working mode. To switch it to the 10G working mode, in the interface configuration mode, run the command: **channel-speed 10000**.
- **SFP+ port**: By default, SFP+ port is in 10G working mode. According to the transmission rate of the fiber-optic module or the fiber-optic-to-copper module, it can be automatically switched to 1G working mode to connect with a 1G interface. If the working mode cannot be switched automatically, in the interface configuration mode, run the command **channel-speed 1000** to manually switch it to the 1G working mode.
- **SFP port**: By default, the SFP port is in 1G working mode. The optical fiber-to-copper module can be inserted into the port. In interface configuration mode, you can use the **speed 100basefx** command to switch the port to 100M working mode.

To restore the default working mode of QSFP28 port and SFP+ port, in interface configuration mode, run the following command:

no channel-speed

To restore the default working mode of SFP port, in interface configuration mode, run the following command:

no speed



Notes:

- Delete relevant configuration of the interface before switching its working mode.
- When the working mode is switched, the fiber-optic module of the switched working mode needs to be inserted into the interface for connection.
- Only the following devices allow you to switch the working mode of SFP port: SG-6000-A5500, A5200, A5100, A3800, A3700, A3600, A3000, A2800, and A2700. When you switch to 100M working mode, the optical port can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers.
- For more information about the supported fiber-optic interfaces of All Series Firewalls, refer to Hardware Reference Guide and Expansion Modules Reference Guide.

Switching Mode

The 2x40GE(QSFP+) and 2x100GE(QSFP28) optical interfaces of SG-6000-A7600/A6800 can be switched to the following three modes through the **exec port-mode** command:

- **2x40GE(QSFP+)+2x100GE(QSFP28) mode**: The port 20 and 21 are in 40GE QSPF+ mode and the port 22 and 23 are in 100GE QSPF28 mode. This mode is the default mode.
- **2x100GE(QSFP28)+2x40GE(QSFP+) mode** : The port 20 and 21 are in 100GE QSPF28

mode and the port 22 and 23 are in 40GE QSPF+ mode.

- **4x100GE(QSFP28) mode**: Port 20-23 are in 100G QSFP28 mode.

To switch the mode, in any mode, use the following command:

exec port-mode { 2x40G+2x100G | 2x100G+2*40G | 4x100G}

- **2x40G+2x100G** - Switch to 2x40GE(QSFP+)+2x100GE(QSFP28) mode. This mode is the default mode.
- **2x100G+2x40G** - Switch to 2x100GE(QSFP28)+2x40GE(QSFP+) mode.
- **4x100G** - Switch to 4x100GE(QSFP28) mode.

Notes: The device needs to be restarted after switching modes.

Configuring the Negotiation Mode of Fiber-optic Interface

Supported models

- A series: A7600/A6800/A5800/A5600/A5555/A5255/A5155/A5500/A5200/A5100/A3815/A3615/A2815/A2715/A3800/A3700/A3600/A3000/A2800/A270-0;
- K series: K9180;
- X series: X8180.

Notes: For X8180 and K9180, before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

Fiber-optic interfaces have the following two negotiation modes:

- Auto-negotiation mode: This is the default negotiation mode. In this mode, an interface operates in auto-duplex mode at 1000Mb/s. After auto negotiation is completed, interfaces at both ends operate in full-duplex mode at 1000Mb/s.
- Forced mode: In this mode, an interface operates in full-duplex mode at 1000Mb/s.

To ensure that interfaces at both ends can complete link negotiation, you need to make the negotiation mode configuration of interfaces at both ends consistent. Negotiation mode configuration involves the following scenarios:

- Interfaces at both ends are in auto-negotiation or forced mode: No configuration is required.
- The peer interface is in forced mode and the local interface is in auto-negotiation mode: In interface configuration mode, use the **sfp-to-copper force** command to set the negotiation mode of the local fiber-optic interface to forced. The negotiation will not succeed until the negotiation mode of interfaces at both ends are consistent.
- The peer interface is in auto-negotiation mode and the local interface is in forced mode: In interface configuration mode, use the **no sfp-to-copper force** command to set the negotiation mode of the local fiber-optic interface to auto-negotiation. The negotiation will not succeed until the negotiation mode of interfaces at both ends are consistent.

Enabling/Disabling the Transceiver Module



Supported models

- A series:
  A7600/A6800/A5800/A5600/A5555/A5255/A5155/A5500/A5200/A5100

/A3815/A3615/A2815/A2715/A3800/A3700/A3600/A3000/A2800/A270-0;

- K series: K9180;
- X series: X8180.

Notes: For X8180 and K9180, before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

After you insert the transceiver module into the device, the module is enabled by default. To avoid that certain devices can complete link negotiation due to the transceiver module even if no network cable is used to connect both ends or a network cable is used to connect both ends but the rates at both ends are inconsistent, you are allowed to manually disable this module.

In interface configuration mode, use the **sfp-to-copper shutdown** command to disable the transceiver module.

To enable the transceiver module again, in interface configuration mode, use the **no sfp-to-copper shutdown** command.

Manually Configuring the Fiber-optic Interface to Negotiate with Peer Port

Supported model

- X series: X8180。

Notes: Before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

After you insert a transceiver module into the device, the fiber-optic interface of the device works in auto-negotiation mode by default. In this case, the device can only interoperate with the 1 GE port at the peer end. To ensure that the fiber-optic interface can negotiate with the peer 100M/10M port, you need to manually configure the fiber-optic interface.

To configure the negotiation mode of the fiber-optic interface to negotiate with the peer port, take the following steps:

1. In interface configuration mode, use the **channel-speed 1000** command to switch to the 1G working mode.
2. Use the **sfp-to-copper tri_speed** command to configure the fiber-optic interface to negotiate with the peer port.

In interface configuration mode, use the **no sfp-to-copper tri_speed** command to restore to the default configuration.

Deleting Configuration Information of Expansion Slots

For some models (X series devices, K9180, K6580) that are running, you might have the requirements of changing/removing the expansion modules.

For the IOM/SIOM modules, the configuration information of the expansion slots is complex. Before executing the hot-swappable action, you must use the **exec unset slot** {*number*} command to check and delete the configuration information of the expansion slots and initiate the modules.

To delete the configuration information of the expansion slots, use the following command:

exec unset slot *slot-number*

- *slot-number* – Specifies the slot number where the IOM/SIOM locates. The range is 1 to 128.

After executing this command, the system will display different prompts according to the different situations. You can perform the operations accordingly.

Notes:

- When the expansion slots are related to the interface configurations, you must first delete the interface configurations that related to the expansion slots and then execute the above command to delete the configuration information of the expansion slots.
- When executing the hot-swappable action for the SCM, SSM and QSM, you do not need to execute the above command.

Viewing the Configuration of Current Object

After the configuration of the specific object is completed, in the current configuration mode, you can use the command **show this** to view the configuration of current object.

The table below shows the object names and its configuration mode that system supported to view.

Object Name	Configuration Mode	Configuration Mode Prompt
Admin	Administrator configuration mode	hostname(config-admin)#
Admin Password Policy	Password policy configuration mode	hostname(config-pwd-policy)#
AAA server	AAA service configuration mode	hostname(config-aaa-server)#
Interface	Interface configuration mode	hostname(config-if-eth0/0)#
Zone	Zone configuration mode	hostname(config-zone-trust)#
Address	Address configuration mode	hostname(config-addr)#
Service	Service configuration mode	hostname(config-service)#
Service group	Service group configuration mode	hostname(config-svc-group)#

Object Name	Configuration Mode	Configuration Mode Prompt
Policy-based Route	PBR configuration mode	hostname(config-pbr)#
VRouter	VRouter configuration mode	hostname(config-vrouter)#
Configure NAT rules for the default VR trust-v	NAT configuration mode	hostname(config-nat)#
Traffic Management	First-level/Second-level traffic control mode	hostname(config-qos-engine)#
Security Policy	Policy rule configuration mode	hostname(config-policy-rule)
Host Book	Host configuration mode	hostname(config-host)#
Application Book	Application configuration mode	hostname(config-application)#
DNS Proxy	DNS proxy rule configuration mode	hostname(config-dns-proxy-rule)#
SSL Proxy	SSL proxy profile configuration mode	hostname(config-sslproxy-profile)#
VSYS	Non-root VSYS configuration mode	hostname(config-vsys)#

Viewing the Information of Optical Module

To view the information of optical module, including serial number, power, temperature, voltage, module type, wavelength and max transmission distance. In any in any mode, use the following commands:

show transceiver [*interface-name*]

- *interface-name* – Specifies the interface name of optical module.

Example:

```
SG-6000# show transceiver
Transceiver status information is shown as below:
================ xethernet0/6 ====================
SFP+/XFP information: FINISARCORP / FTLF8519P2BNL / 111230
Serial Number: PLT4PH9  (Displays the serial number of the transceiver module.)
Transmission media: Multi-mode  (Displays the transmission mode of the transceiver module, including Single-mode and Multi-mode.)
Module temperature: 32.38  (Displays the current temperature of the transceiver module.)
Module temperature warning range:[-30.00 , 93.00 ]  (Displays the temperature range of the transceiver module.)
Tx supply voltage: 3.34 V  (Displays the transmit supply voltage of the transceiver module.)
Tx supply voltage warning range:[ 2.90 , 3.70 ]  (Displays the transmit supply voltage range of the transceiver module.)
Tx bias current: 5.59 mA  (Displays the transmit bias current of the transceiver module.)
Tx bias current warning range:[2.00 , 14.00 ]  (Displays the transmit bias current range of the transceiver module.)
Tx optical power: -5.55 dBm  (Displays the transmit power of the transceiver module.)
Tx optical power warning range:[-11.00 ,-2.00 ]  (Displays the transmit power range of the transceiver module.)
Rx optical power: -6.69 dBm  (Displays the receive power of the transceiver module.)
Rx optical power warning range:[-18.01 , -1.00 ]  (Displays the
```

receive power range of the transceiver module.)

`Module Wavelength: 850.00 nm` (Displays the wavelength of the transceiver module.)

`single module max transmit distance: 0 km` (Display the max transmission distance of single mode.)

`OM1 max transmit distance: 150 m` (Display the max transmission distance of OM1 fiber.)

`OM2 max transmit distance: 300 m` (Display the max transmission distance of OM2 fiber.)

`OM3 max transmit distance: 0 m` (Display the max transmission distance of OM3 fiber.)

`copper max transmit distance: 0 m` (Displays the max transmission distance of the copper cable.)

```
==========================================================
===
```



Notes: Due to physical differences in hardware, some optical ports may fail to read information about the transceiver modules through this command.

Deleting Configuration Information of a virtual NIC

If the virtual NIC is forced to be deleted in CloudEdge, the unsaved data may be lost or other abnormal situation may happen. Therefore, to ensure the integrity of data, take the following steps when you delete the virtual NIC:

- Firstly, to shut down a virtual NIC, in any mode, use the following command:

  exec detach-port port *port-number*

  - *port-number* - Specify the port number of the virtual NIC that needs to be shut down. The value of *port-number* is equal to the value of "X" of Etherent0/X on the device.

- After the above command has been executed, the status of physical / protocol / link state, etc. of the corresponding interfaces will become **Down** (you can view it via the **show interface** command).
- Secondly, delete the virtual NIC on the virtual manager.
- Finally, to make the module initialize normally, in the execution mode, delete the configuration information of virtual NIC via the following command: **exec unset-port port** *port-number*

    - *port-number* – Specify the port number of the virtual NIC of which the configuration information needs to be deleted. The value of *port-number* is equal to the value of "X" of Etherent0/X on the device and the *port-numbe*r value of command exec detach-port port *port-number*.

  After the above commands are executed, The NIC is removed safely.



Notes:

- Don’t delete the interface etherent0/0, otherwise the product license will be invalid.
- CloudEdge supports up to 10 virtual NICs. The corresponding port number of virtual NIC will continue to increases in accordance with the sequence of NIC being inserted until the interfaces reach 10. When a port between two ports is deleted, and then a vacancy will generate. At this time, if a new virtual NIC is inserted, the port number of the new NIC will inherit the deleted port number.

Configuring Banner

Banner used to display the statement after logining the system, the user can customize the Banner information content. To edit the Banner, in the global configuration mode, use the following

command:

admin login-banner *Banner-content*

- *Banner-content* - Specifies the Banner content. The length varies from 1 characters to 4096 characters. After executing this command, the system will create the Banner of specified content. If the Banner already exists, it will modify the Banner for the specified content.

In the global configuration mode, use **no admin login-banner** command to delete the Banner.



Notes:

- In the edit Banner content, if you need to wrap, enter "\n", if you need a space, enter the double quotes "".
- Support for displaying Banner when login to the device over SSH, Telnet, or Console port.

Configuring the system language

System information includes log information, error information, and prompt information. The device supports both Simplified Chinese and English. To define the system language, in the global configuration mode, use the following command:

language {**en** | **zh_CN**}

- **en** – Specifies the system language to English. By default, the system language is English.
- **zh_CN** – Specifies the system language to Chinese.

To restore to default value, in global configuration mode, use the command **no language**.

It should be note that, this configuration does not affect the language of WebUI.

System Maintenance and Debugging

Testing tools, the commands Ping and Traceroute, are used to test network availability and diagnose system errors. Hillstone device also provides debugging feature for users to check and

analyze the system.。

Ping

Ping is used mainly for testing network connection and host accessibility.

To check network availability, in any mode, use the following command:

ping [**ipv6**] {*ip-address* | *hostname*} [**count** *number*] [**size** *number*] [**source** *ip-address*] [**timeout** *time*] [**vrouter** *vrouter-name*]

- **ipv6** - Specifies the type of peer IP address as IPv6.
- *ip-address* | *hostname* - Specifies the IP address or hostname of the destination. When using the dual-stack firmware, you can specify the IPv6 address.
- **count** *number* - Specifies the number of Ping packets. The value range is 1 to 65535. The default value is 5.
- **size** *number* - Specifies the size of ping packet. The value range is 28 to 65500 bytes.
- **source** *ip-address* - Specifies the source interface name or source IP address of ping packets.
- **timeout** *time* - Specifies the timeout value for the ping packets. The range is 0 to 3600 milliseconds. The default number is 0, which means no timeout.
- **vrouter** *vrouter-name* - Specifies the VRouter of the interface sending ping packets. The default value is trust-vr.

The output of ping command includes the response status for each Ping packet and the final statistics:

- The response status for each Ping packet. If there is no response, the output is "Destination Host Not Responding"; otherwise, the output is the packet sequence, TTL and responding time of the response packet. If the Ping packet does not reach the destination route or the interface that sends the Ping packet changes, the output is "Network is unreachable". If the destination address of the Ping packet cannot be resolved, the output is "unknown host

hostname".

- Final statistics. The final statistics includes sent packet number, received packet number, lost packet percentage and time.

Here is a **ping** command example:

```
hostname(config)# ping 10.200.3.1
Sending ICMP packets to 10.200.3.1
Seq ttl time(ms)
1 128 2.53
2 128 1.48
3 128 1.48
4 128 1.47
5 128 1.46
statistics:
5 packets sent, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.464/1.689/2.536/0.423 ms
```

Traceroute

Traceroute is used to test and record gateways of packets from source host to the destination. It is mainly used to check whether the destination is reachable, and analyze the fault gateway in the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet cannot be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As result, the path from the originating host to the destination is identified.

To trace the gateways the command traceroute has traversed, in any mode, use the following command:

traceroute [**ipv6**] {*ip-address* | *hostname*} [**numberic**] [**port** *port-number*] [**probe** *probe-number*] [**timeout** *time*] [**ttl** [*min-ttl*] [*max-ttl*]] [**source** *interface*] [**use-icmp**] [**vrouter** *vrouter-name*]

- **ipv6** - Specifies the type of peer IP address as IPv6.
- *ip-address* | *hostname* - Specifies the destination IP address or host name of traceroute. When using the dual-stack firmware, you can specify the IPv6 address.
- **numberic** - Specifies to display the address in numeric format without resolution.
- **port** *port-number* - Specifies the UDP port number. The value range is 1 to 65535. The default value is 33434.
- **probe** *probe-number* - Specifies the number of probe packet in each hop. The range is 1 to 65535. The default value is 3.
- **timeout** *time* - Specifies the timeout value of next probe packet. The range is 1 to 3600 seconds. The default value is 5.
- **ttl** [*min-ttl*] [*max-ttl*] - *min-ttl* is the minimum TTL value, with range from 1 to 255 and default value being 1. *max-ttl* is the maximum TTL value, with range from 1 to 255 and default value being 30. Specifying TTL is used to display the echo from the *min-ttl* hop to the *max-ttl* hop.
- **source** *interface* - Specifies the the name of the interface sending traceroute probe packets.
- **use-icmp** - Uses ICMP packets to probe. If this parameter is not defined, the system uses UDP packets to probe.
- **vrouter** *vrouter-name* - Specifies the VRouter of the egress interface of traceroute probe packets. The default value is the default VRouter (trust-vr).

Here is an example of applying command **traceroute** in network analysis:

```
hostname(config)# traceroute 210.74.176.150
traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52 byte packets
```

```
1 10.200.3.1 (10.200.3.1) 0.572 ms 0.541 ms 0.359 ms

2 192.168.3.1 (192.168.3.1) 0.601 ms 0.754 ms 0.522 ms

3 202.106.149.177 (202.106.149.177) 1.169 ms 1.723 ms 1.104 ms

4 61.148.16.133 (61.148.16.133) 2.272 ms 1.940 ms 2.370 ms

5 61.148.4.17 (61.148.4.17) 2.770 ms 61.148.4.101 (61.148.4.101) 6.030 ms 61.148.4.21 (61.148.4.21) 2.584 ms

6 202.106.227.45 (202.106.227.45) 4.893 ms 5.010 ms 3.917 ms

7 202.106.193.70 (202.106.193.70) 5.407 ms 202.106.193.126 (202.106.193.126) 4.247 ms 202.106.193.70 (202.106.193.70) 6.954 ms

8 61.148.143.30 (61.148.143.30) 3.459 ms 3.758 ms 2.853 ms

9 * * *

10 * * *
```

This example shows which gateways the packets have traversed during the process from source host to destination host and fault gateways.

System Debugging

System debugging helps you to diagnose and identify system errors. Basically, all the protocols and functions can be debugged. By default, debugging of all functions is disabled. The debugging function can only be configured through CLI.

To enable system debugging, in any mode, use the following command:

debug {**all** | *function-name*}

- **all** - Enables all debugging functions.
- *function-name* - Enables the specified protocol or feature debugging.

To disable all or one debugging function, in any mode, use the following command:

undebug {**all** | *function-name*}

You can disable debugging by pressing ESC key. As some debugging information has been cached, the closing process may take several minutes.

To see the status of the debugging function, in any mode, use the following command:

show debug



Notes: If you want to view debugging information on your terminal, enable debug logging function (execute the command **logging debug on**).

Collecting and Saving Tech-support Information to File

In order to locate the system fault, you should collect the displayed information of all the **show** commands and save as tech-support file. To collect and save the tech-support information to file, in any mode, use the following command:

show tech-support [**cpu** cpu-number | **all**]

- *cpu-number* – Collects and saves the tech-support information of specified CPU to file. You can configure this parameter only in system with multiple CPUs.
- **all** – Collects and saves all the tech-support information to file. You can configure this parameter only in system with multiple CPUs.



Notes: You can collect and save all the tech-support information to file through command **show tech-support** in system with single CPU.

Viewing the Tech-support Information

To view the tech-support information through Console port, in any mode, use the following command:

show tech-support [**cpu** *cpu-number* | **all**] **toconsole**

- *cpu-number* – Displays the tech-support information of specified CPU to Console port. You can configure this parameter only in system with multiple CPUs.

- **all** – Displays all the tech-support information to Console port. You can configure this parameter only in system with multiple CPUs.



Notes: You can view all the tech-support information though Console port by command **show tech-support toconsole** in system with single CPU.

Viewing the Information of Nvramlog or Watchdoglog File

To view the log information of nvramlog or watchdoglog in tech-support file, in any mode, use the following command:

show tech-support *log-name*

- *log-name* – Specifies the name of log information which is required to be displayed. You can specify the name as vramlog or watchdoglog.

Rebooting the System

During the operation of the device, users may need to restart the device or expansion module for various reasons. For device restart, users can choose to directly power off and then power on again, or perform a restart operation through CLI or WebUI. For the restart of the expansion module, users can perform a restart operation through CLI.

Rebooting the Device

To reboot the device, in the execution mode, use the following command: **reboot**

```
hostname# reboot

System configuration has been modified. Save? [y]/n (type y or press Enter
to save the settings; type n to give up changes.)

Building configuration..

Saving configuration is finished

System reboot, are you sure? y/[n]  (type y to reboot the system; type
n or press Enter to go back to the execution mode.)
```

Save the current settings before rebooting the device if you don't want to lose unsaved configurations. Be careful when you execute this command, because network disconnection occurs during the rebooting process.

Rebooting the Expansion Module

To reboot the expansion module, in the execution mode, use the **reboot slot** {*slot-number*} command:

```
hostname# reboot slot slot8
Reboot slot8, are you sure? y/[n]:  (type y to reboot the slot8; type n
or press Enter to go back to the execution mode.)
```

Upgrading StoneOS

When using the device, you may need to upgrade the version of StoneOS, the system firmware of the device. This section introduces StoneOS starting-up system and describes how to upgrade StoneOS.

- "Upgrading StoneOS via CLI" on Page 727
- "Upgrading StoneOS via Sysloader" on Page 734
- "Upgrading StoneOS by Using Hotfix" on Page 747

Upgrading StoneOS via CLI

You can upgrade StoneOS in the CLI by using an FTP server, TFTP server, FTPS server, SFTP server, or a USB drive.

Upgrading StoneOS via FTP Server

1. After logging into the CLI, import the file of the version to be upgraded via the FTP server by using the following command in execution mode:
   import image from ftp server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*
   - *ip-address* – Specifies the IP address of the FTP server.
   - **user** *user-name* **password** *password* – Specifies the username and password for the FTP server.
   - *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTP server.

- *file-name* – Specifies the name of the file of the version to be upgraded. If the version file is in the root directory of the FTP server, enter the version file name directly. If the version file is in a subdirectory, enter the "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0422.img is in the test/5.5R11 directory on the FTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0422.img as the file name.

2. After importing the version file, follow these prompts to save the version file to be upgraded:

```
Save this image? [y]/n: y ( Select 'y' to save the
current version file to be upgraded, select 'n' to
exit the upgrade)

2 image can be saved, please remove ( Up to two ver-
sion files can be stored in the Flash of the
device. If two version files are already saved in
the Flash, delete a stored one based on the
prompt.)

1: SG6000-ADNV-MX_MAIN-r0305(Active) ( Delete the
current system version file)

2: SG6000-ADNV-MX_MAIN-V6-t0301(Backup) ( Delete
the current backup version file)

3: remove all ( Delete all version files except the
one to be upgraded)

4: cancel ( Do not delete any files, select 4 to
exit the upgrade)

Which one do you select: 2

Are you sure? [y]/n: y

Remove SG6000-ADNV-MX_MAIN-V6-t0301...

Saving ...
```

```
Set SG6000-ADNV-MX_MAIN-r0422 as active boot image
```

3. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. Follow the prompts:

```
System configuration has been modified. Save?
[y]/n: y( There are configuration changes in the
system, select y to save the current system con-
figuration to the startup file.)
Building configuration.
Saving configuration is finished
System reboot, are you sure? y/[n]: y
2 configuration in system, please choose one to be
loaded.
================================================-
==================
Name Version Save Time Size (bytes)
------------------------------------------------
------------------
[a]: Startup 5.5R11 2024-04-23 18:50:18 33099
[b]: Backup 0 5.5R11 2024-04-23 18:50:18 33099
================================================-
==================
Press enter to use system current setting
Please choose one: a
```

4. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via TFTP Server

1. After logging into the CLI, upgrade StoneOS via the TFTP server by using the following command in execution mode:

   import image from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

   - *ip-address* – Specifies the IP address of the TFTP server.
   - *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the TFTP server.
   - *file-name* – Specifies the name of the file of the version to be upgraded. If the version file is in the root directory of the TFTP server, enter the version file name directly. If the version file is in a subdirectory, enter the "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0401.img is in the test/5.5R11 directory on the TFTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the file name.

2. After importing the version file, follow the prompts in the CLI to save the version file to be upgraded and delete the previous version file as needed. You can refer to Step 2 of Upgrading StoneOS via FTP Server.

3. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. You can refer to Step 3 of Upgrading StoneOS via FTP Server.

4. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via FTPS Server

1. After logging into the CLI, upgrade StoneOS via the FTPS server by using the following command in execution mode:

   import image from ftps server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

   - *ip-address* – Specifies the IP address of the FTPS server.
   - **user** *user-name* **password** *password* – Specifies the username and password for the FTPS server.
   - *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTPS server.
   - *file-name* – Specifies the name of the file of the version to be upgraded. If the version file is in the root directory of the FTPS server, enter the version file name directly. If the version file is in a subdirectory, enter the "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0401.img is in the test/5.5R11 directory on the FTPS server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the file name.

2. After importing the version file, follow the prompts in the CLI to save the version file to be upgraded and delete the previous version file as needed. You can refer to Step 2 of Upgrading StoneOS via FTP Server.

3. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. You can refer to Step 3 of Upgrading StoneOS via FTP Server.

4. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via SFTP Server

1. After logging into the CLI, upgrade StoneOS via the FTPS server by using the following command in execution mode:

   import image from sftp server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

   - *ip-address* – Specifies the IP address of the SFTP server.
   - **user** *user-name* **password** *password* – Specifies the username and password for the SFTP server.
   - *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the SFTP server.
   - *file-name* – Specifies the name of the file of the version to be upgraded. If the version file is in the root directory of the SFTP server, enter the version file name directly. If the version file is in a subdirectory, enter the "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0401.img is in the test/5.5R11 directory on the SFTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the file name.

2. After importing the version file, follow the prompts in the CLI to save the version file to be upgraded and delete the previous version file as needed. You can refer to Step 2 of Upgrading StoneOS via FTP Server.

3. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. You can refer to Step 3 of Upgrading StoneOS via FTP Server.

4. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via USB Drive



Notes: To upgrade StoneOS via USB drive, save the version file to be upgraded in the root directory of the USB drive.

1. Copy the version file to the root directory of the USB drive.
2. Insert the USB drive into the USB port of the device.
3. After logging into the CLI, upgrade StoneOS via USB drive by using the following command in execution mode:

   import image from {**usb0** | **usb1**} *file-name*

   - **usb0** | **usb1** – Specifies the USB port of the device used for the upgrade.
   - *file-name* – Specifies the name of the version file to be upgraded. Example: SG6000-ADNV-MX_MAIN-r0401.img.
4. After importing the version file, follow the prompts in the CLI to save the version file to be upgraded and delete the previous version file as needed. You can refer to Step 2 of Upgrading StoneOS via FTP Server.
5. In execution mode, enter the **reboot** command to restart the system and apply the new StoneOS version. You can refer to Step 3 of Upgrading StoneOS via FTP Server.
6. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.
7. Remove the USB drive promptly after the upgrade is completed.

Upgrading StoneOS via Sysloader

When the device fails and cannot boot into the StoneOS system, you can upgrade StoneOS via Sysloader by using an FTP server, TFTP server, or USB drive.

Introduction to the Boot System

Hillstone Networks firewall devices have a boot system divided into three parts: Bootloader, Sysloader, and StoneOS. Some devices only include Sysloader and StoneOS. Their functions are as follows:

- Bootloader – The first program that runs when the device is powered on. Bootloader loads and executes StoneOS or Sysloader.
- Sysloader - Used to upgrade StoneOS.
- StoneOS – The operating system of the device.

When the device starts, you can press the "ESC" key as prompted, and the Bootloader will attempt to start Sysloader. StoneOS is the OS of the device. Sysloader allows for updating and selecting StoneOS and supports upgrade via FTP, TFTP, and directly via USB Host port.

During device startup, some devices require pressing "Ctrl+W" to enter Sysloader, and it may prompt for a password or username and password. The actual device prevails. If you need a username and password, contact 1-800-889-9860.



Notes: Only A200, A200W, A200G4B, A1600, A1800, A2200, and X8180 devices need to enter Sysloader via Bootloader.

Physical Connection Requirements for the Device

When you upgrade StoneOS via Sysloader, the PC needs to be directly connected to the firewall via the Console port or connected by using a serial server.

PC Directly Connected to the Firewall via the Console Port

Upgrade personnel in a data center environment can connect the Console port of the firewall directly to the PC by using an RS-232 cable to perform the upgrade operation.

PC Connected to the Firewall via a Serial Server

If the data center has a serial server and the serial port of the server is connected to the Console port of the firewall via an RS-232 cable, the upgrade personnel can connect to the firewall remotely by using the serial server, thus performing the upgrade operation.

Run a terminal emulation program on the PC of the user, connect to the firewall by using the serial server, and enter the following command:
telnet *ip-address port*

- *ip-address* – Specifies the IP address of the serial server.
- *port* – Specifies the server port number of the serial server connected to the firewall.

Upgrade Procedure

In Sysloader, you can upgrade StoneOS by using an FTP server, TFTP server, FTPS server, SFTP server, or a USB drive.



Notes: Before upgrading StoneOS via Sysloader, complete the following steps:

1. The Console port (CON port) of the firewall is connected to the serial port of PC via a standard RS-232 cable. If the firewall is connected to a serial server, the PC of the user can be connected to the firewall through remote access to the serial server.
2. Obtain the baud rate of the Console port of the firewall in advance. Ensure that the baud rate of the terminal emulation program matches the baud rate of the device when running terminal emulation program on the PC to establishing a connection with the firewall. Use the **show console** command to



view the baud rate of the Console port of the device. If the device does not change the baud rate, you can refer to **Hardware Reference Guide** to obtain the default baud rate of the device.

3. Connect the MGT port of the device to the FTP/TFTP server. If there is no MGT port, use the eth0/0 interface.
4. After completing the above steps, restart the device and enter the boot system of the device.

Upgrading StoneOS via TFTP Server in Sysloader

Sysloader can obtain the version file to be upgraded from a TFTP server, allowing you to quickly upgrade StoneOS through the network. To do this, take the following steps:

1. After the CON port of the device is connected to the serial port of the PC via an RS-232 cable, restart the device and enter Sysloader during the reboot process. If Sysloader cannot be selected by using the up and down arrow keys, press "Ctrl+W" first and then enter Sysloader. For example, the SG-6000-K6580 device requires pressing "Ctrl+W" to enter Sysloader. The returned information may vary based on devices.

   Take SG-6000-X25803 as an example:

```
                GNU GRUB version 2.02
SG6000-XN-5.5R11B5-v6
SG6000-XN-5.5R11B8-v6
*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)
Loading Sysloader
[ 7.253642]
```

```
[ 7.255125] Arbitrating

[ 7.373235] -> Master

Sysloader 2.0.4 Jul 19 2023 - 11:40:32

Enter the password to stop autoboot: 3( Enter the
password that is used to log into Sysloder within 5
seconds and press Enter. To obtain the password,
contact 1-800-889-9860.)

sysloader(M)#

1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)

4 Select backup firmware as active

5 Show on-board firmware

6 Reset

7 Reset Administrator password

8 Load sysloader via TFTP
```

Take SG-6000-A2000 as an example:

```
                        GNU GRUB version 2.02

SG6000-ADNV-MX_MAIN-V6-t0419

SG6000-ADNV-MX_MAIN-r0420

*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)

Sysloader 1.0.5 Sep 23 2020 - 16:09:24

sysloader#

1 Load firmware via TFTP
```

```
2 Load firmware via FTP
3 Load firmware from USB disks (available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
```

For devices that need to enter Sysloader via Bootloader, follow these prompts (using SG-6000-A200 as an example):

```
Press ESC to stop autoboot: 2( Press "ESC" to enter the interactive mode of Bootloader)
load sysloader from USB? [y]/n: n( Type "n" for not upgrading Sysloader via USB)
Run on-board sysloader? [y]/n: y( Type "y" to enter Sysloader)
Loading: #
Starting kernel ...
Sysloader 8.0.10 Feb 2 2023 - 09:16:23
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
```

For SG-6000-K6580, press "Ctrl+W" and then select Sysloader. Follow these prompts:

```
                              GNU GRUB version 2.06
SG6000-HYGON-MX_MAIN-V6-r0420
SG6000-HYGON-R10_F-V6-r0409
*SYSLOADER( Select Sysloader by using the up and
down arrow keys and press Enter to enter Sys-
loader)
Enter username:(Enter the username used to log into
Sysloder and press Enter. To obtain the username,
contact 1-800-889-9860.)
Enter password:(Enter the password used to log into
Sysloder and press Enter. To obtain the password,
contact 1-800-889-9860.)
Loading Sysloader
▒
Sysloader 8.0.12 May 22 2023 - 01:52:42
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (not available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Clear button
9 Load sysloader via FTP
```

2. From the Operation Selection menu of Sysloader, select Upgrade StoneOS via TFTP Server. Follow these prompts (using SG-6000-A2000 as an example):

   Note: The startup option of Sysloader may vary based on platforms. For more information, see Introduction to the Sysloader Menu.

```
Sysloader 1.0.5 Sep 23 2020 - 16:09:24
sysloader#
1 Load firmware via TFTP
2 Load firmware via FTP
3 Load firmware from USB disks (available)
4 Select backup firmware as active
5 Show on-board firmware
6 Reset
7 Reset Administrator password
8 Load sysloader via TFTP
sysloader# 1( Enter "1" here and press Enter)
```

3. Configure the IP address of Sysloader, the IP address of TFTP server, the gateway IP address, and the version file name to be upgraded. Follow these prompts (using SG-6000-A2000 as an example):

```
Local ip address [ ]: 192.168.1.1/16 ( Enter the IP address of Sys-
loader and press Enter)
  Server ip address [ ]: 192.168.1.20 ( Enter the IP address of the
  TFTP server and press Enter)
  Gateway ip address [ ]: 192.168.1.2 ( If the IP addresses of Sys-
  loader and the TFTP server do not belong to the
  same CIDR block, enter the IP address of the gate-
  way and press Enter; otherwise, just press Enter)
```

```
File name : SG6000-ADNV-MX_MAIN-r0401.img( Enter the version
file name to be upgraded and press Enter. The sys-
tem will start to obtain the version file to be
upgraded via TFTP. If the version file is not in
the root directory of the TFTP server, you need to
enter "full path + version file name". For example,
if SG6000-ADNV-MX_MAIN-r0401.img is in the
test/5.5R11 path on the TFTP server, enter
test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the
file name.)

SG6000-ADNV-MX_MAIN- 100%
|*****************************| 327M 0:00:00 ETA
```

4. Save the version file to be upgraded. Follow these prompts (using SG-6000-A2000 as an example):

```
Save this image? [y]/n: y( Type "y" or press Enter to save
the obtained version file)

Only 2 image can be saved, please remove( A maximum
of two version files can be stored in the Flash of
the device. If two version files are already stored
in the Flash, follow the prompts to delete the
stored version file.)

1: SG6000-ADNV-MX_MAIN-r0420(Backup)( Delete the
currently backed-up version file)

2: SG6000-ADNV-MX_MAIN-V6-t0419(Active)( Delete the
current system version file)

3: remove all( Delete all version files except for
the one to be upgraded)

4: cancel( Do not delete any files, select 4 to
exit the upgrade)
```

```
Which one do you select: 2

Are you sure? [y]/n: y

Remove SG6000-ADNV-MX_MAIN-V6-t0419...

Saving

..................................................-
.........

Checking saved firmware

.......................................... OK

Set SG6000-ADNV-MX_MAIN-r0401 as active boot image
```

5. Restart the system. The system will start with the new version file. Follow these prompts (using SG-6000-A2000 as an example):

```
1 Load firmware via TFTP

2 Load firmware via FTP

3 Load firmware from USB disks (not available)

4 Select backup firmware as active

5 Show on-board firmware

6 Reset

7 Reset Administrator password

8 Load sysloader via TFTP

sysloader# 6( Enter "6" here and press Enter, the
system will restart)
```

6. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.

Upgrading StoneOS via FTP Server in Sysloader

The device support to obtain the version file to be upgraded from an FTP server. To upgrade StoneOS via FTP in Sysloader, take the following steps:

1. Enter Sysloader, select "2" from the Operation Selection menu of Sysloader, and press Enter. For more information about how to enter Sysloader, refer to Step 1 of Upgrading StoneOS via TFTP Server in Sysloader.
2. Configure the IP address of Sysloader. Enter the IP address configured for the Sysloader after "*Local ip address [ ]:*" and press Enter.
3. Configure the IP address of the FTP server. Enter the IP address of the FTP server after "*Server ip address [ ]:*" and press Enter.
4. If the IP addresses of Sysloader and the FTP server do not belong to the same CIDR block, configure the Sysloader's gateway IP address. Enter the gateway IP address after "*Gateway ip address [ ]:*" and press Enter.
5. Enter the FTP username after "*User Name [anonymous]:*" and press Enter.
6. Enter the corresponding password for the username after "*Password :*" and press Enter.
7. Enter the version file name to be upgraded after "*File name :*" and press Enter. The system will start to obtain the specified StoneOS via FTP. If the version file is not in the root directory of the FTP server, you need to enter "full path + version file name". For example, if SG6000-ADNV-MX_MAIN-r0401.img is in the test/5.5R11 path on the FTP server, enter test/5.5R11/SG6000-ADNV-MX_MAIN-r0401.img as the file name.
8. After the version file is transferred, the system will ask if you want to save the version file. Type "y" and the system will save the version file to the Flash of the device.
   Note: A maximum of two version files can be stored in the Flash of the device. If two version files are already stored in the Flash, follow the prompts to delete the stored version file.

9. After the version file is saved, press Enter, the Operation Selection menu of Sysloader will appear again. Select "6" and press Enter. The system will restart with the new version file.

10. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.



Tips: For anonymous FTP servers, directly press Enter after "*User Name* [*anonymous*]:" and "*Password* :" (Step 5 and Step 6).

Upgrading StoneOS via USB Port in Sysloader

You can also upgrade StoneOS via the USB Host port of the device by saving the version file to be upgraded in a USB flash drive.



Notes: To upgrade StoneOS via USB, you need to save the version file to be upgraded in the root directory of the USB flash drive.

Take the following steps:

1. Copy the version file to be upgraded to the root directory of the USB flash drive.

2. Insert the USB flash drive into the USB port of the device.

3. Enter Sysloader and select "3" from the Operation Selection menu of Sysloader, and press Enter.

4. Enter "y" after the version file to be upgraded, and the system will start to obtain the version file from the USB flash drive. The returned information may vary based on devices. Follow these prompts:

```
sysloader# 3( Enter "3" here and press Enter)
```

```
Please select firmware
1 SG6000-ADNV-MX_MAIN-r0401.img (usb0) [y]/n: n
2 SG6000-ADNV-MX_MAIN-V6-t0422.img (usb0) [y]/n: y
```

Note: If two USB flash drives are inserted into the device, and the version file to be upgraded is on USB1, first type "n" for the version file on USB0.

5. After the version file is transferred, the system will ask if you want to save the version file. Type "y" and the system will save the version file to the Flash of the device.
   Note: A maximum of two version files can be stored in the Flash of the device. If two version files are already stored in the Flash, follow the prompts to delete the stored version file.
6. After the version file is saved, press Enter, the Operation Selection menu of Sysloader will appear again. Select "6" and press Enter. The system will restart with the new version file.
7. During the upgrade process, do not perform any operations. After the upgrade is completed, log into the CLI and enter the **show version** command to verify whether the system is successfully upgraded to the new version.
8. Remove the USB drive promptly after the upgrade is completed.

Introduction to the Sysloader Menu

Sysloader uses menu prompts to help you complete specified operations. This section introduces the functions of each menu option in Sysloader, as described in the following table.

Menu Option	Function
1 Load firmware via TFTP	Upgrade StoneOS via TFTP.
2 Load firmware via FTP	Upgrade StoneOS via FTP.
3 Load firmware from USB disks	Upgrade StoneOS via USB flash drive.
4 Select backup firmware as active	Select the backup version file saved in the system as the current StoneOS startup sys-

Menu Option	Function
	tem.
5 Show on-board firmware	Display the name and status of version files saved in the system.
6 Reset	Restart the system.
7 Clear button	Delete all configurations and restore to factory settings. **Note**: The SG-6000 A/X/K9180 platform does not support this option. The sequence number of this option may vary based on devices.
7 Reset administrator password	Reset the password of the default administrator (hillstone). The reset password is randomly generated and is only effective for the first reboot. Change the password promptly after the first reboot. **Note**: The sequence number of this option may vary based on devices.
8 Load sysloader via TFTP	Upgrade Sysloader via TFTP. **Note**: The SG-6000 A/X/K platform supports this option. SG-6000-A200/A200W/A200G4B also supports to upgrade Sysloader via USB. After enter the Bootloader interaction mode, enter "y" after the "load sysloader from USB?" prompt to upgrade Sysloader via USB.
9 Load sysloader via FTP	Upgrade Sysloader via FTP.

Menu Option	Function
	Note: SG-6000-K6580 supports this option.

Follow the menu prompts and enter the corresponding number of the menu option after "sys-loader#", then press Enter.

Upgrading StoneOS by Using Hotfix

Hotfix upgrade allows the system to fix issues of the current software version without interrupting ongoing services. You can upload a patch file via an FTP server, TFTP server, FTPS server, or SFTP server, load the patch into the process, and then activate/run the patch to make it take effect.



Notes:

- The patch upgrade can only be performed via CLI.
- By default, the imported patch file is in the UNLOAD state and needs to be loaded into the system before being activated/run.
- The difference between **activate** and **run** in the **exec patch** *patch-name* {**activate** | **run**} command is as follows: **activate** activates the loaded patch to make it take effect, and it will automatically change to **RUNNING** after 48 hours. **run** directly runs the loaded patch, and the patch remains in the running state even after a device reboot. If the device with an **ACTIVE** patch is rebooted, the patch will revert to the UNLOAD state.
- The patch upgrade takes effect without needing to reboot the device.
- Patches are version-specific. After a version upgrade, previously running patches will become invalid.

To upgrade hotfix, take the following steps:

1. Import the patch file from the FTP/TFTP/FTPS/SFTP server to the device. For more information, see Importing a Patch File.
2. Use the **exec patch** *patch-name* **load** command to load the imported patch file into the StoneOS system. For more information, see Loading/Activating/Running/Deleting a Patch.
3. Use the **exec patch** *patch-name* {**activate** | **run**} command to activate or run the patch file to successfully upgrade the patch. For more information, see Loading/Activating/Running/Deleting a Patch.
4. Use the **show patch** command to view the patch status. The **ACTIVE** or **RUNNING** state should be displayed based on the configuration of Step 3. For more information, see Viewing the Patch Status.

To delete hotfix, take the following steps:

1. Use the **exec patch** *patch-name* **unload** command to unload the activated/running patch file.
2. Use the **show patch** command to view the patch status, which is displayed as **UNLOAD**.
3. Use the **exec patch** *patch-name* **delete** command to delete the patch file from the device. Only patches in the **UNLOAD** state can be deleted.

Importing a Patch File

In execution mode, use the following command to import the patch file to the system by using the FTP server:

import patch from ftp server *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name***password** *password*] *filename*

- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP server.

- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the FTP server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the FTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the TFTP server:

import patch from tftp server *ip-address* [**vrouter** *vrouter*] [*filename*]

- *ip-address* – Specifies the IP address of the TFTP server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the TFTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the TFTP server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the TFTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the FTPS server:

import patch from ftps server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTPS server.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTPS server.

- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the FTPS server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the FTPS server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the FTPS server, enter patch/5.5R11/K5680-r0426.patch as the file name.

In execution mode, use the following command to import the patch file to the system by using the SFTP server:

import patch from sftp server *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* – Specifies the IP address of the SFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password for the SFTP server.
- *vrouter-name* - Specifies the Vrouter associated with the device interface used to access the SFTP server.
- *filename* – Specifies the name of the patch file to be imported. If the patch file is in the root directory of the SFTP server, enter the patch file name directly. If the patch file is in a sub-directory, enter the "full path + patch file name". For example, if K5680-r0426.patch is in the patch/5.5R11 directory on the SFTP server, enter patch/5.5R11/K5680-r0426.patch as the file name.

Loading/Activating/Running/Deleting a Patch

To delete, load, activate, or run a patch, in any mode, use the following command:

exec patch *patch-name* {**delete** | **load** | **unload** | **activate** | **deactivate** | **run**}

- *patch-name* – Specifies the name of the patch file on which you want to perform operations.
- **delete** – Deletes the specified patch file. Only patches in the **UNLOAD** state can be deleted.
- **load** – Loads the specified patch file.
- **unload** – Unloads the specified patch file.
- **activate** – Activates the specified patch file to make it take effect. After a device reboot, the patch state will revert to the UNLOAD state.
- **deactivate** – Reverts the specified patch to the deactivated state.
- **run** – Runs the specified patch file. After a device reboot, the patch state remains running.

Viewing the Patch Status

After loading, activating, running, or deleting a patch, you can view the current patch status.

To view the patch status, in any mode, use the following command:

show patch

Synchronizing the Firmware

This function is only available on SG-6000-X10800.

When configuring two SCMs for the device, you should synchronize the firmware from the master SCM to the backup SCM. By default, system will synchinoize automatically when starts. If there’s a problem of automatic synchronization (such as failing to strart the backup SCM), in the execution mode, use the following command to synchronize the firmware manually:

exec image sync

SCM HA

Some Hillstone devices (All platforms of X series, and K9180) support SCM HA. When a device is installed with two SCMs, the SCM that is plugged into slot SCM0 is used as the master module,

and working in the Master mode; the SCM that is plugged into slot SCM1 is used as the backup module, and working in the Backup mode. If a device is installed with only one SCM, the SCM is used as the master module, and the newly installed SCM (if any) is used as the backup module. In such a case the master and backup modules are not determined by the slot positions. If the master SCM fails, the backup SCM will be promoted to the master module automatically to assure continuous business operation.

When using SCM HA, keep in mind that:

- Never configure any option on the backup SCM.
- After master-backup switching, the new backup SCM still works in the Backup mode after rebooting, and will not preempt the master SCM.
- After master-backup switching, you need to re-establish the management connection, such as Telnet or HTTP connection.
- To assure proper synchronization of license information, the system might prompt to reboot the system (with network disconnection). Continue your operation as prompted.

To view the SCM HA status, use the command **show module**. In the output the module that is labeled with M (e.g., Master) is the master SCM, and the module that is labeled with B (e.g., Backup) is the backup SCM.

Device HA Switchover When Switch Module failed

For some devices which are based on a fully distributed architecture (SG-6000-X9180， SG-6000-X10800, and SG-6000-X25812), the Switch Module (SWM) of the devices plays an important role in data forwarding. When the SWM fails, it may result in packet loss, packet error or traffic failure. In order to solve this problem, the system can take corresponding measures to ensure continuous business operation when it detects the failure of the SWM, including:

- In a dual-SWM scenario, if only one SWM fails, the user can configure whether to switch the device HA.

- In a dual-SWM scenario, if both SWMs fail, the device HA switchover is performed by default.
- In a single-SWM scenario, if the SWM fails, the device HA switchover is performed by default.

When the SWM fails, the device HA switchover is performed by default. To configure not to perform the device HA switchover, in the execution mode, use the following command:

ha config-swm-fault no-switchover

To configure to perform the device HA switchover when the SWM fails, in the execution mode, use the following command:

no ha config-swm-fault

To view the device HA switchover configuration when the SWM fails, in any mode, use the following command:

show ha config-swm-fault

License Management

License is used to authorize users features, services or extending the performance. If you do not buy and install the corresponding License, the features, services and performances which is based on License will not be used, or can not achieve the higher performance.

License classes and rules.

Platform License	Description	Valid Time	Whether to Restart
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are	You cannot modify the existing configuration when License expires. If the device is restar-	Not required.

	not effective. The device have been pre-installed platform trial license for 15 days in the factory.	ted, the previous configuration is retained but cannot be modified.	
Platform	You can install the platform license after the device formal sale. The license provide basic firewall and VPN function.	System cannot upgrade the OS version when the license expires, but the system could still work normally.	Not required.
Function License	**Description**	**Valid Time**	**Whether to Restart**
VSYS	Authorizing the available number of VSYS.	Permanent	Restart is required for each installation.
SSL VPN Trial License	Authorizes the maximum number of SSL VPN users that can be connected to the platform. The duration of use of the license is short.	After the trial license expires, the number of SSL VPN users that can be connected to the platform is restored	Not required.

	The actual available duration is determined by the protocol for the license. The available duration is a relative time, such as 30 days. Multiple SSL VPN trial licenses can be used together.	to its prior value.	
SSL VPN	Authorizing the number of SSL VPN access. Through installing multiple SSL VPN licenses, you can add the number of SSL VPN access.	Permanent	All versions, except the following should be restarted after each installation. Versions that do not need restarting are5.5R6P21 and later 5.5R6P versions, 5.5R8P7 and later 5.5R8P versions,

			5.5R9 and later.
ZTNA	Authorizing the maximum number of ZTNA access. ZTNA license has a higher priority than the ZTNA trial license. Multiple ZTNA licenses can be installed to increase the authorized number of ZTNA access. When the authorized number of SSL VPN access is inadequate, SSL VPN access can use the ZTNA license. ZTNA access cannot use the SSL VPN license.	Permanent	Not required.
ZTNA Upgrade	Converting the specified number of SSL VPN access to	Permanent	Not required.

	the equal number of ZTNA access. The SSL VPN license type is not limited. Multiple ZTNA Upgrade Licenses can be installed, but the converted number of access cannot exceed the total number of SSL VPN access. If the converted SSL VPN license is not permanent, the validity period of the ZTNA license is the same as the SSL VPN license before the conversion.		
ZTNA Trial	Providing ZTNA trial. Multiple ZTNA trial licenses can be installed to increase the number and validity period	When the license expires, you can only use the default authorization of 8 ZTNA con-	Not required.

	of ZTNA access.	current users.	
QoS/iQoS	Enable QoS function.	Permanent	Not required.
Cloud sandbox License	Providing Cloud sandbox function and white list update, authorizing the number of suspicious files uploaded per day. Including 4 licenses: Cloud sandbox-200, Cloud sandbox-300, Cloud sandbox-500 and Cloud sandbox-1000. The number of files allowed to upload per day is different for different licenses.	The valid time including 1 year, 2 years and 3 years. System cannot analyze the collected data and cannot update the white list when the license expires. The Cloud sandbox protection function can only be used according to the local database cache results. If you restart the device, the function cannot be used.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Twin-mode License	Providing the twin-mode function. The related parameters of the twin-mode	System cannot upgrade the twin-mode function and cannot	Not required.

	function can be displayed and configured.	provide the maintenance service when License expired.	
EPP	Providing the End Point Prevention function.	The End Point Prevention function cannot be used when the license expires.	Not required.
Service License	**Description**	**Valid Time**	**Whether to Restart**
AntiVirus	Providing antivirus function, and antivirus signature database and antivirus intelligence file engine database update. The following devices support the antivirus intelligence file engine database: • A-series: Devices except SG-	System cannot update the antivirus signature database and antivirus intelligence file engine database when the license expires, but the antivirus function and intelligence file engine detection function could still be used normally	Restart is required for the first installation. Do not require restart when you renew the subscription.

	6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200. • K-series: SG-6000-K2680, SG-6000-K2380, SG-6000-K6280-GS, SG-6000-K6580, and SG-6000-K9180. • X-series: SG-6000-X25803 and SG-6000-X25812. • CloudEdge: CloudEdge that is		

	deployed on X86-based server.		
URL DB	Providing URL database and URL signature database update.	System cannot provide the search URL database online function when the license expires, but the user-defined URL and URL filtering function can be used normally.	Restart is required for the first installation. Do not require restart when you renew the subscription.
IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when the license expires, but the IPS function could still be used normally.	Restart is required for the first installation. Do not require restart when you renew the subscription.
APP signature	APP signature license is issued with platform license, you do not	System cannot update the APP signature database when the license	Not required.

	need to apply alone. The valid time of license is same as platform license.	expires, but the included functions and rules could still be used normally.	
Threat Prevention	A package of features, including AntiVirus, IPS, threat intelligence, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.	Whether to restart, please refer to the restart policies for the individual licenses of AntiVirus, IPS, threat intelligence.
IP Reputation	Providing Perimeter Traffic Filtering function of IP reputation and IP reputation database update. From 5.5R6, StoneOS will support the Perimeter Traffic Filtering function of IP Reputation instead of predefined black list.	System cannot update the IP reputation database when the license expires.	Restart is required for the first installation. Do not require restart when you renew the subscription.

	You can buy the license of IP reputation to upgrade.		
StoneShield	A package of features, including Abnormal Behavior Detection, Advanced Threat Detection, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Antispam	Providing Anti-Spam function.	The Anti-Spam function cannot be used when the license expires.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Botnet Prevention	Providing Botnet Prevention function and Botnet Prevention database update.	System cannot update all signature databases when license expires. But the functions included and	Restart is required for the first installation. Do not require restart when you renew the sub-

		rules could be used normally.	scription.
IoT monitor&control	Providing the IoT policy function.	Permanent.	Not required.
IoT monitor&control trail	After the installation of IoT monitor&control trail license, you will get the same IoT policy function as system with IoT monitor&control license. But the duration will be shorter.	The IoT policy function cannot be used when the license expires. If you restart the device, the existing IoT policy configurations will not be lost, but won't take effect.	Not required.
Threat intelligence License	Providing the threat intelligence function.	The threat intelligence function cannot be used when the license expires.	Not required.
Bundle License1	A package of features, including IPS, AntiVirus, threat intelligence, QoS, URL DB, and corresponding sig-	For expiration, refer to the respective license policy.	Whether to restart, please refer to the restart policies for the individual licenses

	nature database update.		of IPS, AntiVirus, threat intelligence, QoS, URL DB.
Bundle License3	A package of features, including IPS, AntiVirus, threat intelligence, QoS, URL DB, Botnet Prevention, IP Reputation, Cloud sandbox, and corresponding signature database update.	For expiration, refer to the respective license policy.	Whether to restart, please refer to the restart policies for the individual licenses of IPS, AntiVirus, threat intelligence, QoS, URL DB, Botnet Prevention, IP Reputation, Cloud sandbox.

CloudEdge License

CloudEdge licenses are categorized to platform licenses, sub licenses, and function licenses . A platform license is the base to install all other types of licenses. You can apply for all kinds of licenses through SN number (i.e., old version license mechanism). If the virtual firewall is reinstalled, due to the change of SN number, you have to re-apply for a license.

From the version 5.5R5, the CloudEdge license has been upgraded to the latest version, with a different licensing mechanism. After the installation of the new platform license, the SN number of the device will be changed to a virtual SN (vSN for short). If you want to continue to obtain function or sub licenses, they can be applied through the vSN number. For the new license does not depend on the SN number of the original system after the re-installation of system, the new license that was originally applied for can still be effective. At the same time, Hillstone provides LMS (license management system) to verify and manage licenses, which can ensure the security of licenses.



Notes: If CloudEdge is a full license product, you do not need to purchase or install any license. It is already a full feature firewall when you purchase it.

CloudEdge Platform Licenses

CloudEdge is pre-installed with a free default license without application. You can apply for the platform license (the old version of the platform license) through the SN number or directly apply for the new version of the license. Old version platform license is divided into base license and trial license. The new platform license is divided into base license and sub license.

- **Default License**

  CloudEdge has a built-in free default license. All features are available in system with default license, such as SSL VPN, iQoS and IPS. However, performance is limited, e.g., only 2 IPSec VPN tunnels and 2 SSL VPN users are supported. The license is valid for 30 days. After expiration, all functions of the system can not be used, the OS version and all the signature databases can not be upgraded.

- **Platform Trial License**

  After the installation of Platform Trial License, you will get the same features as system with Platform Base License. But the duration will be shorter. The duration is determined by the agreement you signed, which is a relative period, for example, one month. After expiration, the existing configuration can not be modified. After the reboot, the original configuration is

retained but cannot be modified, and only the platform functions are available while the performance is limited.

- **Platform Sub License**

  After the installation of Platform Sub License, you will get the same features as system with Platform Base License. But the duration will be shorter. The duration is determined by the agreement you signed, which is an absolute period, for example, March 1 to March 31. After expiration, the existing configuration can not be modified. After the reboot, the original configuration is retained but cannot be modified, and only the platform functions are available while the performance is limited.

- **Platform License**

  When a CloudEdge is officially purchased, you can buy a Platform License. Platform License provides fundamental firewall features.

  When it expires, the system can be normally functioning, but cannot be upgraded to higher version.

CloudEdge Sub Licenses

Sub licenses control whether corresponding functions are enabled or not and the time limit as well.

- **IPSEC VPN Sub License**

  IPSEC VPN sub license enables IPSec VPN function and authorizes the maximum number of IPSec VPN accesses. After installing multiple IPSEC VPN licenses, you can increment the maximum number of IPSec VPN accesses. When the license expires, the IPSec VPN connection will be disconnected. IPSec VPN function will not be allowed to configure. Until the device is restarted, all the configurations of IPSec VPN will not be lost.

- **SSL VPN Sub License**

  SSL VPN sub license enables SSL VPN function and authorizes the number of SSL VPN

accesses. After installing multiple SSL VPN sub licenses, you can increment the number of SSL VPN accesses. When the license expires, the SSL VPN connection will be disconnected. SSL VPN function will not be allowed to configure. Until the device is restarted, all the configurations of SSL VPN will not be lost.

- ZTNA Sub License

  The priority of ZTNA sub license is higher than the ZTNA trial license and lower than the ZTNA license. Multiple ZTNA sub licenses can be installed to increase the number and validity period of ZTNA access. The optimal validity period is adopted. When the license expires, you can only use the default authorization of 8 ZTNA concurrent users.

- iQoS Sub License

  iQoS sub license enables iQoS function. When the iQoS sub license expires, all the configurations of iQoS will not be lost until the device is restarted.

- Virtual CPU License

  Virtual CPU license authorizes the maximum number of vCPUs available to the CloudEdge. The virtual CPU license does not expire. Different models of CloudEdge require different vCPU and memory. You can apply for the corresponding number of vCPU licenses as the follows:

Platform Models	Minimum Configuration
SG-6000-VM01	2 vCPU,2 GB memory
SG-6000-VM02	2 vCPU,4 GB memory
SG-6000-VM04	4 vCPU,8 GB memory
SG-6000-VM04	8vCPU,16GB memory

- Virtual CPU Sub License

  Virtual CPU sub license authorizes the maximum number of vCPUs available to the

CloudEdge. After the license expires, system will restart and the number of available vCPUs will revert to 2vCPU, which is the configuration of the minimum model SG-6000-VM01.

CloudEdge Function Licenses

Some functions are only enabled when that corresponding license is installed. The function service includes:

- **ZTNA License**

  Providing the ZTNA function, including the following types:

  a. ZTNA license: ZTNA license is permanently valid and has the highest priority. Multiple ZTNA licenses can be installed to increase the authorized number of ZTNA access. When the authorized number of SSL VPN access is inadequate, SSL VPN access can use the ZTNA license. ZTNA access cannot use the SSL VPN license.

  b. ZTNA Trial License: Providing ZTNA trial. Multiple ZTNA trial licenses can be installed to increase the number and validity period of ZTNA access. When the license expires, you can only use the default authorization of 8 ZTNA concurrent users.

  c. ZTNA Upgrade License: Converting the specified number of SSL VPN access to the equal number of ZTNA access. The SSL VPN license type is not limited. Multiple ZTNA Upgrade Licenses can be installed, but the converted number of access cannot exceed the total number of SSL VPN access. If the converted SSL VPN license is not permanent, the validity period of the ZTNA license is the same as the SSL VPN license before the conversion.

- **Intrusion Prevention System (IPS) License**

  IPS License provides IPS function and its signature database upgrade. IPS License has its own validity. When it expires, the IPS function works normally, but IPS signature database cannot be upgraded.

- Anti-Virus (AV) License

  AV License provides anti-virus function, and antivirus signature database and antivirus intelligence file engine database upgrade. AV License has its own validity. When it expires, the anti-virus function and intelligence file engine detection function work normally, but AV signature database and AV intelligence file engine database cannot be upgraded.

- Sandbox License

  Sandbox License provides sandbox function, which controls the suspicious file quantity allowed to be uploaded to the cloud sandbox every day, also, it provides white list upgrade. Sandbox License has its own validity. When it expires, the cloud analysis is stopped and the white list can not be upgraded. However, if the suspicious traffic still matches the analysis entries in the local cache, the sandbox function is still valid. After the system is restarted, the sandbox function will not be used.

- URL DB License

  URL DB License provides URL filter function and allows URL database to upgrade. URL DB License has its own validity. When it expires, the URL filter function works normally, but URL database cannot be upgraded.

- APP DB License

  APP DB License allows APP database to upgrade. APP DB license is issued with platform license. There is no need to apply for it. The validity of APP DB License also follows platform license. When the platform license expires, APP signature database cannot be upgraded.

- SR-IOV Throughput License /Trial License

  SR-IOV Throughput License provides throughput improvements for SR-IOV network cards of CloudEdge.When the license is installed, the throughput of SR-IOV card will be improved. SR-IOV Throughput License will not be expired, but the trial license will expire.And the throughput will return to the default value after expired.The default throughput of SR-IOV

network cards varies from platform, and the magnitude of increase after installing the license varies as follows:

SR-IOV Throughput	VM01	VM02	VM04	VM08
Default	2Gbps	4Gbps	8Gbps	16Gbps
After Installing License	10Gbps	20Gbps	40Gbps	80Gbps



Notes:

- Besides the licenses listed above, a hardware platform from Hillstone Networks can install other types of licenses, e.g. StoneShield, but currently, CloudEdge does not support licenses other than those listed here.
- Perimeter Traffic Filtering (PTF) function can be seen in StoneOS, but it is not available for the moment. Future versions will support the two functions.
- Currently, Anti-Virus (AV) License and Sandbox License are not available in CloudEdge for private cloud platform.

Applying for a License

To apply for a license, take the following steps:

Use the command **exec license apply applicant** *string* to generate a license application request. For more information, see Managing a License Using CLI” 。

Send the request to the Hillstone agent.

Installing a License

A license contains a string of characters. When you get the license, take the following steps to install it in the device:

If you use CLI to install a license, in any mode, use the command **exec license install** *license-string*. For more information, see Managing a License Using CLI. After installing, you need to reboot system to make the license effective.



Notes: Although license can be removed, you are strongly suggested not to uninstall any license.

Connecting to License server

For Hillstone CloudEdge virtual firewall, after installing the license, you need to connect to the license server to verify the validity of the license to prevent the license from being cloned. System supports two ways, one is connecting the firewall to the public network license server via Internet to verify, the other is connecting the firewall to the internal network LMS (License Management System) via LAN to verify.You can choose one of the two ways according to the need.

- The way that used to verify validity via public network license server is applicable in some small private clouds or industry cloud scenarios. After the virtual firewall being connected to the public server, the server will verify validity of the license, (currently the public network server does not support the distribution and management of the license). If the cloned license is found or the virtual firewall is not connected to server to verify, the virtual firewall will be restarted in 30 days.
- The way that used to verify validity via LAN vLMS is applicable in the large-scale public cloud scenarios. After the virtual firewall being connected to the vLMS, the vLMS not only verifies the validation of license, but also support automatic distribution and management of license. If the cloned license is found, the server will recycle all virtual firewall licenses of either the clone or the cloned one and restart the virtual firewall; if the virtual firewall does not connect to the server to verify, it will restart in 30 days.

If you use CLI to connect to the license server, in any mode, use the command **exec connect** { **public-server** | **license-server***A.B.C.D***ssl-port** *port-number*} **vrouter***vrouter-name*.

For more information, see Connecting to License server. After connecting, you need to reboot system to make the license effective.

For more information about LMS, refer to 《License Management System User Guide》.

Notes:

- CloudEdge with version 5.5R7 or above must connect the LMS with the version 3.0 or above.
- If there are CloudEdges with 5.5R7 and the previous version, when LMS discovers the license cloning behavior, the CloudEdge with the previous version of 5.5R7 will be judged as cloning device.
- **Suggestion**: Please upgrade the LMS to version 3.0 or above, and then upgrade the CloudEdge to 5.5R7 before connecting to the LMS.

Managing a License Using CLI

This section describes how to apply, install and uninstall a license using command lines.

Generating a Request for License

To generate a request for license, in any mode, use the following command:

exec license apply applicant *string*

- *string* - Specifies the name of the applicant.

Installing/Uninstalling a License

After obtaining the license, to install it, in any mode, use the following command:

exec license install *license-string*

- *license-string* - Pastes the license string.

To uninstall a license, in any mode, use the following command:

exec license uninstall *license-name*

- *license-name* - Specifies the name of the license you want to uninstall.

After installing some licenses, you need to type the command **reboot** to reboot system.

The following licenses will take effect after the reboot and other licenses will take effect directly.

- After installing the following licenses for the first time, you need to reboot the system: Platform Trial, Platform, AV, AV Trial, IPS, IPS Trial, Botnet C&C Prevention, Botnet C&C Prevention Trial, Stoneshield, URL, Sandbox, Virtual CPU, LLB, IP Reputation.
- The system needs to be rebooted each time the following licenses are installed: AEL, VSYS.

Verifying the Licenses

For Hillstone CloudEdge virtual firewall, after installing the licenses, you need to connect to the LMS to verify the validity of licenses, in any mode, use the following command :

exec lms enable { **public** | **private ip** *A.B.C.D* **port** *port-number*} **vrouter** *vrouter-name*

- **public** – Specify the public LMS to verify the validity of license .
- **private** *A.B.C.D* – Specify the Intranet LMS to verify the validity of license and specifies its IP address. **Note**: If the actual deployed network topology is connected to the License server through a proxy server, specify the address and port of the proxy server here.
- **port** *port-number* – Specify the port number of LMS. The value ranges from 1 to 65535.
- **vrouter** *vrouter-name*: Specifies the VRouter name.

The license will take effect after the device is rebooted. If it has not been rebooted before, after successfully connecting to LMS, enter the command **reboot** to restart the device.



Notes: When you verify your license through public LMS, make sure that the interface connected to the public server is in the trust-vr zone and that you can access the Internet through the trust-vr zone.

Viewing License Summary Information

To view the license summary information, including the feature name, license state, license type, expiration and resource, in any mode, use the following command:

show license summary

For example:

```
hostname# show license summary
==================================================
Feature State Type Expiration Resource
--------------------------------------------------------------------------------
URL DB Authorized Service license 2020/03/05(Upgrade effective time expired) 1
APP signature Authorized Service license 2020/03/05(Upgrade effective time expired) NULL
IPS Authorized Service license 2020/03/05(Upgrade effective time expired) 1
AntiVirus Authorized Service license 2020/03/05(Upgrade effective time expired) NULL
VSYS Authorized Permanent license Permanent 5
Cloud sandbox Authorized Service license 2020/03/05(Upgrade effective time expired) 1
Platform Authorized Service license 2030/10/02(Upgrade effective time) NULL
QoS Expired Trial license 0 days left NULL
Host route No License NULL NULL NULL
SSL VPN No License NULL NULL NULL
IP Reputation No License NULL NULL NULL
Twin mode No License NULL NULL NULL
Botnet C&C Prevention No License NULL NULL NULL
Threat intelligence No License NULL NULL NULL
==================================================
```

The parameters in the results of above **show** command are explained as follows:

- Feature: Displays the names of all features that are controlled by the license.
- State: Displays the installation status or effective status of the license, including Expired, Authorized, To be effective and No License.
- Type : Displays the types of the license, including Permanent license, Service license, Subscribe license and Trial license.
- Expiration: Displays the expiration time of the license, which is different for different types of licenses:
    - Permanent license: "Permanent" indicates no expiration time.
    - Service license: "Upgrade effective time expired" indicates that the feature is available, but the upgrade effective time of the signature database has expired and the signature database cannot be upgraded. "Upgrade effective time" indicates that it's within the upgrade effective time of the signature database.
    - Subscribe license: "2021/08/30 to 2021/09/28 (29 days left)" indicates that the feature can be used for 29 days within the time range.
    - Trial license: "2 days left" indicates that the feature can be used for 2 days. "0 days left" indicates that the feature is expired and the state is shown as Expired.
- Resource: Displays the number of resources available for this feature, such as the number of SSL VPN users or the number of IPSec VPN tunnels.

The priority of the license effective mechanism is: Permanent license > Service license > Subscription license > Trial license > Default license. For example, if the device installs both an IPSec VPN subscription license with 150 tunnels and an IPSec VPN permanent license with 30 tunnels, the permanent license takes effect and the number of tunnel resources is 30. If you uninstall the permanent license, the subscription license takes effect and the number of tunnel resources is 150.

Configuring HA Backup Device to Communicate with LMS through Master Device

For Hillstone CloudEdge virtual firewall, when CloudEdge is deployed as HA, if there is not enough public network IP available for backup devices to connect to the public network LMS, you can configure communication through the master device to connect to the public publix LMS to complete license verification. In this case, the master device will act as the proxy for the backup device, and the authentication requests between the backup device and the public LMS will be firstly forwarded to the master device through the HA link, and then to the public LMS server. This function is disabled by default. To enable LMS connection through the master device, using the following commands in the global configuration mode of the master device:

lms master-auth-proxy { **enable** | **disable** }

- **enable** - Enable LMS connection through the HA master device. When enabled, the master device will act as the proxy for the backup device, and the authentication requests between the backup device and the public LMS will be firstly forwarded to the master device through the HA link, and then to the public LMS server.
- **disable** - Disable LMS connection through the HA master device. This function can be disabled when the backup device itself can connecte to the LMS.

Replacing the Digital Certificate used for Connecting CloudEdge and LMS

When CloudEdge is connected to LMS, digital certificates are used for authentication (two-way authentication for authenticating the connection while one-way authentication for distributing the connection). After the authentication is successful, CloudEdge and LMS are successfully connected. You need to create a trust domain in CloudEdge to store CA certificates, local certificates, and the private keys, which will be used for authenticating the connection between CloudEdge and LMS. To create a trust domain and configure certificates and private keys, refer to Configuring PKI.

LMS references the configured trust domain to obtain new certificates. In the global configuration mode, use the following command:

lms trust-domain*trust-domain-name*

- *trust-domain-name* – Specifies the name of the configured trust domain where new certificates and private keys are stored. If this parameter is not configured, the default built-in certificates are used.

View LMS Information

To view LMS information, in any mode, use the following command:

show lms

Example:

```
hostname(config)# show lms
================================================================
======
Server IP: 10.182.21.12
Server Port: 8001
VR: trust-vr
Master Auth Proxy status: Disable
Trust-domain:
Lock Time: Locked
Authentication Connection Status: Disconnected and waiting
for reconnection(The network is unreachable)
Distribution Connection Status: Disconnected and waiting for
reconnection(The network is unreachable)
================================================================
======
```



Notes: Lock Time has the following four statuses:

- When CloudEdge is connected to LMS, **Lock Time** is displayed as **Do not lock**.
- When CloudEdge is disconnected from LMS within 30 days, **Lock Time** is displayed as **After***time***hours**. The configuration will be locked when the value of *time* becomes 0.
- When CloudEdge is disconnected from LMS for more than 30 days, **Lock Time** is displayed as **Locked**. At this point, you cannot operate on the WebUI and cannot enter the global configuration mode of CLI. Please check the system configuration and network. The configuration can be unlocked only after CloudEdge is reconnected to LMS.
- When CloudEdge is disconnected from LMS for more than 30 days, restart the device. After the device is restarted, **Lock Time** is displayed as **Temporary unlocking**. You can operate the device within 8 hours. If the connection is not restored, the configuration will still be locked.

Batch Installing Licenses

When installing licenses to a large amount of devices, using this batch method will simplify the process and minimize the mistakes.

Batch Installing Procedure

To install licenses in batch, take the following steps:

1. If you require many licenses, you need provide the device serial numbers and license types information to Hillstone. For information about license, consult the local agent.

2. Hillstone generates license files according to your requests and send them to you in proper ways, like email.

3. When you receive the license files, copy them to a FAT32 USB disk under the directory named "\license" (the name must be in lower case). The license files cannot be changed; otherwise they are unable to be installed.

4. Install the licenses to all the devices in the USB disk. See the section below.

Installing a License

After copying the license files to the proper directory in the USB disk, insert the USB disk into the USB port of the device, the device automatically scans the USB disk and install the matched license. You can view the status by checking the LED lights.

Power on the device, wait until it shows login prompt.

Insert the USB disk into the USB port.

The device automatically scans the USB disk, searches for a license with the same serial number of the device, and installs it. The ALM light shows the installation status, as shown in the table below:

Status	ALM Indicator
Searching for a matched license from the directory "license" in USB disk.	Blinking green until installation completes
The installation is completed.	Restore to former status
No matched license is found.	Blinking red for 10 seconds and then restore to the former status.
No "license" directory is found.	No change.

Remove the USB disk from the device and you can install licenses to other devices using the same method.

All matched licenses can be installed into the devices. To avoid reinstallation, used licenses are removed from the "license" directory to a "license_installed" directory (automatically created).

Reboot system to make license effective.

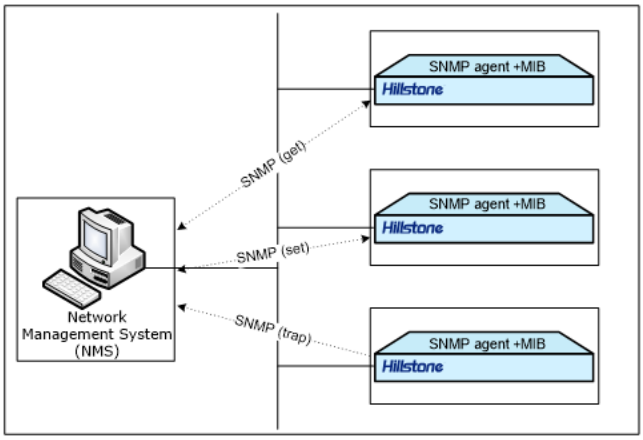
Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application layer protocol for managing devices on IP networks. It consists of four key components: Network Management System (NMS), Network Management Protocol, SNMP agent and Management Information Base (MIB).

- Network Management System (NMS): A software system which uses the network managers (like adventnet, solarwinds) to send requests, such as Get and Set, and receives the responses from the SNMP agent so that it can manage and monitor network devices.
- SNMP Agent: A software module on a managed network device, which sends the local device information to NMS.
- Network Management Protocol: It is used to exchange SNMP packets between NMS and SNMP agent. It supports three basic functions, which are GET, SET and Trap. Get is used by NMS to fetch the MIB value from the SNMP agent; Set is used by NMS to configure the MIB value of the SNMP agent; Trap is used by the SNMP agent to sent event notifications to NMS.
- Management Information Base (MIB): An information database maintained by SNMP Agent, which contains specific characteristics of managed network devices, comprises object variables. The object variables can be requested or set by NMS.

Hillstone SNMP

Hillstone devices support SNMP agent function, which receives requests from and responds the device information to NMS. Figure below illustrates how a NMS interacts with a security device via SNMP.



Supported RFCs

Hillstone security device supports the following SNMP versions:

- SNMPv1: Simple Network Management Protocol. See RFC-1157.
- SNMPv2: See the following RFCs:
  - RFC-1901 - Introduction to Community-based SNMPv2;
  - RFC-1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol;
  - RFC-1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol.
- SNMPv3: See the following RFCs:
  - RFC-2263 - SNMPv3 Applications;
  - RFC-2264 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
  - RFC-2265 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

SNMPv1 protocol and SNMPv2 protocol use community-based strings to limit the NMS to get device information. SNMPv3 protocol introduces a user-based security module for information security and a view-based access control module for access control.

Supported MIBs

The device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213, the Interfaces Group MIB (IF-MIB) using SMIv2 defined in RFC-2233, the User-based Security Model (USM) for version 3 defined in RFC-2574 and the View-based Access Control Model (VACM) defined in RFC-2575. Besides, StoneOS offers a private MIB, which contains the system information, IPsec VPN information and statistics information of the device. You can use the private MIB by loading it into a SNMP MIB browser on the management host.

Supported Traps

Trap is an asynchronous notification from SNMP agent to SNMP client. The following traps are supported in StoneOS:

- Warm start
- Authentication Ffailure
- Interface link down/up
- VPN SA negotiation status change
- HA status change
- System status changes, including CPU utilization over 80%, fan status change, memory low, etc.
- Network attacks, including ARP spoofing, IP Spoofing, SYN Flood attack, etc.
- Configuration changes

Configuring SNMP

Hillstone device provides the following SNMP configuration options:

- Enabling/Disabling the SNMP agent function
- Configuring the SNMP port number
- Configuring SNMP engineID
- Creating an SNMPv3 user group
- Creating an SNMPv3 user
- Configure the IP address of the management host
- Configuring the recipient of a SNMP trap
- Configuring sysContact
- Configuring sysLocation
- Specifying the VRouter on which the SNMP is enabled
- Configuring SNMP Server
- Clearing the ARP Table Information of SNMP Server
- Viewing the SNMP Server Information
- Viewing SNMP Information
- Enabling/Disabling the SNMP OID Statistics Function
- Viewing SNMP OID Statistics
- Clearing SNMP OID Statistics
- Exporting the SNMP MIB file

Enabling/Disabling the SNMP Agent Function

By default, the SNMP agent function is disabled. To enable the function, in the global configuration mode, use the following command:

snmp-server manager

To disable it, use the command **no snmp-server manager**.

Configuring the SNMP Port Number

To specify the port number of the SNMP agent, in the global configuration mode, use the following command:

snmp-server port *port-number*

- *port-number* - Specifies the port number. The value range is 1 to 65535. The default value is 161.

Configuring SNMP Engine ID

SNMP EngineID is a unique identifier for the SNMP engine. The SNMP engine is the essential component of the SNMP entity (NMS or network devices managed by SNMP). The functions of the SNMP engine are sending/receiving SNMP messages, authenticating, extracting PDU, assembling messages, communicating with SNMP applications, etc.

To configure the SNMP engineID of the local device, in the global configuration mode, use the following command:

snmp-server engineID *string*

- *string* - Specifies the engineID. The length is 1 to 23 characters.

Creating an SNMPv3 User Group

To configure a SNMPv3 user group, in the global configuration mode, use the following command:

snmp-server group *group-name* **v3 {noauth | auth | auth-enc} [read-view {mib2 | privmib | vacm | usm}] [write-view usm]**

- *group-name* - Specifies a name for the user group. The value range is 1 to 31 characters.
- **noauth** | **auth** | **auth-enc** - Specifies the security level of the user group. The security level determines the security mechanism used when handling a SNMP packet. **noauth** means no authentication nor encryption; **auth** means it requires MD5 or SHA authentication; **auth-enc** indicates that it uses MD5 or SHA authentication and AES or DES packet encryption.
- **read-view** {**mib2** | **privmib** | **vacm** | **usm**} - Specifies the read-only MIB view names of the user group. The SNMPv3 user group can read the specified MIB, including the public MIB defined in RFC-1213 and RFC-2233 (**mib2**), Hillstone Networks private MIB (**privmib**), the View-based Access Control Model MIB defined in RFC-2575 (**vacm**) and the User-based Security Model MIB for version 3 defined in RFC-2574 (**usm**). If this parameter is not specified, the SNMPv3 user group can read all MIB views.
- **write-view usm** - Specifies the writable MIB view names of the user group. The SNMPv3 user group can modify the User-based Security Model MIB for version 3 defined in RFC-2574 (**usm**). If this parameter is not specified, the SNMPv3 user group can modify all MIB (USM) views.

The system allows up to five user groups, each of which with a maximum of five users. To delete the specified user group, in the global configuration mode, use the command **no snmp-server group** *group-name*.

Creating an SNMPv3 User

To configure a SNMPv3 user, in the global configuration mode, use the following command:

snmp-server user *user-name* **group** *group-name* **v3 remote** *A.B.C.D/M* [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* - Specifies a name for the user. The value range is 1 to 31 characters.
- **group** *group-name* - Specifies a configured user group to the user.

- **remote** *A.B.C.D/M* - Specifies the IP address of the remote management host and network mask.
- **auth-protocol** {**md5** | **sha**} - Specifies that the user should be authenticated with MD5 or SHA algorithm. If this parameter is not specified, no authentication nor encryption is required for the user.
- **auth-pass** - Specifies authentication password. Use 8 to 40 characters.
- **enc-protocol** {**des** | **aes**} - Specifies that the user is encrypted with DES or AES.
- *enc-pass* - Specifies the encryption password. Use 8 to 40 characters.

The system allows up to 25 users. To delete the specified user, in the global configuration mode, use the command **no snmp-server user** *user-name*.

Configuring the IP Address of the Management Host

To configure the management host's address, in the global configuration mode, use the following command:

snmp-server host { *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *ip-address* | *ip-address/mask* | **range** *start-ip end-ip* - Specifies the IP address or IP range of the management host.
- **version** [*1* | *2c*] - Specifies that SNMP version is SNMPv1 (1) or SNMPv2C (2c).
- **community** *string* - Community strings are shared password between the managing process and agent process, therefore, an SNMP packet whose community string does not match that of the security device will be dropped. Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.

- **ro** | **rw** - Specifies the read and write privileges of community string. The **ro** (read-only) community string can only read MIB; **rw** (read and write) community string can read and change MIB. This is optional. By default, community string has read-only privilege.
- **version** *3* - Specifies that the SNMP version is version 3.

To delete the specified management host, in the global configuration mode, use the command **no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*}.

Configuring Recipient of SNMP Trap

To configure the recipient of the SNMP trap packets, in the global configuration mode, use the following command:

snmp-server trap-host *host-ip* [**source-ip** *ip-address*] {**version** {**1** | **2c**} **community** *string* | **version 3 user** *user-name* **engineID** *string* } [**port** *port-number*]

- *host-ip* - Specifies the IP address of SNMP trap recipient.
- **source-ip** *ip-address* – Specifies the source IP address that sends SNMP trap packets.
- **port***port-number* – Specifies the host port number used to receive trap packets. Valid values: 1 to 65535. Default value: 162.
- **version** {**1** | **2c**} – Specifies the SNMP version used to send trap packets. It can be SNMPv1 or SNMPv2C.
- **community***string* – Specifies the community string of SNMPv1 or SNMPv2C.
- **version 3** – Specifies to use SNMPv3 to send trap packets.
- **user***string* – Specifies the SNMPv3 user name.
- **engineID***string* – Specifies the engineID of trap recipient.

To delete the specified trap recipient host, in the global configuration mode, use the command **no snmp-server trap-host** *host-ip* [**source-ip**].



Notes: In the HA environment, the backup device does not synchronize with the source IP address (**source-ip**) configured in the primary device for sending SNMP trap packets. To specify the source IP address for the added trap host to send SNMP trap packets, you can use the**snmp-server trap-host** *host-ip* **source-ip** *ip-address* command in the backup device.

Configuring sysContact

sysContact specifies the contact name for this managed device (here refers to the security device), as well as information about how to contact this person.

To configure a sysContact, in the global configuration mode, use the following command:

snmp-server contact *string*

- *string* - Specifies the contact string. You can specify up to 255 characters.

To delete the contact, in the global configuration mode, use the command **no snmp-server contact**.

Configuring sysLocation

sysLocation specifies the physical location of this managed device (here refers to the security device).

To configure sysLocation, in the global configuration mode, use the following command:

snmp-server location *string*

- *string* - Specifies the location string. You can specify up to 255 characters.

To delete the sysLocation, in the global configuration mode, use the command **no snmp-server location**.

Specifying the VRouter on Which the SNMP is Enabled

You can specify the VRouter on which the SNMP function is enabled. To specify the VRouter, in the global configuration mode, use the following command:

snmp-server vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of the VRouter.

To disable the SNMP function in the VRouter, in the global configuration mode, use **no snmp-server vrouter**.

Configuring SNMP Server

You can configure the SNMP server to get the ARP information through the SNMP protocol. To configure the SNMP server, in the global configuration mode, use the following command:

arp-mib-query server *ip-address* **community** *string* [**vrouter** *vrouter-name*] [**source** *interface-name*] [**port** *port-number*] [**interval** *value*]

- *ip-address* – Specifies the IP address of SNMP server.
- **community** *string* – Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.
- **vrouter** *vrouter-name* – Specifies the name of VRouter.
- **source** *interface-name* – Specifies the name of the source interface for receiving ARP information on the SNMP server.
- **port** *port-number* – Specifies the port number of SNMP server. The value range is 1 to 65535, the default value is 161.
- **interval** *value* – Specifies the interval for receiving ARP information on the SNMP server. The value range is 5 to 1800 seconds, the default value is 60 seconds.

To delete the SNMP server, use the command **no arp-mib-query server** *ip-address*.

Clearing the ARP Table Information of SNMP Server

To clear the ARP table information of SNMP server, in any mode, use the following command:

clear arp-mib-query

Viewing the SNMP Server Information

To view SNMP server information, in any mode, use the following commands:

- Show SNMP server status: **show snmp-server**
- Show the ARP table information of the SNMP server: **show snmp-group**
- Show SNMP server configurations: **show snmp-user**

Viewing SNMP Information

To view SNMP configurations, in any mode, use the following commands:

- Show SNMP configurations: **show arp-mib-query status**
- Show SNMP configurations: **show arp-mib-query table** [*ip-address*]
- Show SNMP configurations: **show configuration arp-mib-query**

Entering the SNMP Agent Configuration Mode

To enter the SNMP agent configuration mode, in global configuration mode, use the following command:

snmp-agent

Enabling/Disabling the SNMP OID Statistics Function

OID (Object Identifier) is an address used to identify managed devices and their statuses. It is represented as a huge number of strings, such as .1.3.6.1.4.1.28557.2.2.1.32. SNMP OIDs are organized in a hierarchical n-ary tree structure with individual variable identifiers. This tree structure contains all the manageable features of all the products arranged in it. Each branch of this tree has a number and a name, and each point is named after the complete path—from the top of the tree down—that leads to that point.

The SNMP OID Statistics function collects basic information about SNMP agent OID to help you quickly troubleshoot SNMP issues. The system provides three types of SNMP OID Statistics

functions: basic information statistics of OID, detailed information statistics for all OIDs of a specified monitor IP, and detailed information statistics for OIDs of all latest monitor IPs. You can enable these three functions at the same time.

By default, the SNMP OID Statistics function is disabled. To enable this function, in SNMP agent configuration mode, use the following command:

snmp-agent statistics {**generic** | **monitor-ip** | **recently**}

- **generic** - Enable the basic information statistics of OID.
- **monitor-ip** - Enable detailed information statistics for all OIDs of a specified monitor IP.
- **recently** - Enable detailed information statistics for OIDs of all latest monitor IPs.

In SNMP agent configuration mode, use the following command to disable the specified SNMP OID Statistics function:

no snmp-agent statistics [**generic** | **monitor-ip** | **recently**]

- **generic** - Disable the basic information statistics of OID.
- **monitor-ip** - Disable detailed information statistics for all OIDs of a specified monitor IP.
- **recently** - Disable detailed information statistics for OIDs of all latest monitor IPs.
- If you do not specify the **generic** | **monitor-ip** | **recently** parameter, all SNMP OID statistics functions are disabled.

Viewing SNMP OID Statistics

When the basic information statistics of OID is enabled, you can use the following command in any mode to view basic statistics of all OIDs and specified OID:

- To view basic statistics information of all OIDs: **show snmp-agent statisticsgeneric**

  Example:

```
hostname# show snmp-agent statistics generic
10.160.25.181
```

```
================================================

Messages delivered to the SNMP entity 3  (Indicates that the SNMP entity transmits 3 messages)

SNMP PDUs which had noError 3  (Indicates that SNMP PDUs have a total of 3 operations with no errors)

GetRequest-PDU accepted and processed 0  (Indicates that the number of Get requests is 0. GetRequest-PDU indicates the operation name of SNMP PDU and 0 indicates the number of operations)

GetNextRequest-PDU accepted and processed 0  (Indicates that the number of Get Next requests is 0)

GetBulkRequest-PDU accepted and processed 0  (Indicates that the number of Get Bulk requests is 0)

Set-PDU accepted and processed 0  (Indicates that the number of Set is 0)

Trap-PDU sent 0  (Indicates that Trap-PDU was sent 0 times)

Trap2-PDU sent 3  (Indicates that Trap2-PDU was sent 3 times)
```

- To view basic statistics of specified OID: **show snmp-agent statistics oid***oid-string***generic**
    - *oid-string* - Specifies the value of the OID string to be viewed. The string ranges from 2 to 256 characters in length, such as .1.3.6.1.4.1.28557.2.2.1.32.

Example:

```
hostname# show snmp-agent statistics oid .1.3.6.1.4.1.28557.3.19 generic

.1.3.6.1.4.1.28557.3.19

================================================

Messages delivered to the SNMP entity 4  (Indicates that the SNMP entity transmits 4 messages)

SNMP PDUs which had noError 4  (Indicates that SNMP PDUs have a total of 4 operations with no errors)
```

When detailed information statistics for all OIDs of a specified monitor IP is enabled, you can use the following command in any mode to view detailed statistics for all OIDs of a specified monitor IP:

show snmp-agent statistics ip*ip-address*

- *ip-address* - Specifies the IP address to be viewed. This IP address needs to be predicted by using the Tab key. The predicted IP address needs to undergone at least 1 SNMP basic operation, such as Set and Get. If you enter any other IP address, an error message "IP address unrecognized" will be displayed.

Example:

```
hostname# show snmp-agent statistics ip ?
10.160.25.181 SNMP detail statistics monitor-ip  (Displays the IP address of the SNMP server connected to the device)
10.160.28.169 SNMP detail statistics monitor-ip
hostname# show snmp-agent statistics ip 10.160.28.169
OID Type Time(ms) Result
================================================
.1.3.6.1.4.1.28557.2.26.1.2.1.5.4 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.26.1.2.1.5.4 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.27.1.1.0 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.27.1.1.0 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.27.1.1.0 getnext 0 NOERROR
```

When detailed information statistics for OIDs of all latest monitor IPs is enabled, you can use the following command in any mode to view detailed statistics for OIDs of all latest monitor IPs is enabled:

show snmp-agent statistics recently-detail

Example:

```
hostname# show snmp-agent statistics recently-detail
```

```
OID ADDR Type Time(ms) Result
=====================================================
.1.3.6.1.4.1.28557.2.2.1.4.0 10.160.28.169 getnext 18
NOERROR
.1.3.6.1.4.1.28557.2.2.1.4.0 10.160.28.169 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.2.1.6.0 10.160.28.169 getnext 0 NOERROR
.1.3.6.1.4.1.28557.2.2.1.7.0 10.160.28.169 getnext 18
NOERROR
```

You can use the following command in any mode to view the statistics status of SNMP OID:

show snmp-agent statisticsstatus

Example:

```
hostname# show snmp-agent statistics status
SNMP generic statistics is off   (The function of basic information statistics of OID is enabled)
SNMP detail recently statistics is off   (The function of detailed information statistics for all OIDs of a specified monitor IP is disabled)
SNMP detail monitor-ip statistics is on   (The function of detailed information statistics for OIDs of all latest monitor IPs is disabled)
```

Clearing SNMP OID Statistics

You can use the following command in any mode to clear all statistics of SNMP OID:

clear snmp-agent statistics

Exporting the SNMP MIB File

To export the SNMP MIB file to the FTP/FTPS/SFTP server, in execution mode, use the following command:

export snmp mibto {**ftp** | **ftps** | **sftp**} **server***ip-address* [**vrouter***vrouter-name*] [**user***user-name***password***password*] [*file-name*]

- *ip-address* - Specifies the IP address of the FTP/FTPS/SFTP server.
- *vrouter-name* - Specifies the name of the virtual router.
- **user***user-name***password***password* - Specifies the username and password used to access the FTP/FTPS/SFTP server.
- *file-name* - Specifies the name of the SNMP MIB file to be exported.

To export the SNMP MIB file to the TFTP server, in execution mode, use the following command:

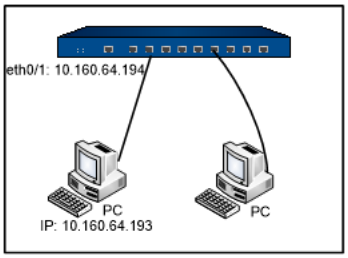
export snmp mib totftp server*ip-address* [**vrouter***vrouter-name*] [*file-name*]

SNMP Configuration Examples

This section provides two SNMP configuration examples.

Requirements

The goal is to connect the NMS (PC with IP address 10.160.64.193) to a security device on interface eth0/1 (IP: 10.160.64.194), as shown below:



- Example 1: Use NMS (PC of 10.160.64.193) to manage the security device through SNMPv2C with community string "public". In addition, the device is allowed to send trap packets to NMS with community string "private".
- Example 2: Use PC of IP 10.160.64.193 to manage the security device through SNMPv3, with security level of MD5 authentication (password: password1) and DES encryption (pass-

word: password2). PC can read MIB-II and only has the right to modify usm MIB. Besides, the security device is allowed to send trap packets.

Example 1

Take the following steps:

Step 1: Configure the security device:

```
To enter the global configuration mode:
hostname# configure
To enable the SNMP service on the interface:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
To enable SNMP of the device:
hostname(config)# snmp-server manager
To configure community and access privilege:
hostname(config)# snmp-server host 10.160.64.193 version 2c community public ro
To configure sysContact and sysLocation:
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
To allow sending trap packets to NMS 10.160.64.193 with community string "private":
hostname(config)# snmp-server trap-host 10.160.64.193 version 2c community private
```

Step 2: Configure Network Management System (NMS).

Example 2

Step 1: Configure the security device:

```
To enter the global configuration mode:
```

```
hostname# configure
To enable the SNMP service on the interface:
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
To enable SNMP of the device:
hostname(config)# snmp-server manager
To configure the local engineID:
hostname(config)# snmp-server engineID hillstone
To specify that the NMS can only read MIB-II but has
write privilege over usm MIB:
hostname(config)# snmp-server group group1 v3 auth-enc read-view mib2 write-view
usm
To specify user with MD5 authentication and DES encryp-
tion:
hostname(config)# snmp-server user user1 group group1 v3 remote 10.160.64.193
auth md5 password1 enc des password2
To configure address of NMS:
hostname(config)# snmp-server host 10.160.64.193 version 3
To configure trap recipient host so that it can send
trap packets to NMS:
hostname(config)# snmp-server trap-host 10.160.64.193 version 3 user user1 engineID
remote-engineid
To configure sysContact and sysLocation:
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
```

Step 2: Configure Network Management System (NMS).

Network Configuration Protocol (NETCONF)

Network Configuration Protocol (NETCONF) provides a mechanism for managing network devices. You can add, modify, and delete configurations of network devices, and obtain configuration and status information of network devices. Through NETCONF, network devices provide standard application programming interfaces (API). Applications can directly use these application programming interfaces to send and obtain configurations from network devices.

Comparison between NETCONF and SNMP:

Function	SNMP	NETCONF
Configuration management	SNMP does not provide a locking mechanism.	NETCONF provides a locking mechanism to avoid configuration conflicts arising from multi-user operations.
Inquiry	You can inquire about one or more nodes of the table through multiple interactions with the system.	You can inquire about all configurations of the system.
Extensibility	Poor extensibility	Good extensibility. NETCONF adopts a layered architecture and each layer is independent. Therefore, the impact on the upper-layer protocol will be minimalized when you extend a layer of NETCONF. Also, NETCONF adopts the XML, which allows the protocol to be extensible in terms of management ability and system compatibility.
Security	Take the latest SNMPv3 as an example. SNMPv3 only provides the user-based	NETCONF exploits current security protocols to provide security protection. It is not bound to a specific security protocol. Therefore, in practice, NETCONF is more flexible than SNMP.

Function	SNMP	NETCONF
	security module and cannot be added to other security modules.	**Note:** SSH is the priority at the NETCONF transport layer. XML message is carried by SSH protocol.

Through the NETCONF client, you can modify the configuration of Hillstone devices and obtain configuration and status information. You can configure the following function modules:

- Object module: You can create/delete/edit address book and host book through the NETCONF client.
- Network module: You can create/delete/edit zone, interface, DNS server, DNS proxy, DHCP, destination route, source route, policy route, OSPF, BGP, IPsec VPN, and SSL VPN through the NETCONF client.
- Policy module: You can create/delete/edit a policy, SNAT, and DNAT through the NETCONF client.



Notes:

- NETCONF function requires you to configure the login type of administrators and the trusted host as NETCONF, and the management method of interfaces as NETCONF. It is recommended to configure the three options before you enable NETCONF.
- When the root VSYS enables NETCONF, you can configure the login type of non-root administrators as NETCONF to enable NETCONF on non-root VSYS.

Enabling/Disabling the NETCONF Agent

By default, the NETCONF agent function is disabled.

To enable the NETCONF agent, in the global configuration mode, use the following command:

netconf-manager enable

To disable the NETCONF agent, in the global configuration mode, use the following command:

no netconf-manager enable

Enabling/Disabling the NETCONF candidate

NETCONF candidate enables you to modify the configuration of the current device but apply the modification later so that the current service traffic is not influenced. You can modify the configuration of the candidate, and replace the current configuration with the candidate configuration according to your own needs. The replacement takes effect immediately. By default, the NETCONF candidate is disabled.

To enable the NETCONF candidate function, in the global configuration mode, use the following command:

netconf-manager candidate

To disable the NETCONF candidate function, in the global configuration mode, use the following command:

no netconf-manager candidate

Configuring the NETCONF Timeout

You can perform operations such as offering configuration to a Hillstone device through the NETCONF client. If you do not perform any operations on the NETCONF client for a certain amount of time, you will be required to log in again to perform subsequent operations. To configure the timeout period, in the global configuration mode, use the following command:

netconf-manager timeout *value*

- *value* – Specifies the response timeout period for the NETCONF client. The value range is from 5 to 30 minutes. The default value is 10 minutes.

Viewing NETCONF Agent Configuration Information

To view configuration information of NETCONF agent, in any mode, use the following command:

show netconf-manager

HSM Agent

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. HSM system consists of three modules: HSM Agent, HSM Server and HSM Client. After deploying these modules and establishing security connection, you can use the HSM Client to view logs, statistics and attributes of managed security devices, as well as monitor system status and traffic information.

StoneOS running on each security device is designed with an HSM agent. After configuring this agent, the device can connect to the HSM server and will be managed and controlled by the server.

In addition, firewall can also send the following information to HSM:

- Interface information, including latency, jitter, packet loss rate, etc.
- Application data information on the interface, including application latency, jitter, upstream and downstream packet loss rate, etc.

You can use command lines or WebUI to configure HSM agent (Hillstone SR Series only supports WebUI). The HSM agent configurations include:

- Configuring HSM agent
- Specifying a trust domain
- Changing Digital Certificate
- Enabling/Disabling HSM agent
- Viewing HSM agent configurations



Tip: For more information about HSM, see Hillstone Security Management™ User Guide.

Configuring HSM Agent

HSM agent on the security device allows HSM server to connect to and manage it.

To specify the IP address of HSM server, in the global configuration mode, use the following command:

network-manager host *ip-address*

- *ip-address* - Specifies the IP address of HSM server. This address cannot be 0.0.0.0, 255.255.255.255 or a multicast address.

To configure the port number of HSM server, in the global configuration mode, use the following command:

network-manager host port *port-number*

- *port-number* - Specifies the port number of HSM server. The value range is 1 to 65535. The default value is 9091.

To configure the connection interface of the HSM server, in the global configuration mode, use the following command:

network-manager host source *interface-name*

- **source** *interface-name* - Specifies the connection interface of HSM server.

To modify the registering mode of the HSM server to plain mode (unencrypted), in the global configuration mode, use the following command:

network-manager host plain

To modify the registering mode of the HSM server to encrypted mode, in the global configuration mode, use the following command:

no network-manager host plain

To specify the password of HSM server, in the global configuration mode, use the following command:

network-manager host password *password*

- *password* - Specifies the password. HSM server uses this password to authenticate the device. The length is 1 to 31 characters.

To specify the VRouter on which the HSM agent is enabled, in the global configuration mode, use the following command:

network-manager host vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To clear the configuration of HSM server, in the global configuration, use the following command:

no network-manager host

To ensure that the device can communicate normally with the HSM server in the NAT environment, you can configure the IP addresses of the FTP servers and log server. By default, the IP address of the FTP server is the IP address of the HSM server, the port numb is 21; the IP address of the log server is the IP address of the HSM server, the port number is 514.

To configure the IP address and the port number of the FTP server, in the global configuration mode, use the following command:

network-manager host ftp-server *ip-address* [**port** *port-number*]

- *ip-address* – Specify the IP address of the FTP server.
- *port-number* – Specify the port number of the FTP server.

In the global configuration mode, use the following command to restore the following values to the default ones:

no network-manager host ftp-server [**port**]

To configure the IP address and the port number of the log server, in the global configuration mode, use the following command:

network-manager host syslog-server *ip-address* [**secure-tcp**] [**port** *port-number*]

- *ip-address* – Specify the IP address of the log server.
- **secure-tcp** – If this parameter is specified, system will transfer logs enerypted to HSM.
- *port-number* – Specify the port number of the log server.

In the global configuration mode, use the following command to restore the following values to the default ones:

no network-manager host syslog-server [**secure-tcp**][**port**]

Changing Digital Certificate

Digital certificates are used for bidirectional authentication when the device is connected to the HSM server. After bidirectional authentication succeeds, the device connects to the HSM server. Create a trust domain to store the new CA certificate and the device can use the certificate to verify the certificate provided by the HSM server. Create another trust domain to store the new local certificate and the private key so that the HSM server can verify the certificate. If the local certificate and private key are not configured, the device implements one-way authentication with the HSM server: That is to say, the device verifies the certificate provided by the HSM server and not vice versa. Import CA certificate, local certificate, and private key to the trust domain and then you can change the digital certificates. To create a trust domain, import certificates and private key, see PKI.

Reference the existing trust domain to obtain a new CA certificate, in the global configuration mode, use the following command:

network-manager host trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the existing trust domain that stores the new CA certificate in the system. If this parameter is not specified, the system uses the default built-in CA certificate.

Reference the existing trust domain to obtain a new local certificate and private key, in the global configuration mode, use the following command:

network-manager agent trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the existing trust domain that stores the new local certificate and private key in the system. If this parameter is not specified, the system uses CA certificate to implement one-way authentication with the HSM server.



Notes: If the HSM server does not support bidirectional authentication, the HSM server will authenticate the device by default after the device provides the local certificate.

Enabling/Disabling HSM Agent

After configuring HSM server parameters on the device, you need to enable the HSM agent service, which by default is disabled.

To enable HSM agent, in the global configuration mode, use the following command:

network-manager enable

To disable the HSM agent, in the global configuration mode, use the following command:

no network-manager enable

Viewing HSM Agent Configuration Information

To view configuration information of HSM agent, in any mode, use the following command:

show network-manager

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of operating systems based on UDP with dedicated port 123.



Tip: For more information about NTP synchronization, see RFC1305.

For a security device, system time influences many functional modules, like VPN tunnel, schedule and signature certificate, etc. NTP is used to synchronize the system time with NTP server. There are two ways to synchronize time: manual setting and using NTP.



Notes: When using the signature license for the first time, do synchronize the system time with the computer time in advance.

Configuring NTP

Configuring System Clock Manually

To configure the system clock manually, in the global configuration mode, use the following command:

clock time *HH:MM:SS Month Day Year*

- *HH:MM:SS Month Day Year* - Specifies the system clock. *HH, MM* and *SS* indicate hour, minute and second respectively, *Month*, *Day* and *Year* indicate month, day and year respectively.

Configuring Time Zone Manually

The system provides multiple predefined time zone. To configure time zone more accurately, you can configure a customized time zone, and configure summer time for the customized time zone.

The default time zone of the system is GMT+8. To configure a time zone, in the global configuration mode, use the following command:

clock zone {*timezone-name* | *cus-timezone-name hours minutes*}

- *timezone-name* - Specifies the name of the pre-efined time zone.
- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- *hours minutes* - Specifies the offset to UTC (Universal Time Coordinated). The value range of *hours* is -13 to 12; the value range of *minutes* is 0 to 59.

For example, to configure a customized time zone named test, and set the offset to UTC to 6 hours and 30 minutes, use the following command:

```
hostname(config)# clock zone test 6 30
```

Configuring Summer Time

Summer time is a local time regulation for saving energy. According to the law issued by the authority, during summer the clock will jump forward for one hour, and will jump backward for one hour when the summer ends. You can specify the absolute time period and the periodic time period of the summer time for the customized time zone.

To specify the absolute time period of the summer time, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **date** *start-date start-time end-date end-time* [*compensation-time*]

- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **date** – Specifies the absolute time period of the summer time.
- *start-date* - Specifies the start date of summer time. The format is month/day/year, for example, 7/20/2011.
- *start-time* - Specifies the start time of summer time. The format is hour:minute, for example, 10:30.
- *end-date* - Specifies the end date of summer time. The format is month/day/year, for example, 7/20/2011.
- *end-time* - Specifies the end time of summer time. The format is hour:minute, for example, 10:30.
- *compensation-time* – Specifies the compensation time when the summer time starts. The default value is 0. For example, when the summer time starts, in some places the clock will jump forward for 1 hour and 30 minutes; when the summer time ends, the clock will jump backward for 1 hour and 30 minutes. In such a case, the compensation time is 1 hour and 30 minutes. The format is hour:minute, such as 1:30.

For example, to configure a customized time zone named test, set the start time and end time of summer time to 6/22/2011 10:30 and 9/23/2011 10:00 respectively, and the summer time is 2 hours and 30 minutes earlier than the non-summer time, use the following command:

```
hostname( config) # clock summer-time test date 6/22/2011
10:30 9/23/2011 10:00 2:30
```

To specify the periodical time period of the summer time, i.e. executing the summer time in a specified time period in every year, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **recurring** { [**Mon**] |[…] | [**Sun**] }{**after** | **before**}*start-day start-month start-time* { [**Mon**] |[…] |[**Sun**]} {**after** | **before**}*end-day end-month end-time* [**compensation-time**]

- *cus-timezone-name* – Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **recurring** – Specifies the periodical time period of the summer time.
- { [**Mon**] |[…] | [**Sun**] }{**after** | **before**}*start-day start-month start-time* – Specifies the start time of the periodical time period. For example, Mon before 22 6 10:30 means the start time of the summer time in every year is 10:30 on the Monday of the first week before 22nd, June.
- { [**Mon**] |[…] |[**Sun**]} {**after** | **before**}*end-day end-month end-time* - Specifies the end time of the periodical time period. For example, Fri after 23 9 10:00 means the end time of the summer time in every year is 10:00 on the Friday of the first week after 23rd, September.
- *compensation-time* – Specifies the compensation time of the summer time when the summer time takes effect. The default value is 0. For example, when the summer time starts, the system adjust the time of certain zones 1.5 hours ahead, and when the summer time ends, adjust the time of certain zones 1.5 hours back. 1.5 hours is the compensation time you defined. The format is "hour:minute", for example, 1:30.

For example, to configure a customized time zone named test, set the start time as 10:30 on the Monday of the first week before 22nd, June and set the end time as 10:00 on the Friday of the first week after 23rd, September. The time during the summer time is 2.5 hours ahead.

```
hostname( config) # clock summer-time test recurring Mon
before 22 6 10:30 Fri after 23 9 10:00 2:30
```



Notes: The summer time may affect logs and modules that rely on time. For example, in the above example, when the summer time ends on 9/23/2011 10:00, the clock will jump backward for 2 hours and 30 minutes, i.e., jump backward to 7:30. Therefore, time range from 7:30 to 10:00 will appear twice on 9/23/2011.

To cancel the summer time configuration, in the global configuration mode, use the command **no clock summer-time** *cus-timezone-name* **date**.

Viewing System Clock Configuration Information

To view the time zone settings, in any mode, use the command **show clock**.

To view the summer time settings, in any mode, use the command **show config**.

Configuring NTP Service

NTP is used to synchronize the system clock with NTP server. The system supports the following NTP configurations:

- Enabling/Disabling NTP Service
- Configuring an NTP Sever
- Configuring the Max Adjustment Value
- Configuring the Query Interval
- Enabling/Disabling NTP Authentication
- Configuring NTP Authentication

Enabling/Disabling NTP Service

By default, NTP service on Hillstone devices is disabled.

To enable/disable NTP service, in the global configuration mode, use the following commands:

- Enable: **ntp enable**
- Disable: **no ntp enable**

Configuring an NTP Server

You can specify up to three NTP servers, one of which with keyword "prefer" is the primary NTP server, or, if no "prefer" is specified, the earliest configured NTP server is the first one for time synchronization.

To configure an NTP server, in the global configuration mode, use the following command:

ntp server {*ip-address* | *host-name*} [**key** *number*] [**source** *interface-name*] [**prefer**] [**vrouter** *vrouter-name*]

- *ip-address* | *host-name*- Specifies the IP address or host name of the NTP server. The length of the host name can be 1 to 127 characters.
- **key** *number* - Specifies the password of the NTP server if it requires so.
- **source** *interface-name* - Specifies the interface on which the security device sends and receives NTP packets.
- **prefer**- If more than one NTP servers are specified, use this keyword to determine the primary server.
- *vrouter-name* - Specifies NTP server for the specified VRouter.

To cancel the NTP server settings, use the command **no ntp server** {*ip-address* | *host-name*}.

Here is an example of configuring a NTP server:

```
hostname(config)# ntp server 10.160.64.5 prefer
```

Configuring the Max Adjustment Value

The maximum time adjustment value represents the acceptable time difference between the device system clock and the time received from an NTP server. The device only adjusts its clock

with the NTP server time if the time difference between its clock and the NTP server time is within the maximum time adjustment value.

To set the maximum adjustment value, in the global configuration mode, use the following command:

ntp max-adjustment *time-value*

- *time-value* - Specifies the time value. The value range is 0 to 3600 seconds. The value of 0 means no adjustment time. The default value is 400.

To restore to the default value, use the command **no ntp max-adjustment**.

Configuring the Query Interval

The device updates its clock with NTP servers at intervals of the value you set here.

To configure the query interval, in the global configuration mode, use the following command:

ntp query-interval *time-interval*

- *time-interval* - The query interval. The value range is 1 to 60 minutes. The default value is 5.

To restore to the default value, use the command **no ntp query-interval**.

Enabling/Disabling NTP Authentication

By default, NTP authentication is disabled.

To enable/disable NTP authentication, in the global configuration mode, use the following commands:

- Enable: **ntp authentication**
- Disable: **no ntp authentication**

Configuring NTP Authentication

If you choose to use NTP authentication, the security device only interact with servers that pass the authentication.

To configure NTP authentication key ID and key, in the global configuration mode, use the following command:

ntp authentication-key *number* **md5** *string*

- *number* - Specifies the key ID number. The value range is 1 to 65535.
- *string* - Specifies MD5 authentication key. The length is 1 to 31 characters.

To cancel the authentication private key settings, in the global configuration mode, use the command **no ntp authentication-key** *number*.

Viewing NTP Status

To view the current NTP configurations, in any mode, use the command **show ntp status**.

NTP Configuration Example

Requirements of this configuration example are:

- NTP server IP address is 10.10.10.10;
- Authentication private key ID and key are 1 and aaaa respectively;
- The query interval is 3 minutes;
- The maximum adjustment time is 5 seconds.

Configure the following commands on the device:

```
hostname(config)# ntp authentication-key 1 md5 aaaa
hostname(config)# ntp server 10.10.10.10 key 1 prefer
hostname(config)# ntp query-interval 3
hostname(config)# ntp max-adjustment 5
hostname(config)# ntp authentication
hostname(config)# ntp enable
hostname(config)# show ntp status
ntp client is enabled, authentication is enabled
ntp query-interval is 3, max-adjustment time is 5
```

```
ntp server 10.10.10.10, key 1, prefer
```

Password-free Login to CLI via WebUI

To improve the convenience of O&M on devices, the system supports the function of password-free login to the CLI via WebUI. After you log in to the device via WebUI, you can click the CLI icon in the upper-right corner. In the command window that appears, you can directly configure the device by using commands without the need to enter the username and password.



Notes: When you use the function:

- We recommend that you use Microsoft Edge or Chrome 45 and later to access the WebUI of the device.
- The management port of the device (some devices have a default MGT port), trusted host, and administrator need to enable the HTTP or HTTPS services.
- If the user is an administrator with a customized administrator role, it is necessary to enable CLI privileges for that administrator role. To enable CLI privileges for an administrator role, please refer to Specifying Administrator Role's Privileges.
- Logging in or out of the CLI generates corresponding event logs.

Configuring Maximum Number of Connections for CLI Window

You can configure the maximum number of connections for the CLI window, which indicates the maximum number of CLI windows that can be opened simultaneously on the same device. To do this, in global configuration mode, use the following command:

webconsole max-clients *number*

- *number* - Specifies the maximum number of connections for the CLI window. The maximum number varies based on the platform. By default, the maximum number is the maximum value that can be configured.

To remove the configuration of the maximum number of connections for the CLI window and restore the maximum number to the default value, in global configuration mode, use the **no web-console max-clients** command.

Viewing Configuration of CLI Window

To view the configuration of the CLI that is logged in from the WebUI without a password, including the current number and maximum number of connections for the CLI window, in any mode, use the following command:

show webconsole

Configuring Schedule

Schedules control the effective time for some functional modules, such as allowing a policy rule or NAT rule to take effect in a specified time, and controls the duration for the connection between a PPPoE interface and Internet. There are two types of schedule: periodic schedule and absolute schedule. The periodic schedule specifies a time point or time range by periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Creating a Schedule

To create a schedule, in the global configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* - Specifies a name for the schedule. The length of it can be 1 to 31 characters.

This command creates a schedule and leads you into the schedule configuration mode; if the schedule exists, you will enter its configuration mode directly.

To delete a schedule, use the command **no schedule** *schedule-name*. Note that you should unbind the schedule from all the functional modules before deleting it.

Configuring an Absolute Schedule

Absolute schedule is a time range in which periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is referenced by any module.

To configure an absolute schedule, in the schedule configuration mode, use the following command:

absolute {[**start** *start-date start-time*] [**end** *end-date end-time*]}

- **start** *start-date start-time* - Specifies the start date and time. *start-date* specifies the start date in the format of month/date/year, e.g. 10/23/2007; *start-time* specifies the start time in the format of hour:minute:second, e.g. 15:30:20. If this parameter is not specifies, it uses the present time.
- **end** *end-date end-time* - Specifies the end date and time. *end-date* specifies the finish date in the format of month/date/year, e.g. 11/05/2007; *end-time* specifies the finish time in the format of hour:minute:second, e.g. 09:00:00. If the parameters are not specifies, there is no end time for the absolute time.

To disable absolute schedule, use the command **no absolute**.

Configuring a Periodic Schedule

A periodic schedule is the collection of all the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into three types:

- Daily: The specified time of every day, such as Everyday 09:00:30 to 18:00:20.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00:15 to 13:30:45.
- Due: A continuous period during a week, such as from Monday 09:30:30 to Wednesday 15:00:05.

To specify a periodic schedule, in the schedule configuration mode, use the following command:

periodic {**daily** | **weekdays** | **weekend** | [**monday**] [···] [**sunday**]} *start-time* **to** *end-time*

- **daily** To specify a periodic schedule, in the schedule configuration mode, use the following command:
- **weekdays** - Workday (from Monday to Friday).
- **weekend** - Weekends (Saturday and Sunday).
- [**monday**] [···] [**sunday**] - Specifies particular days. For example, if you want Tuesday, Wednesday and Saturday, type the key words tuesday wednesday saturday.
- *start-time* - Specifies the start time in the format of hour:minute:second, e.g. 09:00:00.
- *end-time* - Specifies the end time in the format of hour: minute:second, e.g. 16:30:30.

Repeat the command to add more entries.

To delete a periodic entry, use the command **no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] [···] [**sunday**]} *start-time* **to** *end-time*.

To configure an entry which specifies a period of time in a week, in the schedule configuration mode, use the following command:

periodic {[**monday**] | [···] | [**sunday**]} *start-time* **to** {[**monday**] | [···] | [**sunday**]} *end-time*

- [**monday**] | [···] | [**sunday**] - Specifies the start day in a week.
- *start-time* - Specifies the start time in the format of hour:minute:second, e.g. 09:00:00.
- [**monday**] | [···] | [**sunday**] - Specifies the end day.
- *end-time* - Specifies the end time in the format of hour:minute:second, e.g. 16:30:30.

Repeat this command to add more entries.

To delete an entry, use the command **no periodic** {[**monday**] | [···] | [**sunday**]} *start-time* **to** {[**monday**] | [···] | [**sunday**]} *end-time*.



Notes: In both absolute schedule and periodic schedule, the interval between the Start time and the End time should not be less than 1 minute.

Configuring a Track Object

Track object is used to track if the specified object (IP address or host) is reachable and if the specified interface is connected, and if the specified object or link is congested. If the object is not reachable or the link is not connected, the system will directly conclude the track fails; if the object is reachable or the link is connected, the system will continue to detect if the object or link is congested based on packet delay or interface bandwidth. Track is mainly used in HA, PBR, LLB scenarios. By configuring track, you can assure the system is always selecting a comparatively healthy link.



Notes:

- When the track failed, the system will drop all the sessions to the track object.
- When the track object is congested, the system will still keep all the existing sessions to the object, but will not allow any new session.

To configure a track object, in the global configuration mode, use the following command:

track *track-object-name* [**local**]

- *track-object-name* - Specifies a name for the track object. The length of it can be 1 to 31 characters.
- **local** - If you enter this parameter, the system will not synchronize configuration of this track with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

This command creates the track object and leads you into the track object configuration mode; if the object exists, you will enter its configuration mode directly.

To delete the specified track object, use the following command:

no track *track-object-name*

You are allowed to track your object by using six protocols of ICMP, HTTP, ARP, DNS, TCP, and BFD. Besides, the object also can be tracked by counting the traffic information of specified interface.



Notes: Only in HA scenario can you track your object by using the BFD protocol.

Viewing the Track Objects Configuration Information

To view a track object configuration information, in any mode, use the following command:

show track*track-object-name*

- *track-object-name* - Specifies a name for the track object. The length of it can be 1 to 31 characters.

To view all the track objects configuration information, in any mode, use the following command:

show track

For example, when track interface status, you can view the interface name, how important this entry failure is to the judgment of tracking failure, interface status. Below is a return example:

```
hostname# show track
=============================================================-
=============================================================
Total track number: 3
Track name: test
------------------------------------------------------------------------------------------------------------------------
----------------------------------------
used type: not used; status: UNKNOWN; link status: UNKNOWN;
track ID: 1; local: no; hold: no; threshold: 255; delay threshold: 255; bandwidth threshold: 255;
if ID: 0; snat cnt: 0; dynamic-ping-msg-id: disable; hold notify: disable


track interface:
```

```
-------------------------------------------------------------------------------------------------------------------
---------------------------------------
Track interface weight status
-------------------------------------------------------------------------------------------------------------------
---------------------------------------
ethernet0/1 255 unknown
- - More - -
```

Track by ICMP Packets

To track an object using Ping packets, in the object configuration mode, use the following command:

icmp {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name* [**prior-used-srcip**]] [**weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the tracked object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface sending Ping packets.
- **interval** *value* - Specifies the interval of sending Ping packets . The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which determines the tracking fails. If the system does not receive response packets of the number specified here, it determines that the tracking has failed, namely, the destination is unreachable. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of Ping packets.
- **prior-used-srcip** – If the secondary IP is specified for the source interface and specifies the IP to be **prior-used-srcip**, system will use the IP to send track packets priorly. If the parameter is not specified, system will use default IP of the source interface to send track packets.

- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more Ping tracking entries.

To delete the specified tracking entry, use the following command:

no icmp {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Dynamic Ping Message ID

When an object is tracked by using Ping packets, the header ID of ICMP messages sent by the same track object is a fixed value. In this case, the ICMP messages may be blocked as DoS attacks by other intermediate security devices . Therefore, the track will fail. To solve this issue, the system supports the dynamic Ping message ID function. With this function enabled, the header ID of ICMP messages sent by the same track object is a dynamic value. To configure this function, use the following command in the object configuration mode:

dynamic-ping-msg-id {**enable** | **disable**}

- **enable** - Enable the dynamic Ping message ID function. With this function enabled, the header ID of ICMP messages sent by the same track object is a dynamic value.
- **disable** - Disable the dynamic Ping message ID function. With this function disabled, the header ID of ICMP messages sent by the same track object is a fixed value.

Track by IPv6 ICMP Packets

To track an object using Ping packets, in the object configuration mode, use the following command:

icmp6 {*ipv6-address* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name* [**prior-used-srcip** *ipv6-address*]] [**weight** *value*]

- *ipv6-address* | **host** *host-name* - Specifies the IPv6 address or host name of the tracked object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface sending Ping packets.

- **interval** *value* - Specifies the interval of sending Ping packets . The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which determines the tracking fails. If the system does not receive response packets of the number specified here, it determines that the tracking has failed, namely, the destination is unreachable. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of Ping packets.
- **prior-used-srcip** *ipv6-address* – If the secondary IP is specified for the source interface and specifies the IP to be prior-used-srcip, system will use the IP to send track packets priorly. If the parameter is not specified, system will use default IP of the source interface to send track packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more Ping tracking entries.

To delete the specified tracking entry, use the following command:

no ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by HTTP Packets

To track an object using HTTP packets, in the track object configuration mode, use the following command:

http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the track object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface of sending HTTP test packets.

- **interval** *value* - Specifies the interval of sending HTTP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 1.
- **src-interface** *interface-name* - Specifies the source interface of the HTTP packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more HTTP tracking entries.

To delete the specified tracking entry, use the following command:

no http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by ARP Packets

To track an object using ARP packets, in the track object configuration mode, use the following command:

arp {*A.B.C.D*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *A.B.C.D* - Specifies the IP address of the track object.
- **interface** *interface-name* - Specifies the egress interface of sending ARP test packets.
- **interval** *value* - Specifies the interval of sending ARP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more ARP tracking entries.

To delete the specified tracking entry, use the following command:

no arp {*A.B.C.D*} **interface** *interface-name*

Track by DNS Packets

To track an object using DNS packets, in the track object configuration mode, use the following command:

dns *A.B.C.D* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*] [**src-interface** *interface-name*]

- *A.B.C.D* - Specifies the IP address of track object.
- **interface** *interface-name* - Specifies the egress interface of sending DNS test packets.
- **interval** *value* - Specifies the interval of sending DNS packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value*- Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **src-interface** *interface-name* - Specifies the source interface of DNS test packets.

Repeat the command to configure more DNS tracking entries.

To delete the specified tracking entry, use the following command:

no dns *A.B.C.D* **interface** *interface-name* [**delay**]

Track by TCP Packets

To track an object using TCP packets, in the track object configuration mode, use the following command:

tcp {A.B.C.D | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of track object. The length of the host name can be 1 to 63 characters.
- **port** *port-number* - Specifies the destination port of the track object. The value range is 0 to 65535.
- **interface** *interface-name* - Specifies the egress interface for sending TCP test packets.
- **interval** *value* - Specifies the interval of sending TCP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of TCP test packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more TCP tracking entries. For one single track object, you cannot configure both the HTTP track on the host and TCP track on port 80 simultaneously.

To delete the specified tracking entry, use the following command:

no tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**delay**]

Track by BFD Packets

Bidirectional Forwarding Detection (BFD) can rapidly detect the forwarding connectivity of links or route IP addresses in the network.

In the HA scenario, the system can track the working status of the device by using BFD. If the track object fails, BFD can quickly detect the issue and notify the system to perform primary and secondary switchover. Compared with other monitoring methods, BFD enables millisecond-level

primary and secondary switchover, ensuring smooth data communication and effectively enhancing network reliability.

To track an object using BFD packets, in the track object configuration mode, use the following command:

bfd {**ipv6** *X:X:X:X::X* | *A.B.C.D*} **interface** *interface_name* **prior-used-srcip** {*X:X:X:X::X* | *A.B.C.D*} [**bfd-template** *bfd_template_name*] [**weight** *value*]

- {**ipv6** *X:X:X:X::X* | *A.B.C.D*} – Specifies the IPv6 address or IPv4 address of the track object.
- **interface** *interface_name* – Specifies the egress interface for sending BFD test packets.
- **prior-used-srcip** {*X:X:X:X::X* | *A.B.C.D*} – Specifies the IPv6 address or IPv4 address of the egress interface. This address needs to be configured as the management IP address of the secondary device to avoid that the secondary device fails to send BFD track packets, resulting in a failure to establish BFD sessions.
- **bfd-template** *bfd_template_name* – When using the BFD multi-hop mode, you need to specify the BFD multi-hop template name so that the template can be bound. If this parameter is not specified, it indicates that the BFD single-hop mode is used. For more information about BFD single-hop mode and multi-hop mode and how to create a BFD multi-hop template, see Configuring BFD Multi-hop Detection.
- **weight** *value* – Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

To delete the specified tracking entry, in the track object configuration mode, use the following command:

no bfd {**ipv6** *X:X:X:X::X* | *A.B.C.D*} **interface** *interface_name* **prior-used-srcip** {*X:X:X:X::X* | *A.B.C.D*} [**bfd-template** *bfd_template_name*]

Notes:

- Only one BFD track entry can be configured in the system and only the HA function can track the working status of the device by using BFD.
- After you configure a BFD track entry, you cannot configure other types of track entries.

Interface Status Track

To track interface status, in the track object configuration mode, use the following command:

interface *interface-name* [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no interface *interface-name*

Interface Bandwidth Track

To track interface bandwidth, in the track object configuration mode, use the following command:

bandwidth interface *interface-name* **direction** {**in** | **out** | **both**} **high-watermark** *value* **low-watermark** *value* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **direction** {**in** | **out** | **both**} - Specifies the traffic direction to be tracked. in indicates ingress, out indicates egress (the default direction), both indicates the both directions.

- **high-watermark** *value* **low-watermark** *value* – Specifies the high watermark and low watermark for the interface bandwidth. The value range is 1 to 100000000 kbps. When the interface bandwidth is below the specified high watermark, the system will conclude the link is normal; when the interface bandwidth exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the interface bandwidth is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.

- **interval** *value* - Specifies the tracking interval. The value range is 1 to 255 seconds. The default value is 3.

- **threshold** *value* – Specifies the threshold number which concludes the entry is congested. If the system detected interface overload for the times specified here in succession, it concludes the entry is congested. The value range is 1 to 255. The default value is 1.

- **weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no bandwidth interface *interface-name*

Interface Quality Track

To track the link state of specified interface by counter the sampling traffic , in the track object configuration mode, use the following command:

traffic-condition [**ipv6**] **interface** *interface-name* [**condition-threshold** *low-watermark high-watermark*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- **ipv6** – Specifies the interface quality track object as the IPv6 type. If this parameter is not specified, the interface quality track object is specified as IPv4 type by default.

- *interface-name* – Specifies the tracked interface name.
- **condition-threshold** *low-watermark high-watermark* – Specifies the threshold value of new session success rate. By default, the threshold low watermark is 30, and the threshold high watermark is 50. The value range is 0 to 100. During a track period, when the new session success rate is below the specified low watermark, system will conclude the track is failed; when the new session success rate exceeds the specified high watermark, system will conclude the track is successful; when the new session success rate is equal to or exceeds the low watermark, and equal to or below the low watermark, system will keep the previous track state.
- **interval** *value* – Specifies the duration of per track period. The unit is second. The value range is 1 to 255. The default value is 3. After a track period is finished, system will reset the tracked value of new session.
- **threshold** *value* – Specifies the threshold value which concludes the track entry is failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* – Specifies how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no traffic-condition [**ipv6**] **interface** *interface-name*

Configuring a Threshold

Threshold is used to conclude if the track object failed or is congested. When the total weight sum of the track entries that belong to the same category in the track object exceeds or equals to the corresponding threshold, the system will conclude the track object failed or is congested.

Monitor Object FailureThreshold

If the sum of weight values of all track entries exceeds or equals to a certain value, the system concludes that the tracking fails. The value is known as the track object failure threshold value.

To configure the track object failure threshold value, in the track object configuration mode, use the following command:

threshold *value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no threshold

Fail Close

With this function enabled, system will check application layer IPS, AV, content filtering and Web Content, application-layer behavior control. If you disable this feature , when the system resources is too low , such as CPU usage high, memory or data packets buffer residual capacity is insufficient, system will pass packets for controlling the resources utilization, so as not to affect other functions. By default, this function is disabled.

Enabling/Disabling Fail Close

To enable fail close, under global configuration mode, use the following command:

fail-close enable

To disable fail close, under global mode, use the command:

no fail-close enable



Notes: Fail close is not applicable for: FTP behavior control, web surfing, MSRPC/SUNRPC/DNS (UDP) check of IPS.

Viewing Fail Close Status

To view the fail close status, in any mode, use the following command:

show fail-close

Enabling/Disabling Application Layer Security Bypass

System supports to bypass the application layer functions, including Intrusion Prevention System, Anti Virus, and other application layer security protection function. To enable application layer security bypass, under global mode, use the command:

app-security-bypass

To disable application layer security bypass, under global mode, use the command:

no app-security-bypass



Notes: When the application layer security bypass and fail close are configured at the same time, the application layer security bypass has a higher priority.

Viewing Application Layer Security Bypass Status

To view the application layer security bypass status, in any mode, use the following command:

show app-security-bypass

Monitor Alarm

The monitor alarm function is designed to monitor the utilization of system resources, and issue an alarm according to the configuration. The current version supports log and SNMP Trap alarms.

You need to enter the monitor configuration mode to configure the monitor alarm function. To enter the monitor configuration mode, in the global configuration mode, use the following command:

monitor

After entering the monitor configuration mode, you can configure a monitor rule as needed for the system resource object:

{**cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **network** | **security** | **traffic**{**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization**} **interval** *interval-value* **absolute rising-threshold** *threshold-value* **sample-period** *period-value* [**count** *count-value*] {**log** [*snmp-trap*] | **snmp-trap**}

- **cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization** - Specifies the monitor object which can be **cpu**, **memory**, **interface-bandwidth**, **log-buffer**, **policy**, **session** or **snat-resource**. When you use the X platforms and enter the cpu keyword, proceed to select modules.
    - *interface-name* - Specifies the name of interface.
    - **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**} - Specifies the log type.
    - **utilization** - Specifies the value of monitor object as the utilization of each object. Since the default value for **cpu** is utilization, so you do not need to specify this parameter for the monitor object of CPU.

- **interval** *interval-value* - Specifies the monitor interval, i.e., the interval for acquiring the value of monitor object within the sampling period (**sample-period** *period-value*). The value range is 3 to 10 seconds.
- **absolute** - Specifies the value of monitor object as an absolute value.
- **rising-threshold** *threshold-value* - Specifies the rising threshold. The system will issue an alarm if the value of monitor object exceeds the percentage specified here. The value range is 1 to 99.
- **sample-period** *period-value* - Specifies the sample period. The value range is 30 to 3600 seconds.
- **count** *count-value* - Specifies the count for the conditions the value of monitor object exceeds the **rising-threshold** within the sampling period (**sample-period**). The value range is 1

to 1000. If this parameter is configured, when the count exceeds the **rising-threshold** within the sampling period, the system will issue an alarm; if this parameter is not configured, when the average value of monitor object exceeds the **rising-threshold**, the system will issue an alarm.

- **log** [**snmp-trap**] | **snmp-trap** - Specifies the method which can be **log**, **snmp-trap** or **both**.

For example:

To configure the peak CPU utilization monitor:

hostname(config)# **monitor**

hostname(config-monitor)# **cpu interval 5 absolute rising-threshold 65 sample-period 600 count 50 log**

After the configuration, if the CPU utilization exceeds the rising threshold of 65% within 600 seconds, and such a condition occurs at least 50 times, then the system will issue a log.

To configure the average session utilization monitor:

hostname(config)# **monitor**

hostname(config-monitor)# **session utilization interval 8 absolute rising-threshold 90 sample-period 600 log**

After the configuration, if the average session utilization exceeds the rising threshold of 90% within 600 seconds, then the system will issue a log.

To delete the specified monitor rule, in the monitor configuration mode, use the following command:

no {**cpu** | **memory utilization** | **interface-bandwidth** interface-name **utilization** | **log-buffer** { **config** | **event** | **ips** | **network** | **security** | **traffic** {**session** | **nat** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization**}



Notes:

- For every monitor object, only the last configured monitor rule takes effect.
- The system does not support monitor alarm for port resources whose IP address is translated into an egress IP address (eif-ip) after SNAT.

To view the monitor alarm configuration, in any mode, use the following command:

show monitor

CPU Cache Error Monitor

CPU Cache Error monitoring function supports SG6000-A2205/A1805/A1605.

To minimize device misfunctions that are caused by CPU Cache Error, you can configure the CPU Cache Error monitoring function. After configuring this feature, you can separately configure the alarm threshold and reboot threshold for CPU Cache Error. The two thresholds are mutually independent. When the alarm threshold is reached, the system generates alarm logs; when the reboot threshold is reached, the device can choose to restart or not restart.

You need to enter the monitor configuration mode to configure the CPU Cache Error monitoring function. To enter the monitor configuration mode, in the global configuration mode, use the following command:

monitor

To configure the alarm threshold for CPU Cache Error monitoring function, in the monitor configuration mode, use the following command:

cache-error-configthreshold-num*num* **alarm**

- **threshold-num***num* - Specifies the alarm threshold. When the number of CPU Cache Error reached the specified alarm threshold, the device will send alarms and generate logs. The value range is from 100 to 500.
- **alarm**- Specifies the action to be taken by the device, that is, alarm (**alarm**), when the number of CPU Cache Error reached the specified threshold.

To configure the reboot threshold for CPU Cache Error monitoring function, in the monitor configuration mode, use the following command:

cache-error-configthreshold-num*num* **reboot**{**enable** | **disable**}

- **threshold-num** *num* - Specifies the reboot threshold. When the number of CPU Cache Error reached the specified reboot threshold, the device will choose to reboot or not reboot. The value range is from 500 to 5000.
- {**reboot enable** | **reboot disable**}- Specifies the action to be taken by the device when the number of CPU Cache Error reached the specified threshold. The action can be restart (**enable**) or not restart (**disable**).

For example:

```
hostname(config)# monitor
hostname(config-monitor)# cache-error-config threshold-num 1000 reboot enable
With the above configuration, if the number of CPU Cache Errors reaches 1000, the device will restart.
```

In the monitor configuration mode, use the command **no cache-error-config** to the CPU Cache Error monitoring function.

To view the CPU Cache Error monitoring configuration, in any mode, use the following command:

show cache-error-reboot-config

- **cache-error-reboot-config**- Show the current reboot threshold of CPU Cache Error.

The Maximum Concurrent Sessions

If multi-VR, AV, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow is enabled on devices, or IPv6 firmware version is used, the maximum concurrent sessions might change. For more information, see the table below:

Platform / Expansion Module	Firmware	Max Concurrent Sessions
SG-6000 A-Series devices	StoneOS IPv4 version	With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions will not change.
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions will not change.
SG-6000 K-Series devices (Excluding K9180)	StoneOS IPv4 version	With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions will not change.
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions will not change.

Platform / Expansion Module	Firmware	Max Concurrent Sessions
QSM	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15); • With anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.5); • With multiple virtual routers plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.5); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25);

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		• With multiple virtual routers and NetFlow plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.25)*(1-0.5).
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is 50% of that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
SSM-300	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15); • With anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled: the maximum concurrent sessions will drop by 50%.

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.5); • With multiple virtual routers plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.5); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25); • With multiple virtual routers and NetFlow plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.25)*(1-0.5).
	StoneOS IPv6	• For X9180 and X10800, the original maximum

Platform / Expansion Module	Firmware	Max Concurrent Sessions
	version	concurrent sessions of the IPv6 version is 2/3 of that of the IPv4 version; • For K9180, the original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
SSM-200 SSM-100	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15); • With anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.5); • With multiple virtual routers plus anti-virus, IPS,

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.5); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25); • With multiple virtual routers and NetFlow plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.25)*(1-0.5).
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is 2/3 of that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
SIOM	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15); • With anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.5); • With multiple virtual routers plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.5); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%.

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25); • With multiple virtual routers and NetFlow plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.25)*(1-0.5).
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
IOM-P100-300 IOM-P40-300	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15);

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		• With anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.5); • With multiple virtual routers plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.5); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25); • With multiple virtual routers and NetFlow plus anti-virus, IPS, URL signature database, Sandbox, Anti-Spam and/or Botnet Prevention enabled simultaneously, the maximum concurrent sessions will further drop.

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.15)*(1-0.25)*(1-0.5).
	StoneOS IPv6 version	• For X9180 and X10800, the original maximum concurrent sessions of the IPv6 version is 88.3% of that of the IPv4 version; • For K9180, the original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
IOM-8SFP+	StoneOS IPv4 version	With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.25). **Note**: Other unlisted functions has no effect on the maximum concurrent sessions of the system.
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is 2/3 of that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS,

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
IOM-200; IOM-100	StoneOS IPv4 version	With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.25). **Note:** Other unlisted functions has no effect on the maximum concurrent sessions of the system.
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is 67.5% of that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.
IOM-80; IOM-20	StoneOS IPv4 version	• With fast forwarding data enabled on the IOM: the maximum concurrent sessions will drop by 60%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		(1-0.6); • With NetFlow enabled: the maximum concurrent sessions will drop by 25%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions* (1-0.25).
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is 50% of that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the change of the maximum concurrent sessions in the IPv6 version is the same as that in the IPv4 version.

Adjusting the Maximum Concurrent Sessions

You can adjust the maximum concurrent sessions of IPv4 of some A series or K series devices as needed. To adjust the maximum concurrent sessions of IPv4, use the following command in the global configuration mode:

exec session-adjust *value*

- *value* - Specifies the maximum concurrent sessions of IPv4. Please refer to the table below for the value range.

Platform	Value
A1000	120,000 - 600,000

Platform	Value
A1100	120,000 - 600,000
A2000	400,000 - 2,000,000
A2600	400,000 - 2,000,000
A2700	440,000 -2,200,000
A2800	500,000 - 2,500,000
A3000	700,000 - 3,500,000
A3600	960,000 - 4,800,000
A3700	2,000,000 - 10,000,000
A3800	2,000,000 - 10,000,000
A5200	3,000,000 - 15,000,000
A5500	3,600,000 - 18,000,000
A5600	5,000,000 - 25,000,000
A5800	6,000,000 - 30,000,000
A6800	7,000,000 - 35,000,000
A7600	8,400,000 - 42,000,000
K2580	2,000,000 - 10,000,000
K3280	3,000,000 - 15,000,000

Connecting to Hillstone Cloud Service Platform

Hillstone Cloud Service Platform is a cloud security services platform, which mainly provides the cloud services including CloudView, Cloud Sandbox and CloudVista (Threat Intelligence Center). Hillstone Cloud Service is the cloud capability center of Hillstone and the brain of the cloud-network integration. After the service is enabled, your device will be connected with the Hillstone

cloud, which will provide you with a wider range of threat intelligence, improve the protection capability of your device, and enable you to carry out real-time monitoring, inspection and report acquisition of the device and traffic on the cloud anytime and anywhere. These Hillstone cloud applications can greatly enhance the security, visibility, and usability of networks.

The following sections describe how to connect to the cloud service platform in StoneOS:

- Configuring the Cloud Service Server
- Changing Digital Certificate
- Enabling CloudView
- Enabling CloudVista
- Joining the User Experience Improvement Program
- Showing Configurations of the Cloud Service Platform



Notes: For more information about the cloud sandbox settings, refer to **Threat Prevention > Sandbox**.

Configuring the Cloud Service Platform Server

Before connecting to the cloud service platform, you need to configure the IP address (or domain name), user name and password of the cloud service platform server. The IP address (or domain name), user name and password of the cloud service platform server should be configured in the Cloud Server configuration mode.

To enter the Cloud Server configuration mode, in the global configuration mode, use the following command:

cloud server

To configure the IP address or domain name of the cloud service platform server, in the Cloud Server configuration mode, use the following command:

address {A.B.C.D | X:X:X:X::X | *domain*}

- A.B.C.D | X:X:X:X::X | *domain* - Specifies the IPv4 address, IPv6 address, or domain name of the cloud service platform server. The default value is cloud.hillstonenet.com.cn.

To cancel the specified IP address or domain name, in the Cloud Server configuration mode, use the command**no address**.

To configure the user name and password of the cloud service platform server, in the Cloud Server configuration mode, use the following command:

username *user-name* **password** *pass-word*

- **username** *user-name* - Specifies the user name of the cloud service platform server to bind the device with this account.
- **password** *pass-word* - Specifies the password of the user。

To cancel the specified user name and password, in the Cloud Server configuration mode, use the command **no username**.

To configure the virtual router of the cloud service platform server, in the Cloud Server configuration mode, use the following command:

vrouter *vr-name*

- *vr-name* – Specifies the VRouter of the cloud service platform server.

To cancel the specified VRouter, in the Cloud Server configuration mode, use the command **no vrouter**.

Changing Digital Certificate

Digital certificates are used for bidirectional authentication when the device is connected to the cloud platform. After bidirectional authentication succeeds, the device connects to the cloud platform. Create a trust domain to store the new CA certificate and the device can use the certificate to verify the certificate provided by the cloud platform. Create another trust domain to store new local certificate and the private key so that the cloud platform can verify the certificate. Import the new CA certificate, local certificate, and private key to the trust domain and then you can change the digital certificates. To create a trust domain, import certificates and private key, see PKI.

Reference the existing trust domain to obtain a new CA certificate, in the Cloud Server configuration mode, use the following command:

server-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the existing trust domain that stores the new CA certificate in the system. If this parameter is not specified, the system uses the default built-in CA certificate.

Reference the existing trust domain to obtain a new local certificate and private key, in the Cloud Server configuration mode, use the following command:

agent-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the existing trust domain that stores the new local certificate and private key in the system. If this parameter is not specified, the system uses the default built-in local certificate and private key.

Enabling CloudView

CloudView is a SaaS product. It is deployed on the public cloud to provide users with online on-demand services. Hillstone devices register with the cloud service platform and upload device information, traffic data, threat events, system logs and so on to the cloud service platform, and the visual display is provided by CloudView . Users can monitor the device status, gain reports and threat analysis through the Web or mobile phone APP. In addition, you can also use CloudView to send configuration to the device. When the Cloud Configuration function is enabled, the system will load the configuration sent from CloudView.

The following sections describe how to enable the CloudView service in StoneOS:

- Enabling CloudView
- Enabling Information Upload
- Enabling Log Report
- Enabling Monitoring Data Uploading

- Enabling Cloud Inspection
- Enabling Cloud Configuration

Enabling CloudView

You can enable the CloudView service in the Cloud View configuration mode. To enter the Cloud View configuration mode, in the global configuration mode, use the following command:

cloud-view

To enable the CloudView service, in the Cloud View configuration mode, use the following command:

enable

To disable the CloudView service, in the Cloud View configuration mode, use the command **no enable**.

Enabling Information Upload

You can upload information generated during the running of the device, including the basic information, threat intelligence information, security log information, and DNS information. To do this, in Cloud View configuration mode, use the following command:

upload-type all

To disable information upload, in Cloud View configuration mode, use the following command:

no upload-type all

Enabling Log Report

To upload log data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

- **log-cf** -Specifies to upload content filter logs of the device to the cloud platform.
- **log-config** - Specifies to upload configuration logs of the device to the cloud platform.
- **log-dlp** - Specifies to upload file content logs of the device to the cloud platform.
- **log-event** - Specifies to upload event logs of the device to the cloud platform. By default, the upload interval is 10 minutes. Before you enable the function, make sure that the device is enabled with the **logging event on** function.
- **log-iot** - Specifies to upload IoT logs of the device to the cloud platform.
- **log-nat** - Specifies to upload NAT logs of the device to the cloud platform.
- **log-nbr** - Specifies to upload network behavior audit logs of the device to the cloud platform.
- **log-network** - Specifies to upload network logs of the device to the cloud platform.
- **log-operat** - Specifies to upload operation logs of the device to the cloud platform.
- **log-sandbox** - Specifies to upload cloud sandbox logs of the device to the cloud platform.
- **log-session** - Specifies to upload session logs of the device to the cloud platform.
- **threat-event** - Specifies to upload threat events of the device to the cloud platform. By default, the upload interval is 60 minutes.
- **all** - Specifies to upload all monitoring data above of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

Notes:

- For X series devices and K6580/K9180 devices, you are not allowed to upload threat logs to the cloud platform.
- The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.

Enabling Monitoring Data Uploading

To upload monitoring data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}

- **traffic-rank** -Specifies to upload the traffic ranking data of the device to the cloud platform.
- **stats-session** - Specifies to upload the session ranking data of the device to the cloud platform.
- **stats-url-rank** - Specifies to upload the URL ranking data of the device to the cloud platform.
- **stats-device** -Specifies to upload the device information data of the device to the cloud platform.
- **scvpn-user** - Specifies to upload the VPN statistics of the device to the cloud platform.
- **stats-interface** - Specifies to upload the interface statistics of the device to the cloud platform, including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface.
- **all** - Specifies to upload all monitoring data of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}



Notes: For X series devices and K6580/K9180 devices, you are only allowed to upload interface statistics to the cloud platform.

Enabling Cloud Inspection

After enabling cloud inspection, the system can receive and execute inspection commands from the cloud and upload the collected inspection data to the cloud platform. This enables real-time monitoring and O&M management for the device and traffic on the cloud.

To enable the cloud inspection function, in Cloud View configuration mode, use the following command:

inspection enable

In Cloud View configuration mode, use the **no inspection enable** command to disable the cloud inspection function.

Enabling the Cloud Configuration

To allow CloudView to send configuration to the device, in the CloudView Configuration mode, use the following command:

load-config enable

In the CloudView Configuration mode, use the **no load-config enable** command to disable cloud configuration.

With the Cloud Configuration function enabled, the system will load the real-time configuration sent by CloudView.

- PTF Dynamic IP Blacklist: Log in to CloudView to send the configuration of the PTF dynamic IP blacklist to the root VSYS of the device. Both IPv4 and IPv6 addresses are

supported. You can also specify the virtual router to take effect as well as the block duration. When the system receives the configuration task from CloucView, corresponding dynamic IP blacklist entries, configuration logs, and operation logs are generated.

Enabling/Disabling Cloud Assets Identification Function

When you enable the cloud assets identification function, the device automatically uploads information about IoT devices within the deployment environment to the cloud, along with the relevant training data that assists the cloud-based detection service.

By default, the cloud assets identification function is disabled. In CloudView configuration mode, use the following command to enable or disable the cloud-based assets identification function.

- Enable: **uptype-iot detect**
- Disable: **no uptype-iot detect**

Configuring Hillstone CloudVista

Hillstone CloudVista includes the following content:

- Entering the CloudVista Configuration Mode
- Enabling/Disabling IOC Details Cloud Collaborative Query
- Configuring Unknown Domain Cloud Collaborative Query (See **Botnet Prevention** section)

Before you start

- The IOC Details Cloud Collaborative Query function is controlled by the Threat Intelligence license. To use the function, please install the Threat Intelligence license first.
- The Unknown Domain Cloud Collaborative Query function is controlled by the Botnet Prevention license. To use the function, please install the Botnet Prevention license first.
- Connect to Hillstone Cloud Platform.

Entering the CloudVista Configuration Mode

Enabling/Disabling IOC Details Cloud Collaborative Query, the Unknown Domain Cloud Collaborative Query (cloud query) function, and cloud query token need to be configured in CloudVista configuration mode. Before you start the configuration, use the following command to enter the CloudVista configuration mode.

To enter the CloudVista configuration mode, in Cloud Server configuration mode, use the following command:

cloud-vista

Enabling/Disabling IOC Details Cloud Collaborative Query

IOC indicates threat intelligence, which is used to query detailed threat information from cloud-based services, assisting the administrator in analyzing and defining threat detection results.



Notes: This function is controlled by license. To use it, you need to install the Threat Intelligence license first.

By default, this function is disabled. Once enabled, it remains enabled even after device restarts.

To enable/disable IOC Details Cloud Collaborative Query, in CloudVista configuration mode, use the following command:

- Enable: **query-ioc enable**
- Disable: **no query-ioc enable**

Joining the User Experience Improvement Program

With the user experience improvement program, the threat prevention data of device and the UDP DNS traffic will be uploaded to the cloud service platform and used for internal research, which reduces the false positives and improves the protection capability of your device. To join the user experience improvement program, in the Cloud Server configuration mode, use the following command:

user-experience-improvement-plan enable

To cancel to join the user experience improvement program, in the Cloud Server configuration mode, use the command **no user-experience-improvement-plan enable**.

Note: When one of the following conditions is met during the capture of UDP DNS traffic: capacity (occupies a maximum of 176 KB in memory), quantity (captures a maximum of 20 DNS packets), or cycle (per minute), the packet capture will stop and the data will be uploaded to the cloud. UDP DNS traffic that fails to be uploaded will be overwritten by new UDP DNS traffic in subsequent cycles and will not be sent to the cloud. X-series devices cannot upload UDP DNS traffic to the cloud.

Showing Configurations of the Cloud Service Platform

To view the configurations of the cloud service platform, in any mode, use the following command:

show cloud server

Connecting to iSource

iSource——Intelligent Security Operation System is a holographic data-driven AI analysis and operation system. It is composed of an analysis platform and a wealth of probes. It can provide customers in various industries with functions such as network threat analysis, situation presentation and traceability, and solve customer monitoring blind zones , potential safety hazards, inefficient operation and maintenance and other issues. iSource has the ability to collect holographic data, collect data through various types of data probes, conduct intelligent data mining and analysis based on massive network traffic, threat events and endpoint logs, presenting the global network security and threat situation, and support multiple dimensions core functions such as screencast display, linkage response, and work order make the safe operation of the enterprise under control.

When the device is enabled for connecting to iSource and configured with correct iSource parameters, it can connect to iSource, the iSource can receive and further analyze information about the firewall device. After the firewall device is connected with iSource as a network device, you can upload threat logs and evidence packets to iSource for analysis.



Notes: For more information about iSource, please refer to *iSource User Guide*.

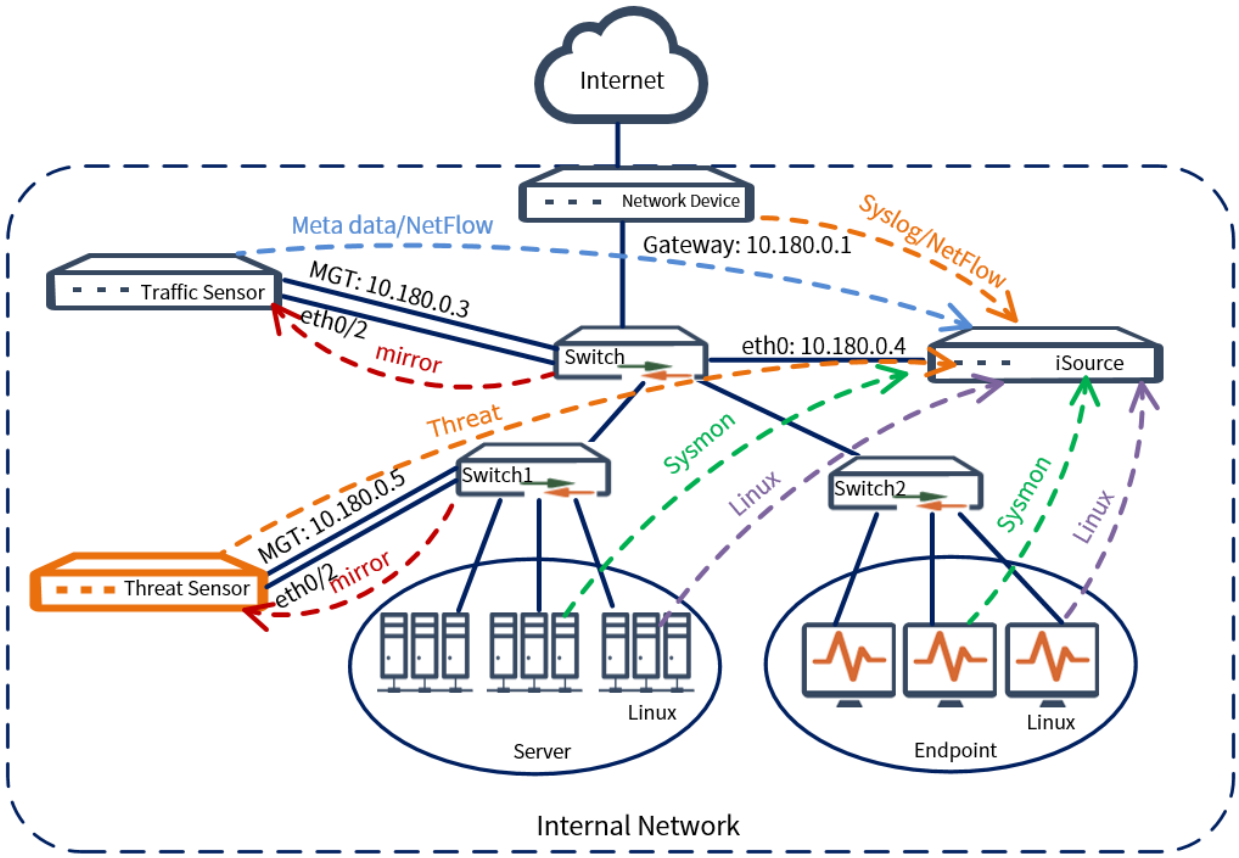
iSource Typical Deployment

The typical deployment of iSource mainly includes four parts: the iSource Security Operation Platform (referred to as iSource Platform), traffic sensor, threat sensor, and ThreatTrace Client. Typical deployment includes stand-alone deployment and cluster deployment.

Stand-alone Deployment

The iSource platform (single machine) , traffic sensor and threat sensor are deployed in the intranet environment, and the ThreatTrace client is deployed on the user's server or endpoint. After the deployment is completed, the iSource platform can receive information (Meta Data, Syslog, NetFlow, Linux, Sysmon, threat information) from traffic sensor, threat sensor, Linux system device, network device, and user servers and endpoints, so as to control all network for monitoring and analysis.

The stand-alone deployment scenario is shown in the figure below:



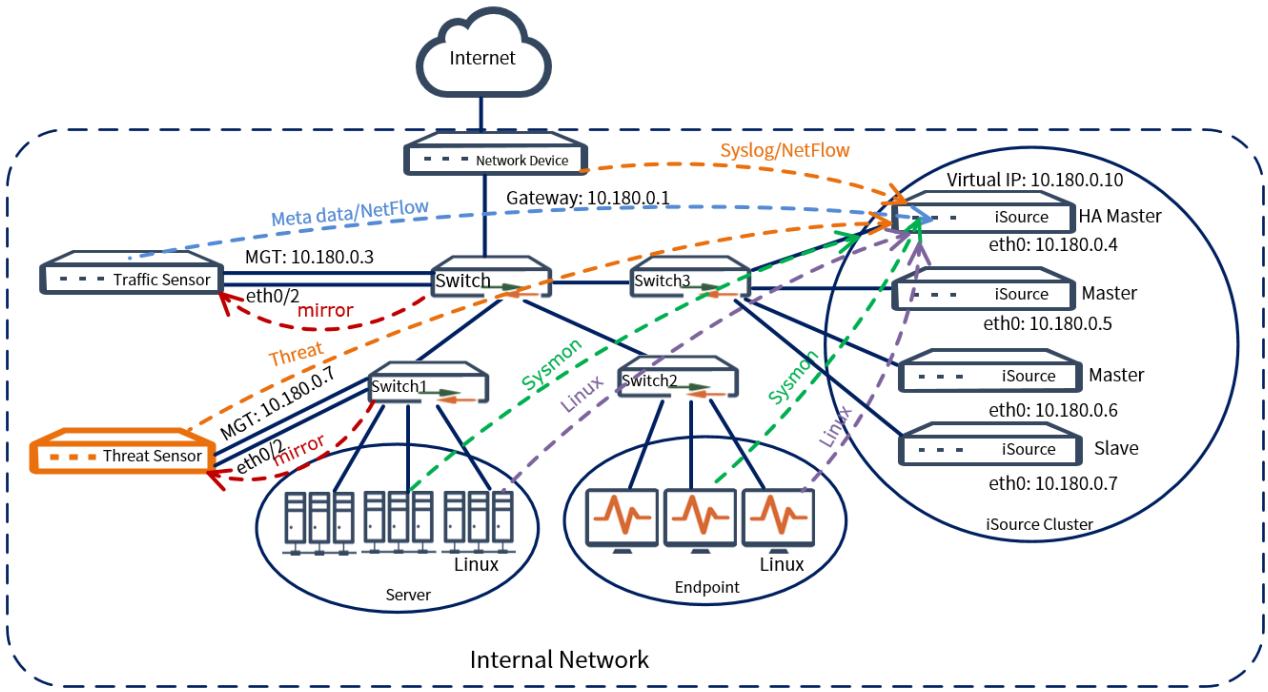
Cluster Deployment

As the amount of user data increases, a single iSource platform may not be able to meet the needs of users. In response to this problem, the iSource platform supports cluster deployment, that is, you can deploy multiple iSource platforms, thereby alleviating the pressure on the data volume of a single iSource platform.

When the number of iSource platforms in the cluster is greater than or equal to 3, the iSource platform cluster will support High Availability (HA) by default, which can provide backup solutions in the event of device failure. When one iSource platform in the cluster fails and becomes unavailable, other iSource platforms in the cluster will continue to receive and process data to ensure uninterrupted data communication and effectively enhance the reliability of the network.

Refer to the following cluster deployment topology. The iSource platform (cluster), traffic sensor, and threat sensor are deployed in the intranet environment, and the ThreatTrace client is deployed on the user's server and endpoint. All iSource platforms in the cluster are deployed on the Layer 2 network. The first iSource platform deployed is the HA Master. The HA Master will allocate available resources for other iSource platforms according to its configured internal IP network segment (IP address). After deployment, HA Master can receive all information (Meta Data, Syslog, NetFlow, Linux, Sysmon, threat information) from traffic sensor, threat sensor, Linux system device, network device, and user servers and endpoints, and then transfer the data Information is distributed to other iSource platforms in the cluster through internal IP addresses.

The cluster deployment scenario is shown in the figure below:



Connecting to iSource

You can connect to iSource by using the CLI or WebUI. To connect the device to iSource, you need to enable the Connecting to iSource function on the device and configure the IP address and VRouter of iSource, as well as the data types sent to iSource. The connecting to iSource configuration includes the following:

- Entering the iSource configuration mode
- Enabling Connecting to iSource
- Configuring the IP address of iSource
- Configuring the VRouter of iSource
- Configuring the Data Types sent to iSource

Enter the iSource Configuration Mode

To enter the iSource configuration mode, in global configuration mode, use the following command:

cloud server isource

Enabling Connecting to iSource

To enable the Connecting to iSource function, in iSource configuration mode, use the following command:

enable

In iSource configuration mode, use the **no enable** command to disable the Connecting to iSource function.

Configuring the IP Address of iSource

To configure the IP address of iSource, in iSource configuration mode, use the following command:

address {*A.B.C.D* | *domain*}

- *A.B.C.D* | *domain* – Specifies the IP address or domain name of iSource.

In iSource configuration mode, use the **no address** command to cancel specifying the IP address or domain name of iSource.

Configuring the VRouter of iSource

To configure the VRouter of iSource, in iSource configuration mode, use the following command:

vrouter {**trust-vr**| **mgt-vr**}

- **trust-vr** | **mgt-vr** – Specifies the name of the VRouter.

In iSource configuration mode, use the **no vrouter** command to cancel specifying the VRouter of iSource.

Configuring the Data Types Sent to iSource

To configure data types sent to iSource, in iSource configuration mode, use the following command:

upload-type {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**}

- **all** – Specifies to send all types of data to iSource.
- **forensic-pcap** – Specifies to send threat-related evidential packets captured by the device to iSource.
- **iot-monitor-property** – Specifies to send detected IoT asset data to iSource.
- **threat-event** – Specifies to send threat logs to iSource

In iSource configuration mode, use the **no upload-type** {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**} command to cancel specifying the data types sent to iSource.



Notes:

- A-series device, K-series device(except K6580/K9180), CloudEdgesupport to upload threat logs to iSource.



- A-series devices that are installed with SSD , K-series devices (except K6580/K9180) that are installed with SSD CloudEdgesupport to upload threat-related evidential packets captured by the device to iSource.
- The X-series devices and K6580/K9180 devices of K series support to upload only detected IoT asset data to iSource.

Showing the Configuration of Connecting to iSource

You can use the show command in any mode to view the configuration of connecting to iSource:

show cloud server isource

Configuring the RESTful API Interface to Upload Files

To upload files through /rest/file interface, in the global configuration mode, use the following command:

restful-api-control /rest/file {**enable** | **disable**}[**version 5.5R4**]

- **enable** - After enabling this function, you can use the /rest/file interface to upload files. The suffix and size of the file will not be checked.
- **disable**- The /rest/file interface cannot be used, and an error will be returned directly when uploading a file. By default, the /rest/file interface is disabled.
- **version 5.5R4** - Compatible with some formats of RESTful API of 5.5R4 version .

Clearing Alarm Status of Indicators

When the LED indicators (PWR, STA, and ALM) on the front panel are red, they indicate abnormalities. When the device restores to normal, you can manually clear the alarm status of the indicators through configuration.

To manually clear the alarm status of the indicators, in the global configuration mode, use the following command:

clear led {PWR | STA |ALM}

- **PWR | STA |ALM** - Specifies the LED indicator (PWR, STA, or ALM) whose alarm status needs to be cleared.

Automatically Clearing Alarm Status of Indicators

If the ALM indicator on the front panel is red due to the following issues, you can configure the system to automatically clear the alarm status of the ALM indicator when the issues are solved and the device restores to normal.

- Lack of power supply module
- Device temperature exceeds the acceptable level
- Fan is broken

To make the system automatically clear the alarm status of the ALM indicator, in the global configuration mode, use the following command:

led-alarm-autoclear

In the global configuration mode, use the **no led-alarm-autoclear** command to cancel the configuration for the system to automatically clear the alarm status of the ALM indicator.

Specifying the Device as an SSH/Telnet Client

The firewall device can act as an SSH or Telnet client to connect and log in to other SSH or Telnet servers.

Specifying the Device as an SSH Client

When the device acts as an SSH client to connect and log in to other SSH servers, 3 authentication methods are supported: password authentication, key-based authentication, and password-key authentication. To specify the device as an SSH client to connect and log in to other SSH servers, take the following steps:

ssh user *user-name* **ip** {*A.B.C.D* | *X:X:X:X::X*} [**port** *port*] [**publickey** *publickey_name*] [**vrouter** *vrouter-name*]

- **user** *user-name* - Specifies the username used to log in to the SSH server.
- **ip** {*A.B.C.D* | *X:X:X:X::X*} - Specifies the IPv4 (*A.B.C.D*) or IPv6 (*X:X:X:X::X*) address of the SSH server to which the device logs in.
- **port** *port* - Specifies the destination port number used to establish the SSH connection. Valid values: 1 to 65535. Default value: 22.
- **publickey** *publickey_name* - Specifies the name of the SSH key pair. After you configure this parameter, if the authentication method on the SSH server is key authentication, the firewall can log in to the SSH server directly; if the authentication method on the SSH server is password-key authentication, you can log in to the SSH server only after entering the valid login password. If this parameter is not configured, the firewall will log in to the SSH server by using password authentication, and you can log in by entering the valid login password. **Note:** To ensure successful key authentication or password-key authentication, you need to configure the public key of the key pair in the SSH format for the SSH server. For more information about how to obtain the public key of the key pair in the SSH format, see Viewing the PKI Configuration Information.
- **vrouter** *vrouter-name* - Specifies the VRouter used to establish the SSH connection. By default, the default VRouter in the current VSYS is used.



Notes: For X-series devices, in SCM HA scenarios, the command configuration above is supported only in the master SCM.

Specifying the Device as a Telnet Client

When the device acts as a Telnet client and logs in to other Telnet servers, the password authentication method is supported. To specify the device as a Telnet client to connect and log in to

other Telnet servers, take the following steps:

telnet ip {*A.B.C.D* | *X:X:X:X::X*} [**port** *port*] [**vrouter** *vrouter-name*]

- **ip** {*A.B.C.D* | *X:X:X:X::X*} - Specifies the IPv4 address (*A.B.C.D*) or IPv6 address (*X:X:X:X::X*) of the Telnet server to which the device logs in.
- **port** *port* - Specifies the destination port number used to establish the Telnet connection. Valid values: 1 to 65535. Default value: 23.
- **vrouter** *vrouter-name* - Specifies the VRouter used to establish the Telnet connection. By default, the default VRouter in the current VSYS is used.



Notes: For X-series devices, in SCM HA scenarios, the command configuration above is supported only in the master SCM.

Switching the Working Mode of SIOM Module

All models of X-series devices and K9180 devices support this function.

The SIOM module has two working modes: SIOM mode and IOM mode. By default, the SIOM module works in SIOM mode. In SIOM mode, SIOM can both send and receive messages and process business. In IOM mode, the SIOM module only sends and receives messages without processing business. You can flexibly switch between the working modes of the SIOM module based on different business scenarios to enhance device performance.

To switch the working mode of the SIOM module to IOM, in global configuration mode, use the following command:

siom-switch-to-iom slot*slot-number*

- *slot-number* - Specifies the number of the slot where the SIOM module resides. You can press Tab next to the **slot** parameter to view the slot number of the installed SIOM module.

In global configuration mode, use the **no siom-switch-to-iom slot***slot-number* command to switch the working mode of the SIOM module to SIOM.

Notes:

- Only StoneOS 5.5R10P5 and later support to switch the working mode of SIOM module.
- After you switch the working mode of SIOM module, you need to restart the device make the configuration take effect.
- If only one SIOM module is inserted on the device, the working mode of the SIOM mode cannot be switched to the IOM mode. That is, make sure that at least one SIOM module works in SIOM mode.
- Regardless of whether SIOM module works in SIOM mode or IOM mode, it cannot be inserted together with the IOM/SSM module.
- After SIOM module is hot-swapped in the device slot, the working mode will be automatically switched to the configured mode for this slot, without the need to restart or reconfigure the device.
- You cannot configure this function and use the **session-schedule-mode local-slot** command at the same time.

Specifying the Maximum Retry Time for Configuration Deployment

For certain function configurations of the system, running a configuration command will automatically temporarily lock the configuration. This could lead to subsequent configuration command deployment failure. For such cases, the system supports to specify the maximum retry time for deploying configurations. Within the specified time, the system continuously redeploys the configurations, after which an error message will be returned if the configuration still fails to be deployed. If you do not specify the retry time, the system continuously redeploys the configurations within 5 seconds by default.

To specify the maximum retry time for deploying configurations, in any mode, use the following command:

exec retrytime*times*

- *times* – Specifies the maximum retry time. Valid values: 0 to 3600 seconds. The value 0 indicates that no configuration is redeployed and an error message is immediately returned.

Enabling/Disabling the Function of IP Fragmented Packets Reassembling in the IOM/SIOM Module

All models of X-series devices and K9180 devices support this function.

By default, for devices that use IOM/SIOM module, IP fragmented packets that enter the device are reassembled and forwarded in the IOM/SIOM module. When the first and non-first packets of IP fragmented packets enter the device from different IOM/SIOM modules, non-packet loss may occur during packet transmission because non-first packet reassembly depends on the first packet, which results in traffic forwarding failure.

To avoid this issue and ensure that traffic can be forwarded as expected, the system allows you to enable/disable the function of IP fragmented packets reassembling in the IOM/SIOM module. After this function is enabled, IP fragmented packets are not assembled in the IOM/SIOM module, but are directly uploaded to the SSM service module for processing.

To enable/disable the function of IP fragmented packets reassembling in the IOM/SIOM module, in global configuration mode, use the following command:

- Enable: **fragment centralized-mode**
- Disable: **no fragment centralized-mode**

By default, this function is disabled, which indicates that IP fragmented packets are reassembled in the IOM/SIOM module.

Viewing the Temperature, Fan, and Power Supply Information of the Device

To view the temperature, fan, and power supply information of the device, in any mode, use the following command:

show environment

Example:

```
hostname(config)# show environment
Temperature information(C):
=========================================
Description Temperature Range
-----------------------------------------
SYS 41 0-90
CPU 63 0-90
-----------------------------------------
Fan information:
=========================================
Description Status
-----------------------------------------
Fan1 4945(rpm)
Fan2 6459(rpm)
-----------------------------------------
Voltage information:
=============================================
Description Voltage Range
---------------------------------------------
Vcore 1.112 0.600-1.300
VBAT 3.040 2.100-3.465
```

```
3.3V 3.280 3.135-3.465

5V 5.040 4.750-5.250

12V 11.904 11.400-12.600

-----------------------------------------
```

Viewing the CPU Utilization of the Device

To view the CPU utilization of the device, in any mode, use the following command:

show cpu

Example:

```
hostname(config)# show cpu

Average cpu utilization : 3.1%

Current cpu utilization : 2.3%

Last 1 minute : 2.4%

Last 5 minutes : 3.1%

Last 15 minutes : 3.1%
```

Viewing Information about MAC Table

By using the CLI, you can view MAC table entries for all VSwitches or a specified interface, and you can also clear MAC table entries for all VSwitches or a specified interface.

Viewing Information about MAC Table

To view information about MAC table, in any mode, use the following command:

show mac [**generic**] | [**interface** *interface-name*]

- **generic** – displays statistics about MAC table, including the total number of MAC table entries and how many of them are in use.
- **interface** *interface-name* – specifies MAC table entries of a specified interface.

Clearing MAC Table Information

To clear MAC table entries, in execution mode, use the following command:

clear mac [**interface** *interface-name*]

Managing SSH Algorithms

During the negotiation phase, SSH connections use multiple SSH algorithms for negotiation. To prevent potential security risks, you can actively disable any vulnerable SSH algorithm, avoiding its adverse impact on the business. Disabled SSH algorithms will not be used during the key negotiation phase. You can re-enable any disabled SSH algorithms once their vulnerabilities are fixed. The types of SSH algorithms that can be managed by the system include: kex algorithms, server host key algorithms, encryption algorithms, and mac algorithms. You can manage these SSH algorithms based on your requirements to improve the security and stability of the SSH connection process.

Managing SSH algorithms includes:

- Disabling a specified SSH algorithm
- Re-enabling an SSH algorithm
- Viewing disabled SSH algorithms

Disabling a Specified SSH Algorithm

To disable a specified SSH algorithm, in global configuration mode, use the following command:

no ssh server algorithms type {**encryption** | **kex** | **mac** | **server-host -key**} *algorithm-name*

- *algorithm-name* - Specifies the name of the SSH algorithm that you want to disable. You can view all SSH algorithm names contained in the current type by entering the Tab key after the {**encryption** | **kex** | **mac** | **server-host -key**} parameter.

Re-enabling an SSH Algorithm

To re-enabling an SSH algorithm, in global configuration mode, use the following command:

ssh server algorithms type {**encryption** | **kex** | **mac** | **server-host -key**} *algorithm-name*

- *algorithm-name* - Specifies the name of the SSH algorithm that you want to re-enable. You can view SSH algorithm names that can be re-enabled in the current type by entering the Tab key after the {**encryption** | **kex** | **mac** | **server-host -key**} parameter.

Viewing Disabled SSH Algorithms

To view disabled SSH algorithms, in any mode, use the following command:

show ssh server algorithms disable

Sample response:

```
hostname#show ssh server algorithms disable
kex_algroithms: diffie-hellman-group14-sha256
server_host_key_algorithms: rsa-sha2-512
encryption_algorithms: aes128-ctr
mac_algorithms: umac-64-etm@openssh.com
```

Chapter 5 Virtual System (VSYS)

Virtual systems (VSYS) divide a physical device into multiple logical virtual firewalls. Each VSYS has its own system resources, performs most of the firewall functionalities, working as a completely independent firewall. VSYSs cannot communicate directly from each other.

VSYS has the following characters:

- Each VSYS has its own administrators;
- Each VSYS has independent virtual routers, zones, address book, service book, etc;
- Each VSYS has independent physical and logical interfaces;
- Each VSYS has independent policy rules.
- Each VSYS has independent logs.

The supported default VSYS number varies from different platforms. You can expand the number by purchasing and installing the license.



Notes: SG-6000-A1100， SG-6000-A1000, SG-6000-A200 , SG-6000-A200W and SG-6000-A200G4B do not support VSYS function.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

The system contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device. When creating or deleting non-root VSYSs, you must follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you must be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see "Administrator".
- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
- A non-root VSYS administrator named admin. The password is *vsys_name-admin*.
    - A VRouter named vsys_name-vr.
    - A L3 zone named vsys_name-trust.

      For example, when creating the non-root VSYS named vsys1, the following objects will be created:
    - The non-root administrator named vsys1\admin with the password vsys1-admin.
    - The default VRouter named vsys1-vr.
    - The L3 zone named vsys1-trust and it is bound to vsys1-vr automatically.
- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating l2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the l2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

Administrator

The admin users of each VSYS are independent from other VSYS. VSYS admin users also have different roles of Administrator, Administrator-ready-only, operator and auditor. Their roles and

previleges are the same with normal admin users.

When creating VSYS administrators, you must follow the rules listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into non-root VSYS.
- After logging into root VSYS, the root administrators can switch to non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after the successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in the format of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

Table below shows the permissions to different types of VSYS administrators.

Operation	Permissions							
	Root VSYS Administrator	Root VSYS Administrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Administrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including save configuration)	√	χ	√	χ	√	χ	√	χ
Managing	√	χ	χ	χ	√	χ	χ	χ

Operation	Permissions							
	Root VSYS Administrator	Root VSYS Administrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Administrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
admin users								
Restore factory default	√	χ	χ	χ	χ	χ	χ	χ
Delete configuration file	√	χ	√	χ	√	χ	√	χ
Roll back configuration	√	χ	√	χ	√	χ	√	χ
Reboot	√	χ	√	χ	χ	χ	χ	χ
View configuration information	√	√	√	χ	View info in current VSYS	View info in current VSYS	View info in current VSYS	χ
View log information	√	√	χ	√	√	√	χ	√
Modify current admin password	√	√	√	√	√	√	√	√
Command import	√	χ	√	χ	√	χ	√	χ
Command	√	√	√	√	√	√	√	√

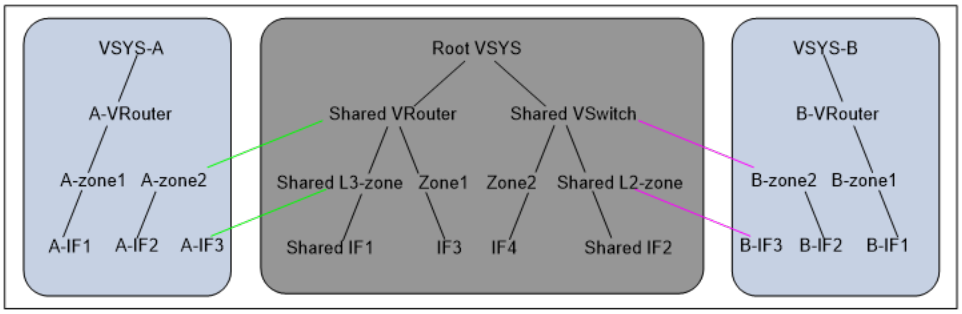
Operation	Permissions							
	Root VSYS Admin-isrator	Root VSYS Admin-isrator-read-only	Root VSYS Oper-ator	Root VSYS Aud-itor	Non-root VSYS Admin-isrator	Non-root VSYS Admin-isrator-read-only	Non-root VSYS Oper-ator	Non-root VSYS Aud-itor
export								
Command clear	√	√	√	√	√	√	√	√
Command ping/tracero-ute	√	√	√	χ	√	√	√	χ
Command debug	√	√	√	χ	χ	χ	χ	χ
Command exec	√	√	√	√	√	√	√	√
Command terminal width	√	√	√	√	√	√	√	χ

VRouter, VSwitch, Zone, Interface

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

- **Dedicated object**: A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object**: A shared object can be shared by multiple VSYSs (CloudEdge, TAI(X8180), and A-series platforms do not support shared object). A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

Figure below shows the reference relationship among dedicated and shared VRouter, VSwitch, zone, and interface.



As shown in the figure above, there are three VSYSs in StoneOS: Root VSYS, VSYS-A, and VSYS B. Root VSYS contains shared objects (including Shared VRouter, Shared VSwitch, Shared L3-zone, Shared L2-zone, Shared IF1, and Shared IF2) and dedicated objects.

VSYS-A and VSYS-B only contain dedicated objects. The dedicated objects VSYS-A and VSYS-B can reference the shared objects in Root VSYS. For example, A-zone2 in VSYS-A is bound to the shared object Shared VRouter in Root VSYS, and B-IF3 in VSYS-B is bound to the shared object Shared L2-zone in Root VSYS.

Shared VRouter

A shared VRouter contains the shared and dedicated L3 zones of the root VSYS. Bind a L3 zone to a shared VRouter and configure this L3 zone to have the shared property. Then this zone becomes a shared zone.

Shared VSwitch

A shared VSwitch contains the shared and dedicated L2 zones of the root VSYS. Bind a L2 zone to a shared VSwitch and configure this L2 zone to have the shared property. Then this zone becomes a shared zone.

Shared Zone

The shared zones consist of L2 shared zones and L3 shared zones. After binding the L2 zone with the shared property to a shared VSwitch, it becomes a shared L2 zone; after binding the L3 zone with the shared property to a shared VRouter, it becomes a shared L3 zone. A shared zone can contain interfaces in both root VSYS and non-root VSYS. All function zones cannot be shared.

Shared Interface

After binding an interface in the root VSYS to a shared zone, it becomes a shared interface automatically.

Interface Configuration

Only RXW administrator in the root VSYS can create or delete interfaces. Configurations to an interface and its sub-interfaces must be performed in the same VSYS.

Configuring VSYS

VSYS configurations include:

- Creating a Non-root VSYS
- Creating a VSYS Profile
- Entering the VSYS
- Configuring the Shared Property
- Exporting a Physical Interface
- Allocating a Logical Interface

- Configuring VSYS Log
- Configuring Cross-VSYS Traffic Forwarding

Creating a Non-root VSYS

The root administrator can create non-root VSYS. To create a non-root VSYS, in the global configuration mode of the root VSYS, use the following command:

vsys *vsys-name*

- *vsys-name* - Specifies the name of the VSYS to be created. It is a string composed of 1 to 23 characters. The word **root** cannot be configured and the backslash (\) cannot be used in the specified name.

After executing the command, the system creates a non-root VSYS with the specified name and enters the configuration mode of the created non-root VSYS. If the specified name exists, the system enters the configuration mode of the non-root VSYS directly.

To delete the specified non-root VSYS, in the global configuration mode of the root VSYS, use the following command:

no vsys *vsys-name*

Configure the Alias of Non-root VSYS

The system does not allow the name of the non-root VSYS to be modified, which might lead to large amount of workload and impact on clients' business when clients need to modify the name of the non-root VSYS. To solve this issue, the system suppots to configure the alias of non-root VSYS, which meets clients' need to modify the name of the non-root VSYS and avoids the negative impact on the business that the non-root VSYS bears when its name is modified.

By default, the alias of non-root VSYS is null.

To configure the alias of non-root VSYS, in the global configuration mode of the non-root VSYS, use the following command:

alias *alias_name*

- *alias_name* - Specify the alias of the non-root VSYS. It is a string composed of 1 to 23 characters. The word **root** cannot be configured and the backslash (\) cannot be used in the specified name. The name only supports lowercase and capital letters a-z, numbers 0-9, "-" and "_".

To delete the specified alias of non-root VSYS, in the global configuration mode of the root VSYS, use the following command:

no alias



Notes:

- When creating a new non-root VSYS, the specified VSYS name cannot be the same with the name or alias of ther non-root VSYS.
- When configuring the alias of non-root VSYS, the specified alias cannot be the same with name or alias of ther non-root VSYS.

Specifying the Description for VSYS

To specify the description for a non-root VSYS, in the VSYS configuration mode, use the following command:

description*string*

- *string* – Specifies the description of the VSYS.

To delete the description of the VSYS, use the following command:

no description

Creating a VSYS Profile

VSYSs work independently in functions but share system resources including concurrent sessions, zone number, policy rule number, SNAT rule number, DNAT rule number, session limit rules number, memory buffer, URL resources and IPS resources. You can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile.

Reserved quota refers to the resource number reserved for the VSYS; maximum quota refers to the maximum resource number available to the VSYS. The root administrator has the permission to create VSYS profiles. The total for each resource reserved quota allocated of all VSYSs cannot exceed the system capacity, and the total for each resource actually allocated of all VSYSs cannot exceed the system capacity.

To create a VSYS profile, in the global configuration mode of the root VSYS, use the following command:

vsys-profile *vsys-profile-name*

- *vsys-profile-name* - Specifies the name of the VSYS profile to be created. It is a string composed of 1 to 31 characters.

After executing the command, the system creates a VSYS profile with the specified name and enters the configuration mode of the created VSYS profile. If the specified name exists, the system enters the configuration mode of the VSYS profile directly.

To delete the specified VSYS profile, in the global configuration mode of the root VSYS, use the following command:

no vsys-profile *vsys-profile-name*



Notes:

- Up to 128 VSYS profiles are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you must delete all the VSYSs referencing the VSYS profile.

Configuring Resource Quota

You can configure the quota of a VSYS, including CPU (**cpu**), concurrent sessions (**session**), zones (**zone**), keywords (**keyword**), keyword categories (**keyword-category**), policy rules (**policy**), SNAT rules (**snat**), DNAT rules (**dnat**), session limit rules number (**session-limit**), statistics se t (**statistic-set**), new session rates (**cps**) and IPSec VPN tunnels (**tunnel-ipsec**).

To configuring the resource quota of a VSYS, in the VSYS profile configuration mode, use the following command:

{cpu | session | zone | keyword {simple | regexp} | keyword-category | policy | snat | dnat | session | session-limit | statistic-set{non-session-based | session-based} | tunnel-ipsec | scvpn-user | cps} max *max-num* [**reserve** *reserve-num*] [**alarm** *alarm-num*]

- {**simple** | **regexp**} - Only applicable to **keyword. simple** is used to specify the quota of simple keyword. **regexp** is used to specify the quota of regular expression keyword.
- **max** *max-num*- Specifies the maximum quota value. The reserved quota and maximum quota vary from different platforms. The reserved quota should not exceed the maximum quota. Table below shows the value range of the maximum quota and minimum number of reserved quota.
- **reserve***reserve-num* - Specifies the reserved quota values.
- **alarm** *alarm-num* - Only applicable to CPU. With this parameter configured, the system will generate alarm logs when the CPU utilization exceeds the specified percentage. The value range is 50 to 99.

System Resource	Value range of maximum quota	Minimum number of reserved quota
CPU	1 – 10000	0
sessions	min (max-num①, 256) – max-num①	0
Zones	(max-num①-res-num③) –	0

System Resource	Value range of maximum quota	Minimum number of reserved quota
	max-num①	
Keywords in each keyword category	• Simple: 0 – max-num① • Regular expression: 0 – 10	0
Keyword categories	0 – max-num①	0
Policy rules	0 – max-num①	0
SNAT rules	0 – max-num1②	0
DNAT rules	0 – max-num1②	0
Session Limit Rules Number	• root VSYS Profile: 128(fixed value) • non-root VSYS Profile: 0 – 118	• root VSYS Profile: 10(fixed value) • non-root VSYS Profile: 0
Statistics set	0 - 32	0
IPSec VPN tunnels	0 – max-num①	0
SSL VPN users' number	0 – max-num①	0
New session rate	10-50000000	--

max-num①: The overall capacity limit of the module

max-num1②: The individual capacity limit of each VSYS of the module

res-num③: The reserved quota of the module

To restore to the default quota, in the VSYS profile configuration mode, use the following command:

no {**cpu** | **session** | **zone** | **keyword** {**simple** | **regexp**} | **keyword-category** | **policy** | **snat** | **dnat** | **session** | **session-limit** | **statistic-set**{**non-session-based** | **session-based**} | **tunnel-ipsec** | **scvpn-user**| **cps**} **max** *max-num* [**reserve** *reserve-num*] [**alarm** *alarm-num*]

Configuring the Quota of Log Buffer

After configuring to send logs to the memory buffer, you can specify the reserved buffer quota and maximum buffer quota for each type of logs in a VSYS by creating a VSYS profile. Reserved quota refers to the memory buffer value reserved for each type of logs; maximum quota refers to the maximum memory buffer value available to each type of logs. The root administrator has the permission to create VSYS profiles. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.

To configure the quota of buffer for each type of logs, in the VSYS profile configuration mode, use the following command:

log {**configuration** | **operation** | **event** | **network** | **threat** | **traffic** {**session** | **nat** | **websurf**}} **buffer-size max** *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num*- Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of configuration logs, operation logs, event logs, network logs, threat logs, traffic logs(including session logs, NAT logs and websurf logs) in a VSYS. The range of reserved quota or maximum quota varies from different platforms. The reserved quota should not exceed the maximum quota.

Configuring URL Filter

The root administrator can configure whether enable URL filter or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable URL filter. VSYSs share URL resources including URL, URL category and URL Profile. You can specify the reserved quota and maximum quota for each type of URL resources.

To enable URL filter or configure URL resources in a VSYS Profile, you need to enter urlfilter configuration mode first, in the VSYS profile configuration mode, use the following command:

urlfilter

To enable or disable URL filter, in the urlfilter configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure URL resources quota, in the urlfilter configuration mode, use the following command:

{**url** | **url-category** | **url-profile**} **max** *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of tatal URLs, user-defined URL category and URL Profile in a VSYS. The range of reserved quota or maximum quota varies from different platforms. The reserved quota should not exceed the maximum quota. Table below shows the value range of the maximum quota and minimum number of reserved quota. The default value of maximum quota is the system capacity. The default value of minimum quota is 0.

URL Resource	Value range of maximum quota	Minimum number of reserved quota
URL	0 – Capacity	0
User-defined URL category	0 – 26	0
URL Profile	0 – 32	0

Configuring IPS

The root administrator can configure whether enable IPS or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable IPS. VSYSs share IPS Profile resources. You can specify the reserved quota and maximum quota.

To enable IPS or configure IPS Profile resources in a VSYS Profile, you need to enter IPS configuration mode first, in the VSYS profile configuration mode, use the following command:

ips

To enable or disable IPS, in the IPS configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure IPS Profile resources quota, in the IPS configuration mode, use the following command:

profile max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* - Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of IPS Profile in a VSYS. You can create up to four IPS profiles in a non-root VSYS. That is, the range of maximum quota is from 0 to 4. The default value is 4. The default value of the reserved quota is 0, which means only predefined IPS Profiles can be used in non-root VSYS.

Configuring Anti-Virus

The root administrator can configure whether enable Anti-Virus or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable Anti-Virus. VSYSs share AV Profile resources. You can specify the reserved quota and maximum quota.

To enable AV or configure AV Profile resources in a VSYS Profile, you need to enter AV configuration mode first, in the VSYS profile configuration mode, use the following command:

av

To enable or disable Anti-Virus, in the AV configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure AV Profile resources quota, in the AV configuration mode, use the following command:

profile max*max-num***reserve***reserve-num*

- **max***max-num***reserve***reserve-num* – Specifies the maximum quota (**max***max-num*) and reserved quota (**reserve***reserve-num*) of AV Profile in a VSYS. The range of maximum quota varies from 0 to 32. The reserved quota should not exceed the maximum quota. The default value of maximum quota is 32 and the default value of reserved quota is 0.

Configuring Perimeter Traffic Filtering

The root administrator can configure whether enable perimeter traffic filtering or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable perimeter traffic filtering. VSYSs share user-defined black/white list resources. You can specify the reserved quota and maximum quota.

To enable perimeter traffic filtering or configure user-defined black/white list resources in a VSYS Profile, you need to enter AV configuration mode first, in the VSYS profile configuration mode, use the following command:

perimeter-traffic-filtering

To enable or disable perimeter traffic filtering, in the perimeter traffic filtering configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure user-defined black/white list resources quota, in the perimeter traffic filtering configuration mode, use the following command:

userdefine max*max-num***reserve***reserve-num*

- **max***max-num***reserve***reserve-num* – Specifies the maximum quota (**max***max-num*) and reserved quota (**reserve***reserve-num*) of user-defined black/white list in a VSYS. The range of maximum quota varies from 0 to 1000. The reserved quota should not exceed the maximum quota. The default value of maximum quota is 1000 and the default value of reserved quota is 0.

Configuring QoS

Root RXW administrators can configure whether enable QoS or not in a VSYS Profile. Then you can bind a VSYS Profile to a non-root VSYS to enable or disable QoS. You can specify the reserved quota and maximum quota for root-pipe.

To enable QoS or configure QoS Profile resources in a VSYS Profile, you need to enter QoS configuration mode first, in the VSYS profile configuration mode, use the following command:

iqos

To enable or disable QoS, in the QoS configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

To configure QoS Profile resources quota, in the QoS configuration mode, use the following command:

root-pipe max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – Specifies the maximum quota (max max-num) and reserved quota (reserve reserve-num)of root-pipe in a VSYS. The reserved quota should not exceed the maximum quota. The default value of maximum quota and reserved quota is 0.

Configuring Botnet Prevention

The root system administrator can configure whether to enable the Botnet Prevention function by using VSYS Profile and bind it to VSYS, thereby controlling whether non-root VSYS supports the Botnet Prevention function. In StoneOS, each VSYS shares the botnet prevention profile resource and the administrator can configure the maximum quota and reserved quota for each VSYS.

Entering the Botnet Prevention Configuration Mode

To enable the Botnet Prevention function or configure the botnet prevention profile resource in VSYS Profile, you need to enter the botnet prevention configuration mode first. To do this, use

the following command in VSYS Profile configuration mode:

botnet-c2-prevention

Enabling or Disabling the Botnet Prevention Function

By default, the Botnet Prevention function is disabled. To enable or disable this function, use the following command in botnet prevention configuration mode:

- Enable: **enable**
- Disable: **no enable**

Configuring the Quota of Botnet Prevention Profile Resource in VSYS

To configure the quota of botnet prevention profile resource in VSYS, use the following command in botnet prevention configuration mode:

profile max*max-num***reserve***reserve-num*

- **max***max-num***reserve***reserve-num* – Specifies the maximum quota (**max***max-num*) and reserved quota (**reserve***reserve-num*) for the number of botnet prevention profiles in VSYS. The valid values for the maximum quota is from 0 to 32. The reserved quota cannot exceed the maximum quota. The default value of the maximum quota and the reserved quota is 32 and 0 respectively.



Notes: You can configure up to a total of 29 custom botnet prevention profiles in the root VSYS and non-root VSYS.

Enabling/Disabling the CPU Resource Quota

By default, the configured CPU resource quota will take effect immediately. You can also use the following command to disable the VSYS CPU resource check. That is, the configured CPU resource quota will not take effect and each VSYS will preempt the CPU resource in system. To disable or enable CPU resource quota, in the global configuration mode of the root VSYS, use the following command:

- Disable: **vsys-resource cpu disable**
- Enable: **vsys-resource cpu enable**



Notes: For some Hillstone devices (X9180, X10800, K9180), it is not supported to enable or disable the configured CPU resource quota.

Binding a VSYS Profile to a VSYS

To bind a VSYS profile to an existing VSYS, in the VSYS configuration mode, use the following command:

profile *vsys-profile-name*

- *vsys-profile-name* - Specifies the name of the VSYS profile to be bound.

To restore to the default binding, in the VSYS configuration mode, use the command **no profile**.



Notes:

- When binding a VSYS profile to a VSYS, if the total number of the reserved quota in all VSYSs exceeds the current capacity, the binding operation will fail.
- Only after cancelling the binding can you delete the VSYS profile.

Entering the VSYS

To enter a **root VSYS**, take the following steps:

1. Start a connection client on the local PC, type the management IP and port to connect with the device.

2. Type the username and password according to the prompt, which can be the username and password of the root administrator or the user configured in the authentication server (local server / Radius server / TACACS+ server) of the root VSYS.

3. Press **Enter** to enter the root VSYS.

To enter a **non-root VSYS**, the following three ways are available:

The first way: to enter a non-root VSYS, take the following steps:

1. Enter a root VSYS.

2. In the global configuration mode of the root VSYS, use command **vsys***vsys-name* to create a non-root VSYS. For more information on creating non-root VSYS, see Creating a Non-root VSYS.

3. Start a connection client on the local PC, type the management IP and port to connect with the device.

4. Type the username (vsys_name\admin) and password (vsys_name-admin) of the non-root administrator according to the prompt.
   For example, if the management IP of root VSYS is 10.90.89.1, after typing the username (hillstone) and password (hillstone), you can enter the root VSYS. After creating the non-root VSYS (vsys1), you should type the management IP 10.90.89.1, the non-root administrator username (vsys1\admin) and password (vsys1-admin), and then you can enter the non-root VSYS directly. For more information on configuring administrators, see Configuring System Admin Users.

5. Press **Enter** to enter the non-root VSYS.



Notes: If you directly enter the non-root VSYS through the above method, you cannot exit the current non-root VSYS and back to the root VSYS by using the command **exit-vsys**. You should logout the system and enter the root VSYS again.

The second way: the root VSYS administrator can enter the non-root VSYS from root VSYS. The administrator in the root VSYS can configure the functions of the non-root VSYS after entering it. To enter a non-root VSYS, in the execution mode or the global configuration mode of the root VSYS, use the following command:

enter-vsys *vsys-name*

- *vsys-name* - Specifies the name of the non-root VSYS.

To enter a non-root VSYS by alias, in the execution mode or the global configuration mode of the root VSYS, use the following command:

enter-vsys alias *alias-name*

- **alias** *alias-name* – Specifies the alias of the non-root VSYS.

To exit the current non-root VSYS and back to the execution mode or global configuration mode of the root VSYS, in the execution mode or global configuration mode of the non-root VSYS, use the command **exit-vsys**.

The third way: to enter a non-root VSYS via the authentication server (local server / Radius server / TACACS+ server) configured in the non-root VSYS, take the following steps:

1. Enter a non-root VSYS.
2. In the global configuration mode of the non-root VSYS, use command **aaa-server***aaa-server-name* [**type**] {**local** | **radius** | **tacacs+**} to create and configure an AAA server (local server / Radius server / TACACS+ server). For more information on AAA server, see "Configuring an AAA Server" on Page 1168.
3. In the global configuration mode of the non-root VSYS, use command **admin auth-server** *server-name* to specify the configured AAA server as the authentication server for the non-root administrator. For more information on specifying an authentication server for the system administrator, see "Configuring Authentication and Authorization for the Server" on Page 1252.

4. Start a connection client on the local PC, type the management IP and port to connect with the device.
5. Type the username and password configured in the AAA server according to the prompt.
6. Press **Enter** to enter the non-root VSYS.

Configuring the Shared Property

To make the VRouter, VSwitch, or zone in the root VSYS shared, in the VRouter/VSwitch/zone configuration mode of the root VSYS, use the following command:

vsys-shared

To remove the shared property, in the VRouter/VSwitch/zone configuration mode of the root VSYS, use the command **no vsys-shared**.



Notes: This feature is only supported on K9180, K6280-GS, K6580, K5680, K3680-GS, K3280, K2580, K2560, K1280, K2680, K2380, X10800 and X9180.

Exporting a Physical Interface

By default, all the physical interfaces on the device belong to the root VSYS. RXW administrator in the root VSYS can export physical interfaces in the root VSYS to non-root VSYSs, and also, the root administrator in the root VSYS can export the physical interfaces in non-root VSYSs back to the root VSYS. The physical interfaces to be exported should not be bound to any zone, or be the member of BGroup interface, aggregate interface, PPPoE interface, VSwitch interface, VLAN interfave or redundant interface, or have any sub-interface. All the interfaces that are related to the physical interface in the non-root VSYS (e.g., the sub-interface created after the physical interface is exported from the root VSYS to non-root VSYS) can only be used in the non-root VSYS.

To export a physical interface to a non-root VSYS, in the interface configuration mode, use the following command:

export-to *vsys-name*

- *vsys-name* – Specifies the non-root VSYS name to which the interface will be exported.

To export a physical interface to a non-root VSYS by alias, in the interface configuration mode, use the following command:

export-to alias *alias_name*

- **alias** *alias_name* – Specifies the non-root VSYS alias to which the interface will be exported.

To export the physical interface in the non-root VSYS back to the root VSYS, in the interface configuration mode, use the command **no export-to**.

Allocating a Logical Interface

The root administrator in the root VSYS can allocate the logical interfaces in the root VSYS to non-root VSYSs, and also, can restore the allocated logical interfaces to the root VSYS.

To allocate a logical interface in the root VSYS to a non-root VSYS, in the interface configuration mode, use the following command:

vsys *vsys-name*

- *vsys-name* - Specifies the name of the non-root VSYS to which the interface will be allocated.

To allocate a logical interface in the root VSYS to a non-root VSYS by alias, in the interface configuration mode, use the following command:

vsys alias *alias_name*

- **alias** *alias_name* – Specifies the alias of the non-root VSYS to which the interface will be allocated.

To restore the interface to the root VSYS, in the interface configuration mode, use the command **no vsys**.

Binding a Track Object

You can bind a track objet to a non-root VSYS, thus monitoring the status of this VSYS. To complete the binding, in the non-root VSYS configuration mode, use the following command:

vsys-track-status track *track-name*

- *track-name* - Specifies the name of the track object. Ensure that this track object is created in this non-root VSYS.

To complete the binding by alias, in the non-root VSYS configuration mode, use the following command:

vsys alias *alias_name*

- **alias** *alias_name* – Specifies the alias of the track object. Ensure that this track object is created in this non-root VSYS.

To cancel the binding, in the non-root VSYS configuration mode, use the following command:

no vsys-track-status track *track-name*



Notes:

- After you cancel the binding, you can delete the track object.
- For more information about configuring track object, see "Configuring a Track Object" of "System Management".

Monitoring a Specified VSYS

In the root VSYS, you can monitor the status of a specified VSYS. According to the change of the status, you can take corresponding actions. To monitor a specified VSYS, use the following command in the track object configuration mode in the root VSYS

vsys *vsys-name* **weight** *value*

- *vsys-name* – Specifies the VSYS name. This is the one that you want to monitor.
- **weight** *value* – Specifies the weight. Specifies how important this entry failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255.



Notes: Monitoring the status of a specified VSYS is only available in High Availability.

Rolling Back to Previous Configurations

To roll back to the previous configuration, there're two ways:

In the execution mode, use the following command to roll back to the previous configuration. StoneOS saves the latest ten versions of system configurations as initial configuration files for you to use in system initiation. When the system restarts, the specified configuration will be used.

rollback configuration backup *number*

- *number* - Specifies the number of initial configuration file.

In the configuration rollback mode, use the following command to roll back to the previous configuration and exit the configuration rollback mode. The configuration will be valid without restarting the device.

exec configuration rollback



Notes:

- In the execution mode, you should use **exec configuration start** command to enter the rollback mode.
- You cannot switch among VSYS when starting the rollback mode.
- For each VSYS, you can enable and disable the rollback mode separately.
- For each VSYS, only one user is allowed to enable and disable the configuration of rollback mode at a time.
- IF configuring the rollback mode for root VSYS, system cannot operate the followings: switching HA status, switching between HA master and backup device, creating or deleting HA Cluster, creating or deleting VSYS, and modifying VSYS resources quota.

For example:

```
hostname# exec configuration start  (Enter the configuration rollback
```

```
mode)
hostname[TRN]# configure (Enter the global configuration mode)
…… (Execute any configuration, and the configuration
will be valid immediately)
hostname[TRN](config)# exec configuration rollback (Roll back the con-
figuration and exit the configuration rollback mode)
hostname#
```

Exiting the Configuration Rollback Mode

To exit the configuration rollback mode directly, you can use the following two ways:

In the configuration rollback mode, use the following command to exit the configuration rollback mode directly.

exec configuration commit

For example:

```
hostname# exec configuration start (Enter the configuration rollback
mode)
hostname[TRN]# configure (Enter the global configuration mode)
…… (Execute any configuration, and the configuration
will be valid immediately)
hostname[TRN](config)# exec configuration commit (Exit the con-
figuration rollback mode directly)
hostname#
```

In the configuration rollback mode, use the command **exit**to exit the terminal directly.



Tip:

- When different users log in the device meanwhile, only the user who enters the configuration rollback mode first can do further configuration, and the later users cannot.
- When a user log in the device through different access methods, the user of a certain access method enters in the configuration rollback mode first can do further configuration, and the later users of other access methods cannot. The user of other access methods can force the user of that access method to exit the configuration rollback mode through command.

Configuring the Action

When exiting the configuration rollback mode by using command **exit**, system wil exit the configuration rollback mode directly by default. To roll back to the previous configuration and exit the configuration rollback mode, in the global configuration mode, take the following command:

cli-exit-action rollback

To restore to the default value, in the global configuration mode, take the following command:

cli-exit-action commit



Notes: For each VSYS, you can use the above command separately to specify its own action.

Configuring VSYS Log

At the time of writing, the system supports logs for AAA, NAT/NAT444, policy, routing, attack defense, interface, DNS, service, DHCP and system management events in VSYS. For more information about how to configure and view logs, see "Logs".



Notes: In non-root VSYS, the system does not support debugging, IPS and NBC logs.

Configuring Cross-VSYS Traffic Forwarding

In order to realize the cross-VSYS traffic forwarding function, the system introduces the concept of Simple-Switch, it is a special VSwitch, which can only learn MAC address, forward the known unicast packet or flooding. You can create a VWANIF interface, and assigned to the designated VSYS, the different VSYS can communicate with each other through the VWANIF interface, so that the device is now directly forwarded across different VSYS traffic data packets.

To configure the cross-VSYS traffic forwarding function, take the following steps:

1. Enabling the cross-VSYS traffic forwarding.
2. Configuring a Simple-Switch.

   Including create a Simple-Switch, create a L2 zone and binding the L2 zone to the Simple-Switch.
3. Creating a VWANIF interface and VPort interface.

   After you create a VWANIF interface, you need to create a corresponding VPort interface for the VWANIF interface.
4. Configuring the VPort interface.

   Binding the VPort interface to the L2 zone that has been added to the Simple-Switch.
5. Configuring the VWANIF interface.

   Allocating the VWANIF interface to a VSYS, configuring the zone and IP address for the VWANIF interface.

Enabling/Disabling the Cross-VSYS Traffic Forwarding

By default, the cross-VSYS traffic forwarding function is disabled. To enable/disable the cross-VSYS traffic forwarding function, in the global configuration mode, use the following commands:

- Enable: **vsys-switch-mode**
- Disable: **no vsys-switch-mode**

Configuring a Simple-Switch

Simple-Switch is a special VSwitch, which can only learn MAC address, forward the known unicast packet or flooding. You can create multiple Simple-Switchs, each Simple-Switch is virtually an independent broadcast domain.

Creating a Simple-Switch

To create a Simple-Switch, in the global configuration mode, use the following commands:

vswitch vswitch *Number* [**simple-switch**]

- *Number* - Specifies the numeric identification for the VSwitch. The value range varies from different platforms. Cannot be specified as VSwitch1.
- **simple-switch** - Specifies this parameter to create the Simple-Switch and enter the Simple-Switch configuration mode .

To delete the Simple-Switch, in the global configuration mode, use the following command:

no vswitch vswitch *Number*

Binding the L2 Zone to the Simple-Switch

Binding the L2 zone to a Simple-Switch in two steps.

First, create a L2 zone. In the global configuration mode, use the following command:

zone *zone-name* **l2**

- *zone-name* - Specifies the name of Layer 2 zone.
- **l2** - Specifies the zone as a Layer 2 zone.

Then, in the zone configuration mode, use the following command to bind the L2 zone to a Simple-Switch:

bind *vswitch-name*

- *vswitch-name* - Specifies the name of Simple-Switch to which the Layer 2 zone is bound.

Creating a VWANIF interface



Notes: Non-root VSYS does not support to create the VWANIF interface.

VWANIF interface is a Layer 3 interface, each time you create a VWANIF interface, you need to create a corresponding VPort interface for the VWANIF interface.

To create a VWANIF interface, in the global configuration mode, use the following command:

interface vwanif *id*

- *id* - Specifies the ID of the VWANIF interface. If the specified VWANIF interface does not exist, this command creates a VWANIF interface and leads you to its configuration mode. If the specified VWANIF interface exists, you will enter its configuration mode directly.

To clear the specified VWANIF interface, use the command **no interface vwanif** *id*

Creating a VPort Interface



Notes: Non-root VSYS does not support to create the VPort interface.

To create a VPort interface, in the global configuration mode, use the following command:

interface vport*id*

- *id* – Specifies the ID of the VPort interface, this number must be the same as the number of the paired VWANIF interface. If the specified VPort interface does not exist, this command creates a VPort interface and leads you to its configuration mode. If the specified VPort interface exists, you will enter its configuration mode directly.

To clear the specified VPort interface, use the command**no interface vport***id*.

After the VPort interface is created, you need to bind the VPort interface to the L2 zone that has been added to the Simple-Switch, in the global configuration mode, use the following command:

zone*zone-name*

- *zone -name* – Specifies the L2 zone name that has been added to the Simple-Switch.

Configuring the VWANIF Interface

In order to realize the cross-VSYS traffic forwarding, you also need to allocate the VWANIF interface to a VSYS, and configure the zone , IP address (IPv4 or IPv6) for the VWANIF interface.



Notes: How to configure the zone and IP address (IPv4 or IPv6) for the VWANIF interface, refer to Configuring Interface section.

Allocating a VWANIF Interface

After you create the VWANIF interface, you need to allocate the VWANIF interface to a VSYS, in the interface configuration mode, use the following command:

vsys *vsys-name*

- *vsys-name* - Specifies the name of the VSYS to which the VWANIF interface will be allocated.

Viewing Cross-VSYS Traffic Forwarding Information

To view the cross-VSYS traffic forwarding information, in any mode, use the following command:

show vsys-switch-mode

Viewing the VWANIF interface Configuration Information

To view the VWANIF interface configuration, in any mode, use the following command:

show interface vwanif *id*

Viewing the VWANIF Interface IPv6 Configuration Information

To view the VWANIF interface IPv6 configuration, in any mode, use the following command:

show ipv6 interface vwanif *id*

Viewing VSYS Information

To view the VSYS information, in any mode of the root VSYS, use the following command:

show vsys [*vsys-name*]

- *vsys-name* - Specifies the name of the VSYS whose information you want to view. If this parameter is not specified, the information of all the VSYSs in the system will be displayed.

To view the VSYS information by alias, in any mode of the root VSYS, use the following command:

show vsys alias *alias_name*

- **alias** *alias_name* – Specifies the alias of the VSYS whose information you want to view.

Viewing VSYS Profile Information

To view the VSYS profile information, in any mode of the root VSYS, use the following command:

show vsys-profile [*vsys-profile-name*]

- *vsys-profile-name* - Specifies the name of the VSYS profile whose information you want to view. If this parameter is not specified, the information of all the VSYS profiles in the system will be displayed.

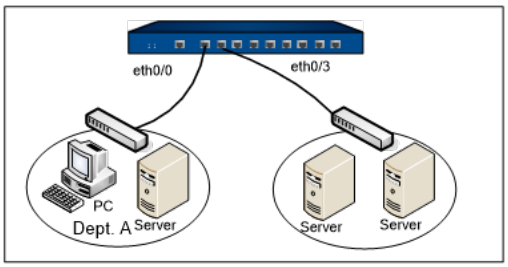
VSYS Configuration Examples

This section describes three typical VSYS configuration examples:

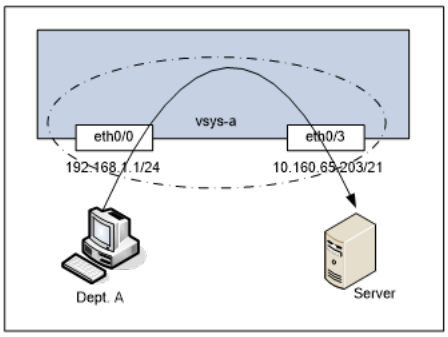
- Example 1: L3 traffic transmitting in a single VSYS
- Example 2: L3 traffic transmitting among multiple VSYSs via shared VRouter
- Example 3: L2 traffic transmitting among multiple VSYSs via shared VSwitch
- Example 4: Traffic transmitting among multiple VSYSs via Simple-Switch

Example 1: L3 Traffic Transmitting in a Single VSYS

An enterprise deploys Hillstone device in its network. The goal is to enable Dept. A to visit Intranet server through ethernet0/0 and ethernet0/3 in a single VSYS. The topology is shown as below:



To meet the above requirement, a VSYS and corresponding policy rules are needed. Below is the logical illustration.



Configuration Steps

Step 1: Create VSYS-a

```
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)#
```

Step 2: Export ethernet0/0 and ethernet0/3 to VSYS-a by the root administrator of the root VSYS:

```
hostname(config)# interface ethernet0/0
hostname (config-if-eth0/0)# export-to vsys-a
```

```
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/3
hostname (config-if-eth0/3)# export-to vsys-a
hostname(config-if-eth0/3)# exit
hostname(config)#
```

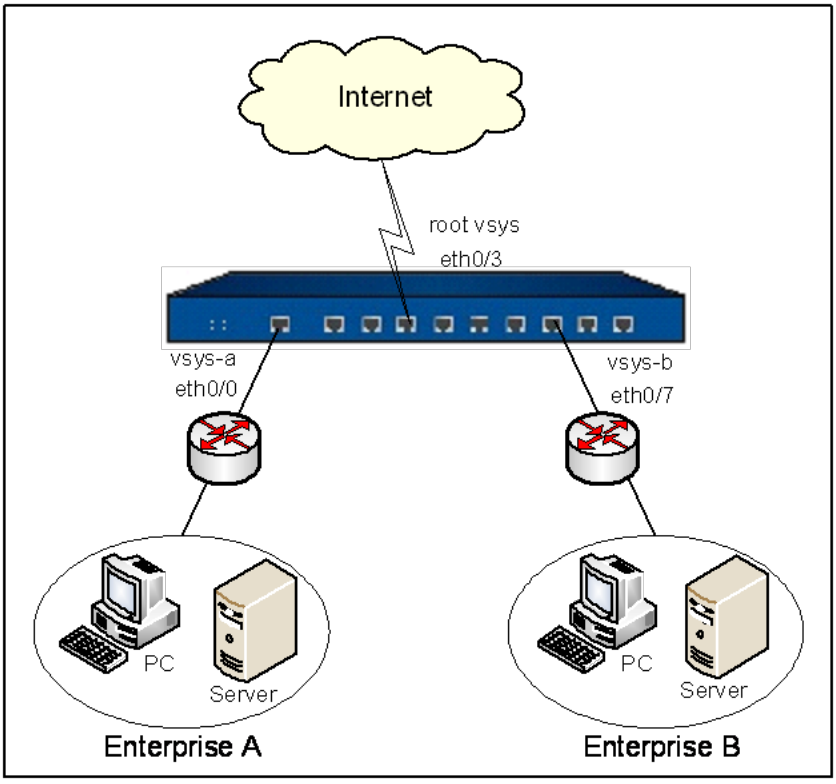
Step 3: Enter VSYS-a to configure ethernet0/0, ethernet0/3 and related policy rules:

```
hostname(config)# enter-vsys vsys-a
hostname(vsys-a)(config)# zone vsys-a-trust
hostname(vsys-a)(config-zone-vsys-a-trust)# exit
hostname(vsys-a)(config)# interface ethernet0/0
hostname(vsys-a)(config-if-eth0/0)# zone vsys-a-trust
hostname(vsys-a)(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(vsys-a)(config-if-eth0/0)# exit
hostname(vsys-a)(config)# zone vsys-a-untrust
hostname(vsys-a)(config-zone-vsys-a-untrust)# exit
hostname(vsys-a)(config)# interface ethernet0/3
hostname(vsys-a)(config-if-eth0/3)# zone vsys-a-untrust
hostname(vsys-a)(config-if-eth0/3)# ip address 10.160.65.203/21
hostname(vsys-a)(config-if-eth0/3)# exit
hostname(vsys-a)(config)# policy-global
hostname(vsys-a)(config-policy)# rule
hostname(vsys-a)(config-policy-rule)# src-zone vsys-a-trust
hostname(vsys-a)(config-policy-rule)# dst-zone vsys-a-untrust
hostname(vsys-a)(config-policy-rule)# src-addr any
hostname(vsys-a)(config-policy-rule)# dst-addr any
hostname(vsys-a)(config-policy-rule)# service any
```

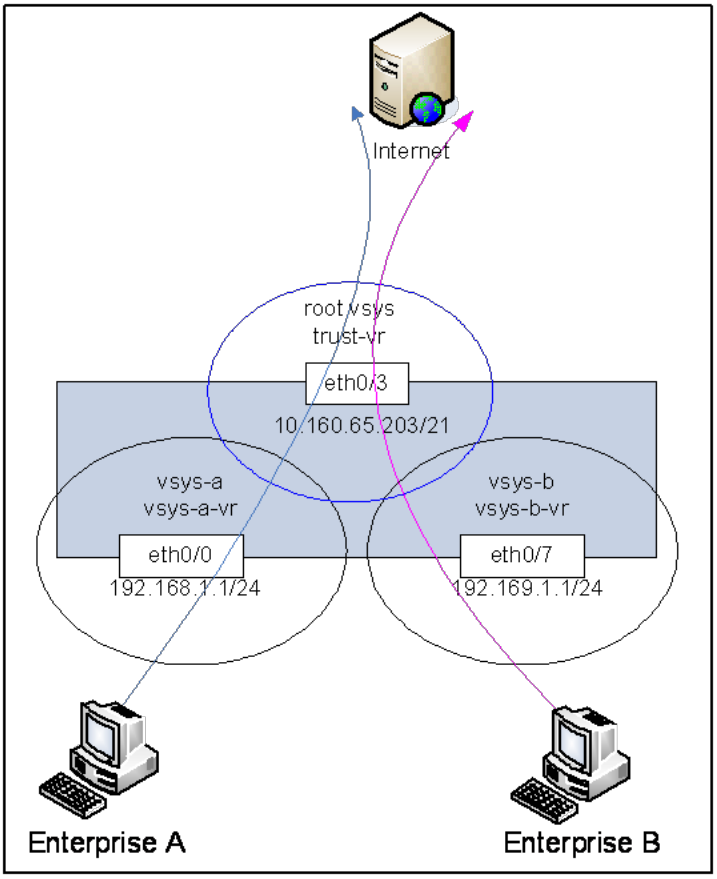
```
hostname(vsys-a)(config-policy-rule)# action permit
hostname(vsys-a)(config-policy-rule)# exit
hostname(vsys-a)(config-policy)# exit
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Example 2: L3 Traffic Transmitting among Multiple VSYSs via Shared VRouters

A Hillstone device is deployed for enterprise A and enterprise B. VSYS-a is configured for enterprise A and VSYS-b is configured for enterprise B. The interface ethernet0/0 is used by enterprise A only and ethernet0/7 is used by enterprise B only. The interface ethernet0/3 is shared by enterprise A and B, and the two enterprises visit Internet through enthernet0/3. See the topology below:



To meet the above requirement, the shared VRouter, corresponding routes, SNAT rules, and policy rules are needed. Below is the logical illustration.



Notes: This case is only supported on K9180, K6280-GS, K6580, K5680, K3680-GS, K3280, K2580, K2560, K1280, K2680, K2380, X10800 and X9180.

Configuration Steps

Step 1: Configure Root VSYS:

```
Create vsys-a and vsys-b
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)# vsys vsys-b
hostname(config-vsys)# exit
hostname(config)#
```

```
Configure ethernet0/3, routes, SNAT rules, and DNS
server
hostname(config)# interface ethernet0/3
hostname(config -if-eth0/3)# zone untrust
hostname(config -if-eth0/3)# ip address 10.160.65.203/21
hostname(config -if-eth0/3)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 10.160.64.1
hostname(config-vrouter)# snatrule from any to any eif ethernet0/3 trans-to eif-ip
mode dynamicport
rule ID=3
hostname(config-vrouter)# exit
hostname(config)# ip name-server 202.106.0.20
hostname(config)#
Share trust-vr in Root VSYS
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# vsys-shared
hostname(config-vrouter)# exit
hostname(config)#
Share untrust zone in Root VSYS
hostname(config)# zone untrust
hostname(config-zone-untrust)# vsys-shared
hostname(config-zone-untrust)# exit
hostname(config)#
```

Step 2: Configure VSYS-a:

```
Login the system using the root administrator's cre-
dential of Root VSYS, and export ethernet0/0 to VSYS-a
```

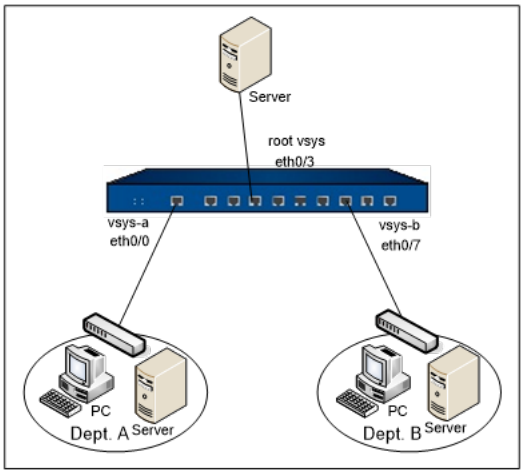
```
hostname(config)# interface ethernet0/0
hostname (config-if-eth0/0)# export-to vsys-a
hostname(config-if-eth0/0)# exit
hostname(config)#
Enter VSYS-a and configure ethernet0/0, policy rules,
and cross-VR routes
hostname(config)# enter-vsys vsys-a
hostname(vsys-a)(config)# interface ethernet0/0
hostname(vsys-a)(config-if-eth0/0)# zone vsys-a-trust
hostname(vsys-a)(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(vsys-a)(config-if-eth0/0)# exit
hostname(vsys-a)(config)# policy-global
hostname(vsys-a)(config-policy)# rule
hostname(vsys-a)(config-policy-rule)# src-zone vsys-a-trust
hostname(vsys-a)(config-policy-rule)# dst-zone untrust
hostname(vsys-a)(config-policy-rule)# src-addr any
hostname(vsys-a)(config-policy-rule)# dst-addr any
hostname(vsys-a)(config-policy-rule)# service any
hostname(vsys-a)(config-policy-rule)# action permit
hostname(vsys-a)(config-policy-rule)# exit
hostname(vsys-a)(config)# ip vrouter vsys-a-vr
hostname(vsys-a)(config-vrouter)# ip route 0.0.0.0/0 vrouter trust-vr
hostname(vsys-a)(config-vrouter)# exit
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Step 3: Configure VSYS-b:

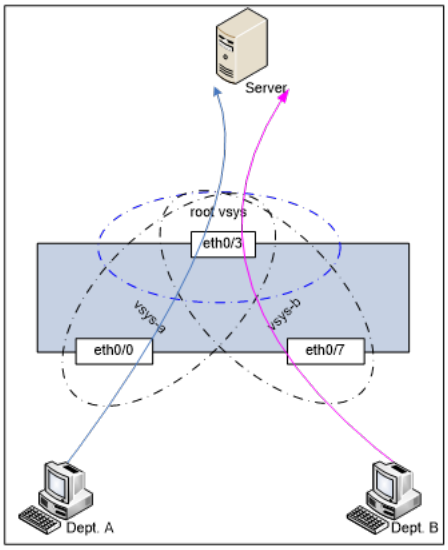
```
Login the system using the root administrator's cre-
dential of Root VSYS, and export ethernet0/7 to VSYS-b
hostname(config)# interface ethernet0/7
hostname (config-if-eth0/7)# export-to vsys-b
hostname(config-if-eth0/7)# exit
hostname(config)#
Enter VSYS-b and configure ethernet0/7, policy rules,
and cross-VR routes
hostname(config)# enter-vsys vsys-b
hostname(vsys-b)(config)# interface ethernet0/7
hostname(vsys-b)(config-if-eth0/7)# zone vsys-b-trust
hostname(vsys-b)(config-if-eth0/7)# ip address 192.169.1.1/24
hostname(vsys-b)(config-if-eth0/7)# exit
hostname(vsys-b)(config)# policy-global
hostname(vsys-b)(config-policy)# rule
hostname(vsys-b)(config-policy-rule)# src-zone vsys-b-trust
hostname(vsys-b)(config-policy-rule)# dst-zone untrust
hostname(vsys-b)(config-policy-rule)# src-addr any
hostname(vsys-b)(config-policy-rule)# dst-addr any
hostname(vsys-b)(config-policy-rule)# service any
hostname(vsys-b)(config-policy-rule)# action permit
hostname(vsys-b)(config-policy-rule)# exit
hostname(vsys-b)(config)# ip vrouter vsys-b-vr
hostname(vsys-b)(config-vrouter)# ip route 0.0.0.0/0 vrouter trust-vr
hostname(vsys-b)(config-vrouter)# exit
hostname(vsys-b)(config)# exit-vsys
hostname(config)#
```

Example 3: L2 Traffic Transmitting among Multiple VSYSs via Shared VSwitch

An enterprise deploys a Hillstone device in its network. VSYS-a is configured for Dept. A, and VSYS-b is configured for Dept. B. The interface ethernet0/0 is used by VSYS-a only and eth-erent0/7 is used by VSYS-b only. The interface etherenet0/3 is shared by Dept. A and Dept. B, and the two departments visit an Intranet server through ethernet0/3. See the topology below:



To meet the above requirement, the shared VSwitch and corresponding policy rules are needed. Below is the logical illustration.





Notes: This case is only supported on K9180, K6280-GS, K6580, K5680, K3680-GS, K3280, K2580, K2560, K1280, K2680, K2380, X10800 and X9180.

Configuration Steps

Step 1 : Configure Root VSYS:

```
Create vsys-a and vsys-b
hostname(config)# vsys vsys-a
hostname(config-vsys)# exit
hostname(config)# vsys vsys-b
hostname(config-vsys)# exit
hostname(config)#
Share VSwitch1 in Root VSYS
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# vsys-shared
hostname(config-vswitch)# exit
Share L2-trust zone in Root VSYS
hostname(config)# zone l2-trust
hostname(config-zone-l2-tru~)# vsys-shared
hostname(config-zone-l2-tru~)# exit
hostname(config)#
Configure ethernet0/3
hostname(config)# interface ethernet0/3
hostname(config -if-eth0/3)# zone l2-trust
hostname(config -if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure VSYS-a:

Log into the system using the root administrator’s credential of Root VSYS, and export ethernet0/0 to VSYS-a

hostname(config)# **interface ethernet0/0**

hostname (config-if-eth0/0)# **export-to vsys-a**

hostname(config-if-eth0/0)# **exit**

hostname(config)#

Enter VSYS-a, and create a VSwitch and a L2 zone. Bind the created L2 zone to the shared VSwitch1

hostname(config)# **enter-vsys vsys-a**

hostname(vsys-a)(config)# **zone a-l2 l2**

hostname(vsys-a)(config-zone-a-l2)# **bind vswitch1**

hostname(vsys-a)(config-zone-a-l2)# **exit**

hostname(vsys-a)(config)#

Configure ethernet0/0 and policy rules

hostname(vsys-a)(config)# **interface ethernet0/0**

hostname(vsys-a)(config-if-eth0/0)# **zone a-l2**

hostname(vsys-a)(config-if-eth0/0)# **exit**

hostname(vsys-a)(config)# **policy-global**

hostname(vsys-a)(config-policy)# **rule**

hostname(vsys-a)(config-policy-rule)# **src-zone a-l2**

hostname(vsys-a)(config-policy-rule)# **dst-zone l2-trust**

hostname(vsys-a)(config-policy-rule)# **src-addr any**

hostname(vsys-a)(config-policy-rule)# **dst-addr any**

hostname(vsys-a)(config-policy-rule)# **service any**

hostname(vsys-a)(config-policy-rule)# **action permit**

hostname(vsys-a)(config-policy-rule)# **exit**

hostname(vsys-a)(config-policy)# **exit**

```
hostname(vsys-a)(config)# exit-vsys
hostname(config)#
```

Step 3: Configure VSYS-b:

```
Log into the system using the root administrator’s credential of Root VSYS, and export ethernet0/7 to VSYS-b
hostname(config)# interface ethernet0/7
```

123

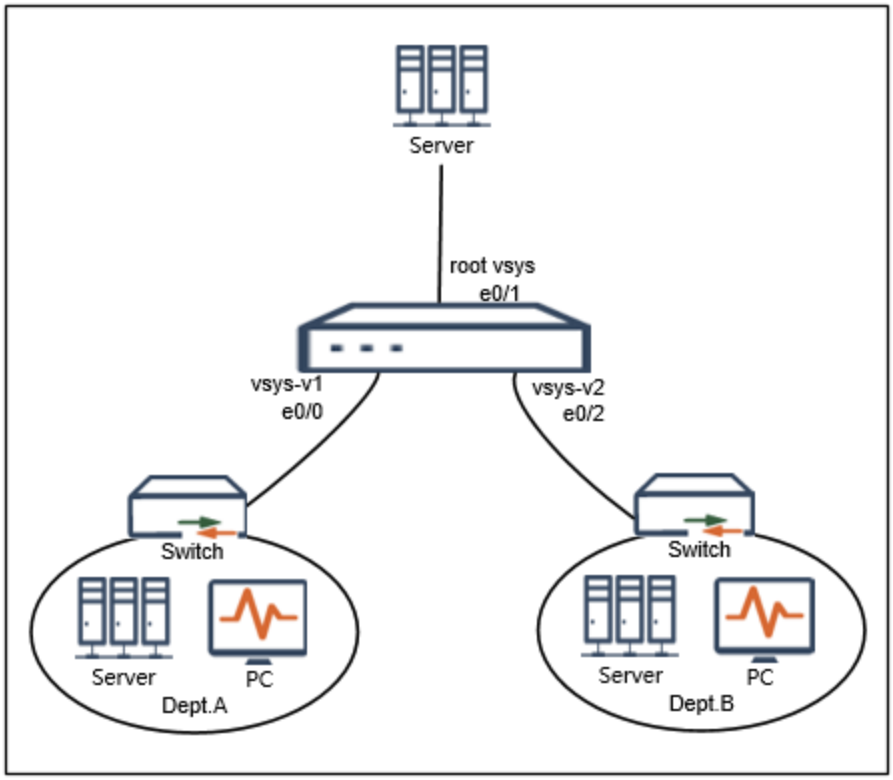
```
hostname (config-if-eth0/7)# export-to vsys-b
hostname(config-if-eth0/7)# exit
hostname(config)#
Enter VSYS-b, and create a VSwitch and a L2 zone. Bind the created L2 zone to the shared VSwitch1
hostname(config)# enter-vsys vsys-b
hostname(vsys-b)(config)# zone b-l2 l2
hostname(vsys-b)( config-zone-b-l2)# bind vswitch1
hostname(vsys-b)( config-zone-b-l2)# exit
hostname(vsys-b)(config)#
Configure ethernet0/7 and policy rules
hostname(vsys-b)(config)# interface ethernet0/7
hostname(vsys-b)(config-if-eth0/7)# zone b-l2
hostname(vsys-b)(config-if-eth0/7)# exit
hostname(vsys-b)(config)# policy-global
hostname(vsys-b)(config-policy)# rule
```

```
hostname(vsys-b)(config-policy-rule)# src-zone b-l2
hostname(vsys-b)(config-policy-rule)# dst-zone l2-trust
hostname(vsys-b)(config-policy-rule)# src-addr any
```

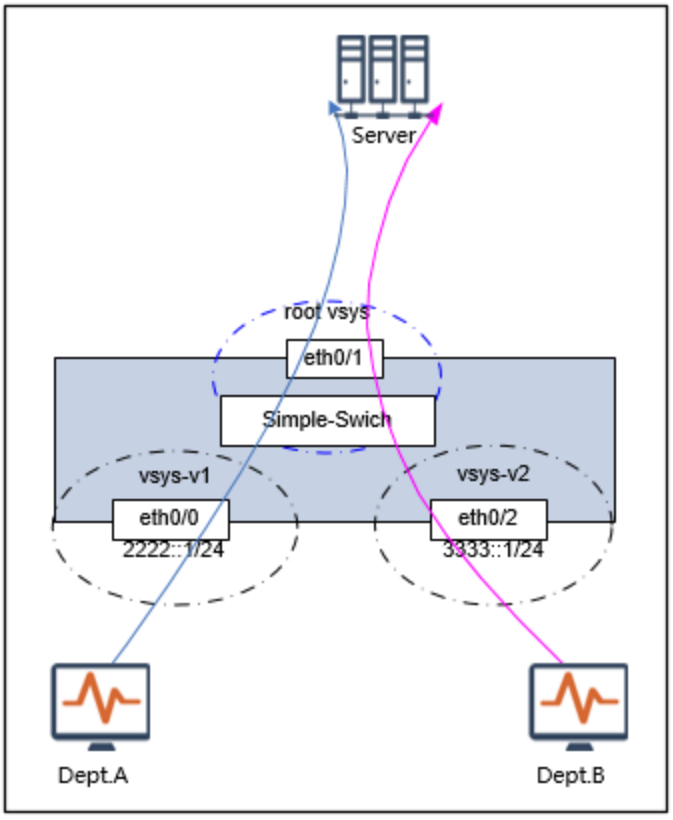
```
hostname(vsys-b)(config-policy-rule)# dst-addr any
hostname(vsys-b)(config-policy-rule)# service any
hostname(vsys-b)(config-policy-rule)# action permit
hostname(vsys-b)(config-policy-rule)# exit
hostname(vsys-b)(config)# exit-vsys
hostname(config)#
```

Example 4: Traffic transmitting among multiple VSYSs via Simple-Switch

An enterprise deploys a Hillstone device in its network. VSYS-v1 is configured for Dept. A, and VSYS-v2 is configured for Dept. B. The interface ethernet0/0 is used by VSYS-v1 only and ethernet0/2 is used by VSYS-v2 only. To make Dept. A and Dept. B belong to two different vsys, and can access each other through ethernet0/0 and ethernet0/2, see the topology below:



To meet the above requirement, the Simple-Switch, VWANIF interface, VPort interface and corresponding route, policy rules are needed. Below is the logical illustration.



Configuration Steps

Step 1: Configure Root VSYS:

```
Create vsys-v1 and vsys-v2
hostname(config)# vsys vsys-v1
hostname(config-vsys)# exit
hostname(config)# vsys vsys-v2
hostname(config-vsys)# exit
hostname(config)#
Configure VSwitch2 Simple-Switch in Root VSYS
hostname(config)# vsys-switch-mode
hostname(config)# vswitch vswitch2 simple-switch
hostname(config-vswitch)# exit
```

```
Configure L2-simple zone in Root VSYS
hostname(config)# zone l2-simple l2
hostname(config-zone-l2-sim~)# bind vswitch2
hostname(config-zone-l2-sim~)# exit
hostname(config)#
Configure vwanif1, vport1
hostname(config)# interface vwanif1
hostname(config -if-vwa1)# vsys vsys-v1
hostname(config -if-vwa1)# exit
hostname(config)#interface vport1
hostname(config -if-vpo1)# zone l2-simple
hostname(config -if-vpo1)# exit
hostname(config)#
Configure vwanif2, vport2
hostname(config)# interface vwanif2
hostname(config -if-vwa1)# vsys vsys-v2
hostname(config -if-vwa1)# exit
hostname(config)#interface vport2
hostname(config -if-vpo1)# zone l2-simple
hostname(config -if-vpo1)# exit
hostname(config)#
Configure ethernet0/0
hostname(config)# interface ethernet0/0
hostname(config -if-eth0/0)# vsys vsys-v1
hostname(config -if-eth0/0)# exit
hostname(config)#
Configure ethernet0/2
```

```
hostname(config)# interface ethernet0/2
hostname(config -if-eth0/2)# vsys vsys-v2
hostname(config -if-eth0/2)# exit
hostname(config)#
```

Step 2: Configure VSYS-v1:

```
hostname(config)# enter-vsys vsys-v1
hostname(vsys-v1)(config)# interface vwanif1
hostname(vsys-v1)(config-if-vwa1)# zone vsys-v1-trust
hostname(vsys-v1)(config-if-vwa1)# ipv6 enable
hostname(vsys-v1)(config-if-vwa1)# ipv6 address 6666::1/64
hostname(vsys-v1)(config-if-vwa1)# exit
hostname(vsys-v1)(config)# interface ethernet0/0
hostname(vsys-v1)(config-if-eth0/0)# zone vsys-v1-trust
hostname(vsys-v1)(config-if-eth0/0)# ipv6 enable
hostname(vsys-v1)(config-if-eth0/0)# ipv6 address 2222::1/64
hostname(vsys-v1)(config-if-eth0/0)# exit
hostname(config)#
Configure route for VSYS-v1
hostname(vsys-v1)(config)# ip vrouter vsys-v1-vr
hostname(vsys-v1)(config-vrouter)# ipv6 route 3333::1/64 6666::2
hostname(vsys-v1)(config-vrouter)# exit
hostname(vsys-v1)(config)# policy-global
hostname(vsys-v1)(config-policy)# default-action permit
hostname(vsys-v1)(config-policy)# exit
hostname(vsys-v1)(config)# exit-vsys
hostname(config)#
```

Step 3: Configure VSYS-v2:

```
hostname(config)# enter-vsys vsys-v2
hostname(vsys-v2)(config)# interface vwanif2
hostname(vsys-v2)(config-if-vwa2)# zone vsys-v2-trust
hostname(vsys-v2)(config-if-vwa2)# ipv6 enable
hostname(vsys-v2)(config-if-vwa2)# ipv6 address 6666::2/64
hostname(vsys-v2)(config-if-vwa2)# exit
hostname(vsys-v2)(config)# interface ethernet0/2
hostname(vsys-v2)(config-if-eth0/2)# zone vsys-v2-trust
hostname(vsys-v2)(config-if-eth0/2)# ipv6 enable
hostname(vsys-v2)(config-if-eth0/2)# ipv6 address 3333::1/64
hostname(vsys-v2)(config-if-eth0/2)# exit
hostname(config)#
Configure route for VSYS-v2
hostname(vsys-v2)(config)# ip vrouter vsys-v2-vr
hostname(vsys-v2)(config-vrouter)# ipv6 route 2222::1/64 6666::1
hostname(vsys-v2)(config-vrouter)# exit
hostname(vsys-v2)(config)# policy-global
hostname(vsys-v2)(config-policy)# default-action permit
hostname(vsys-v2)(config-policy)# exit
hostname(vsys-v2)(config)# exit-vsys
hostname(config)#
```

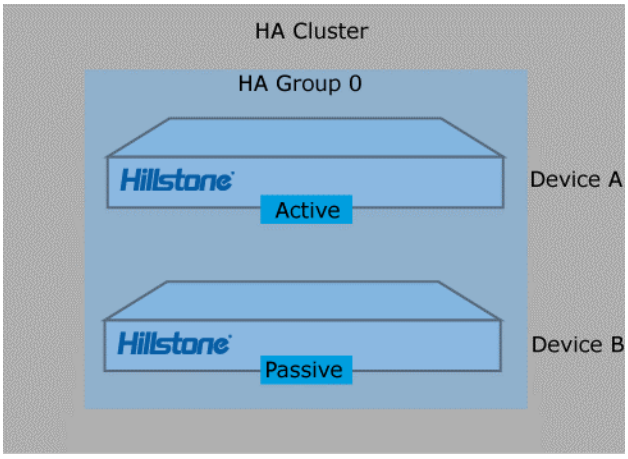
Chapter 6 High Availability (HA)

Overview

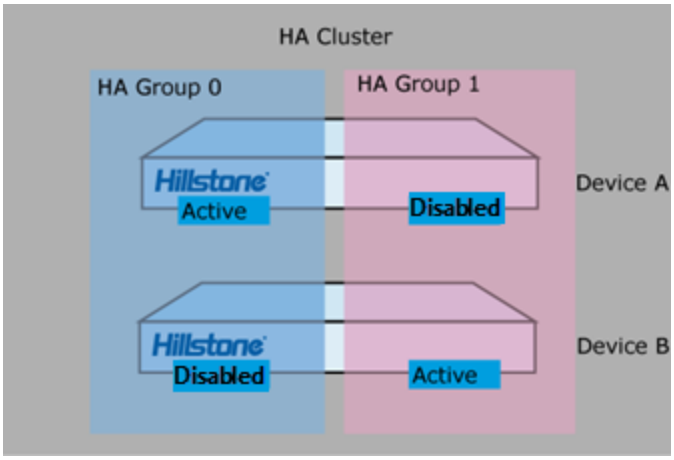
HA (High Availability) provides a failover solution for malfunction of the communication line or devices in order to ensure smooth communication and effectively improve the network reliability. To implement the HA function, you need to group two Hillstone devices as an HA cluster, using the identical hardware platform, firmware version, and licenses. When one device is unavailable or cannot handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

Hillstone devices support two HA modes: Active-Passive (A/P) and Peer Active-Active (A/A) mode.

- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a master device and the other acting as its backup device. The master device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the master device fails, the backup device will be promoted to master and take over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage. The relationship between the devices in A/P mode is shown below:



- Peer Active-Active (A/A) mode: the Peer A/A mode is an HA Active-Active mode. In the Peer A/A mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer A/A mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer A/A mode is more flexible and is suitable for the deployment in the asymmetric routing environment. The relationship between the devices in the Peer A/A mode is shown in the figure below:



HA Cluster

For the external network devices, an HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying an HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the master and backup device of the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The master device is in active state and processes network traffic. When the master device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0. In Peer Active-Active (A/A) mode, the latest Hillstone version supports two HA groups, i.e., Group 0 and Group 1.

HA Node

To distinguish the HA device in an HA group, you can use the value of HA Node to mark the devices. StoneOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, the device whose HA Node value is 0 is at the disabled status and the device whose HA Node value is 0 is active.

HA Group Interface and Virtual MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as Virtual Forward Interface. The master device of each HA group manages a virtual MAC (VMAC) address which corresponds to its interface and the traffic is forwarded on the interface. Different HA groups in an HA cluster cannot forward data among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In an HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the master device.

HA Synchronization

To ensure the backup device can take over the work of the master device when it fails, the master device will synchronize its information with the backup device. System supports two methods to synchronize: real-time synchronization and batch synchronization. When the primary device has just been selected successfully, the batch synchronization will be used to synchronize all information of the primary device to the backup device. When the configurations change, the real-time synchronization will be used to synchronize the changed information to the backup device.

Except for the HA related configurations and local configurations (for example, the host name), all the other configurations will be synchronized.

There are 3 types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- SSL VPN information
- DNS cache mappings
- ARP table
- PKI information
- DHCP information
- MAC table
- WebAuth information



Notes:

- If you configure Local property for an interface , the system will not synchronize this configuration with the backup device. For this reason, it is recommended not to configure the Local property for the business interface.
- For configurations in some functional modules (policy (excluding aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, and ordered address book), if the order of configurations in the secondary device is not the same as that of the primary device, the system adjusts the order of configurations in



the secondary device to be the same as that of the primary device when it performs batch synchronization.

- No configuration changes are allowed on the primary and secondary devices until the batch synchronization is completed.

Limits on Configuring NAT in HA Scenario

When you use the NAT function in HA scenario, take note of the following limits:

- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the same dynamic port (**dynamicport**) SNAT rule, you need to enable the SNAT port distribution function by using the **split-port-pool by ha-node** command. This ensures that ports assigned for the two devices in the HA group are not duplicate.
- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the same dynamic IP (**dynamicip**) SNAT rule, the SNATed IP address may be reused because IP occupation is not synchronized between the devices in the HA group.
- The source or destination address in the NAT rule cannot contain the IP address of the HA link interface (heartbeat interface). This avoids abnormal heartbeat link communication when heartbeat packets are NATed.
- In the Peer Active-Active (A/A) scenario, if both devices in the HA group are configured with the SNAT rule that translates the source IP address to Egress IF IP (**eif-ip** or **eif-ipv6**), the two devices in the HA group may behave inconsistently after an HA switchover because their NATed IP addresses may be different.

Configuring HA

To configure the HA function, take the following steps:

1. Configure an HA group, including specifying the device priority (for selection) and HA packets-related parameters.
2. Configure an HA virtual forward interface.
3. Configure the HA link, including an HA link interface and an HA link IP address, for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the HA cluster ID and HA node ID, and enable the HA function.

WebUI: Select **System > HA** from the menu bar. In the HA dialog, configure the options.

Configuring an HA Group

The HA group need to be configured in the HA group configuration mode. To enter the HA group configuration mode, in the global configuration mode, use the following command:

ha group *group-id*

- *group-id* – Specifies the HA group ID. The value range is 0 to 1.

After executing the command, the system will enter the HA group configuration mode. To delete the specified HA group, in the global configuration mode, use the following command:

no ha group *group-id*

In the HA group configuration mode, you can perform the following configurations:

- Specifying the priority
- Specifying the Hello interval
- Specifying the Hello threshold
- Configuring the preempt mode
- Specifying the gratuitous ARP packet number

- Specifying the description
- Specifying the track object

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device. To specify the priority, in the HA group configuration mode, use the following command:

priority *number*

- *number* – Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the HA group configuration mode, use the following command:

no priority



Tip: When the priorities are identical, the device with smaller value in the 10th to 14th bit of the device S/N will be priorized.

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the HA group configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* – Specifies the interval for sending heartbeats. The value range is 50 to 10000 milliseconds. The default value is 200.

To restore to the default Hello interval, in the HA group configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device's heartbeat fails. To specify the Hello threshold, in the HA group configuration mode, use the following command:

hello threshold *value*

- *value* – Specifies the Hello threshold value. The value range is 3 to 255. The default value is 15.

To restore to the default Hello threshold, in the HA group configuration mode, use the following command:

no hello threshold

Specifying the Hello Packet Transport Protocol

In the HA scenario, when you use the VRRP protocol to transmit HA Hello packets, the restriction of the core switch on both the transmission rate and the packet size of VRRP packets can affect the synchronization between the HA master and the backup device. Therefore, you can configure Hello packets to use the UDP protocol for transmission to prevent the core switch from imposing these restrictions. By default, Hello packets of X series (except X8180) use the VRRP protocol for transmission, and Hello packets of SG-6000-A series/X8180/K series and CloudEdge use the UDP protocol for transmission. To specify that Hello packets use the UDP protocol for transmission, in global configuration mode, use the following command:

ha transmit udp

To restore to the default protocol VRRP, use **no ha transmit udp** command:



Notes:

- When device is added to HA cluster, you can not change the Hello transport protocol. If you want to change it, execute the command**no ha cluster**firstly.



- The master device and the backup device should be configured with the same Hello transport protocol.

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the HA group configuration mode, use the following command:

preempt [*delay-time*]

- *delay-time* – Specifies the delay time. The value range is 1 to 600 seconds. The default value is 30.

To cancel the preempt mode, in the HA group configuration mode, use **no preempt** command.

Specifying the Gratuitous ARP Packet Number

When the backup device is selected as the master device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. This command is used to specify the number of ARP packets the upgraded master device will send. The maximum number of gratuitous ARP packages sent by new master device is determined by the number of sending gratuitous ARP packets specified by this command. The system will send five gratuitous ARP packets immediately after device switching, and sending one ARP packets per second until the number of gratuitous ARP packets reaches the number specified by this command. To specify the gratuitous ARP packet number, in the HA group configuration mode, use the following command:

arp *number*

- *number* – Specify the gratuitous ARP packet number. The value range is 10 to 180. The default value is 15.

To restore to the default gratuitous ARP packet number, in the HA group configuration mode, use **no arp** command.

Sending Gratuitous ARP Packets

When the backup device is promoted to the master device, since the new master device only sent rather limited ARP packets to the network, some servers in the network may be unable to receive any ARP packets and therefore unable to update the ARP table. As a result, these servers may be unable to provide normal service within a short period. To solve the problem, the system supports sending gratuitous ARP packets manually via a specified interface. To send gratuitous ARP packets via the specified interface, in the execution mode, use the following command:

send gratuitous-arp interface *interface-name* [**count** *num* | **interval** *num*]

- **interface** *interface-name* – Specifies the interface on which gratuitous ARP packets are sent. This interface can be a physical interface, VSwitch interface, aggregate interface or redundant interface with an IP address configured.
- **count** *num* – Specifies the count for sending ARP packets. The value range is 0 to 60. The default value is 5. Value 0 indicates sending the packets consistently. You can stop sending by pressing Ctrl+C.
- **interval** *num* – Specifies the interval for sending ARP packets. The value range is 1 to 60 seconds. The default value is 1.

Specifying the Description

To specify description information, in the HA group configuration mode, use the following command:

description *string*

- *string* – Specifies the description information.

To cancel the description information, in the HA group configuration mode, use **no description** command.

Specifying the Track Object

The track object is used to monitor the working status of the device. When the device cannot work normally, the system will take the corresponding action. To specify the track object, in the HA configuration mode, use the following command:

monitor track *track-object-name*

- *track-object-name* – Specifies the name of the track object configured in the system.

To cancel the track object, in the HA configuration mode, use **no monitor track** command.



Notes: It is recommended that the track object in the HA group should be configured with the Local property. For more information about how to configure the track object, see "Configuring a Track Object" of "System Management".

Configuring an HA group interface

To configure the interface for HA Group 0, in the global configuration mode, use the following command:

interface {**ethernet** *m/n* | **redundant** *number* | **aggregate** *number* | **tunnel** *number* | **loopback** *number* | **bgroup** *number* | **ethernet** *m/n.tag* | **redundant** *number.tag* | **aggregate** *number.tag* | **vswitch** *number*}



Tip: For more information about how to create and configure an interface, see "Interface" of "Firewall".

To configure the interface for HA Group 1, in the global configuration mode, use the following command:

interface {**ethernet** *x/y:1* | **redundant** *x:1* | **aggregate** *x:1* | **tunnel** *x:1* | **loopback** *x:1* | **ethernet** *x/y.u:1* | **redundant***x.y:1* | **aggregate***x.y:1* | **vswitchif** *x:1*}

- **ethernet** *x/y:1*: Specifies ethernetx/y as the interface for Group 1 and uses this interface for data forwarding.
- **redundant** *x:1*: Specifies redundantx as the interface for Group 1 and uses this interface for data forwarding.
- **aggregate** *x:1*: Specifies aggregatex as the interface for Group 1 and uses this interface for data forwarding.
- **tunnel** *x:1*: Specifies tunnelx as the interface for Group 1 and uses this interface for data forwarding.
- **loopback** *x:1*: Specifies loopbackx as the interface for Group 1 and uses this interface for data forwarding.
- **ethernet** *x/y.u:1*: Specifies ethernetx/y.u as the interface for Group 1 and uses this interface for data forwarding.
- **redundant***x.y:1*: Specifies redundantx.y as the interface for Group 1 and uses this interface for data forwarding.
- **aggregate** *x.y:1*: Specifies aggregatex.y as the interface for Group 1 and uses this interface for data forwarding.
- **vswitchif** *x:1*: Specifies vswitchifx as the interface for Group 1. In HA peer mode, vswitchifx:1 is used for data forwarding in mix mode of Layer 2 and Layer3, and users can manage the device through this interface in transparent Mode.

To cancel the specified interface, in the global configuration mode, use the following command:

no interface {**ethernet** *x/y:1* | **redundant** *x:1* | **aggregate** *x:1* | **tunnel** *x:1* | **loopback** *x:1* | **ethernet** *x/y.u:1* | **redundant** *x.y:1* | **aggregate***x.y:1* | **vswitchif** *x:1*}

Configuring the Next-hop IP Address of the Interface

In the HA Peer mode network environment, to avoid the situation that fails to find the routes when synchronizing data with the peer device, you can configure the next-hop IP address of the interface, which ensures the successful creation of the sessions. To specify the next-hop IP address of the interface, use the following command in the interface configuration mode:

direct-send default-nexthop { *A.B.C.D* | *X:X:X:X::X*} [**local**]

- *A.B.C.D* | *X:X:X:X::X* – Specifies the next-hop IPv4 or IPv6 address of the interface.
- **local** – If you enter this parameter, the system will not synchronize this configuration with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

In the interface configuration mode, use the following command to cancel the above configurations:

no direct-send default-nexthop { *A.B.C.D* | *X:X:X:X::X*} [**local**]

Configuring SNAT Port Distribution

HA supports the SNAT port distribution function. The function is that when you configure the same SNAT address pools for two HA devices, the system will averagely distribute the SNAT port resources according to the values of HA Node. If you disable this function, the SNAT address pool configured for each HA device must differ and each device will occupy the entire port resources. The SNAT port distribution function can only take effect I the HA Peer mode.

To enable the SNAT port distribution function, use the following command in the global configuration mode:

split-port-pool by ha-node

In the global configuration mode, use the following command to disable this function:

no split-port-pool by ha-node

Configuring a HA Link

The synchronization between the master and backup device and the Hello packets are transmitted over the HA link.

There are two types of HA links, control link and data link. Control link is required and data link is optional. Specifically, for SG-6000-X25812/X25803/X10800/X9180/X8180, both control link and data link are required.

- If only the control link is configured, all data between two devices is transmitted over the control link, including Hello packets and session information, etc.
- If both the control link and data link are configured, the heartbeat messages between two devices is trasmitted over both the control and data links. The synchronization of configuration information between two devices will be done over the control link. And the synchronization of session information between two devices will be done over the data link.

You need to specify the HA link interface first, and then specify the IP address of the interface.



Notes: To configure the HA link interface of SG-6000-X25812/X25803/X10800/X9180/X8180, you need to pay attention to the following:

- You can only synchronize the data information through HA date link interface.
- By default, all HA interfaces (HA0 and HA1) of SCMs will be configured as the the HA control link automatically, and you don't need to configure. To connect the HA control link, take the following methods:
  - Connect the HA0 of master SCM on the master device with the HA0 of the master SCM on the backup device.
  - Connect the HA1 of master SCM on the master device with the HA0 of the backup SCM on the backup device.

- Connect the HA0 of backup SCM on the master device with the HA1 of the master SCM on the backup device.
- Connect the HA1 of backup SCM on the master device with the HA1 of the backup SCM on the backup device.

Specifying an HA Link Interface

You can specify up to two HA control link interfaces. The later configured HA link interface serves as the backup interface for the first configured one. When the first interface disconnects, the later configured interface will take over the task of transmitting HA packets.

For X series devices, the system supports to configure the interface on I/O module as the HA control link interface in order to avoid the abnormal HA heartbeat and synchronization message due to the abnormal link of the interface on the control module. By default, the HA control link interface is on the control module.

To specify an HA control link interface, in the global configuration mode, use the following command:

ha link interface *interface-name*

- *interface-name* – Specifies the name of the interface. You can configure the physical interface or aggregate interface as the interface of the control link. You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.

To specify a HA data link interface, in the global configuration mode, use the following command:

ha link data interface *interface-name*

- *interface-name* – Specifies the name of the interface.
- **data** – Specify the type of the HA link as the data link. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link. You can specify at most one aggregate interface as the HA data link interface, or at most two physical interfaces as the HA data link interface.

To delete the specified HA link interface, in the global configuration mode, use the following command:

no ha link interface *interface-name*

no ha link data interface *interface-name*

Specifying the Work Mode of HA Link Interface

The two physical interfaces of the HA data link interface can work in Active-passive mode or Load-balance mode. To specify the work mode of the HA data link interface, in the global configuration mode, use the following command:

ha data-link mode {**active-passive** | **load-balance**}

- **active-passive** – Specify the work mode of the HA data link interface as Active-passive mode. After specifying this work mode, the first configured HA data link interface works as the master interface, and the later configured HA data link interface serves as the backup interface for the first one. When the first interface fails, the later configured interface will take over the work of the failure interface. When the master interface restores to normal, it will take all the data link work again.
- **load-balance** - Specify the work mode of the HA data link interface as Load-balance mode. The load-balance mode is the default mode. After specifying this work mode, the two HA data link interfaces perform their own tasks simultaneously, and monitor the operation status of each other. When one interface fails, the other will take over the work of the failure inter-

face and also run its own work simultaneously. When the failure interface restores to normal, the two HA data link interfaces perform their own work again.

To restore to the default work mode of the HA data link interface, in the global configuration mode, use the following command:

no ha data-link mode

Specifying the IP Address of HA link

To configure the IP address (IPv4 or IPv6 address) of the HA link, in the global configuration mode, use the following command:

ha link {**ip** *ip-address/Mask* | **ipv6** *ipv6-address/Mask*}

- **ip** *ip-address/Mask* – Specifies the IPv4 address and the netmask of the HA link, both IP/netmask (e.g. 1.1.1.1/24) and IP wildcard netmask (e.g. 1.1.1.1 255.255.255.0) are supported.
- **ipv6** *ipv6-address/Mask* - Specifies the IPv6 address prefix and the prefix length of the HA link. The value range of the prefix length is 1 to 128.

To cancel the specified IP address, in the global configuration mode, use the following command:

no ha link {**ip** *ip-address/Mask* | **ipv6** *ipv6-address/Mask*}

Specifying an HA Assist Link Interface

In the Active-Passive (A/P) mode, you can specify the HA assist link interface to receive and send heartbeat packets (Hello packets), and ensure the main and backup device of HA switches normally when the HA link fails.

To specify an HA assist link interface, in the global configuration mode, use the following command:

ha assist-link interface *interface-name*

- *interface-name* – Specifies the name of the interface. You can configure only one HA assist link interface.

To delete the specified HA assist link interface, in the global configuration mode, use the following command:

no ha assist-link interface *interface-name*



Notes:

- Before the HA link is restored, the HA assist link interface can only receive and send heartbeat packets and the data packets cannot be synchronized. You are advised not to modify the current configurations. After the HA link is restored, execute the command **`exec ha sync rdo session`** to manually synchronize session information.
- The HA assist link interface must use an interface other than the HA link interface and be bound to the zone.
- You need to specify the same interface as the HA assist link interface for the main and backup device, and ensure that the interface of the main and backup device belongs to the same VLAN.

Specifying the MAC Address of HA Link Interface on ClouldEdge

The MAC address of HA link interface refers to the source MAC address for the HA device to send heartbeats (Hello packets) to other devices in HA group. By default, system uses the default MAC address to send Hello packets. Users can specify the MAC address of control link interface or customize a MAC address as the MAC address of HA link interface. To specify the MAC address of HA link interface, in the global configuration mode, use the following command:

ha link mac { **1st-interface-mac** | *mac-address*}

- **1st-interface-mac** – Specifies the MAC address of control link interface as the MAC address of HA link interface. When there is more than one configured control link interfaces, system will use the MAC address of the first control link interface as the MAC address of HA link interface.
- *mac-address* – Specifies a customized MAC address as the MAC address of HA link interface.

In the global configuration mode, use the following command to restore the default MAC address of HA link interface.

no ha link mac

Enable the Real MAC Address of Interface On CloudEdge

This function is only supports for the interface of CloudEdge, except HA link interface and the interface configured with the Local property. By default, the interface forwards traffic with the virtual MAC address provided by system. After configuring the function, each interface will use its real MAC address for communication. To enable the real MAC address of interface, in the global configuration mode, use the following command:

no ha virtual-mac enable

To restore to the default virtual MAC address, in the global configuration mode, use t**ha virtual-mac enable** command.



Notes:

- When device is added to HA cluster and HA function take effective, you can not change the MAC address of interface.If you want to change it, execute the command **no ha cluster** firstly.
- If a custom HA MAC address is configured for an interface, the interface forwards traffic based on the custom HA MAC address, and other interfaces forward traffic based on this function.

Configuring a Custom HA MAC Address

By default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device.



Notes:

- To ensure that the custom HA MAC takes effect, you need to enable the HA function.
- The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.

To configure a custom HA MAC address, in interface configuration mode, use the following command:

ha-vmac*mac-address*

- *mac-address* - Specifies the custom HA MAC address.

To delete the custom HA MAC address, in interface configuration mode, use the following command:

no ha-vmac

Configuring HA Negotiation through Two Layer Unicast Mode

System supports HA negotiation through two-layer unicast mode. You can configure the HA peer IP address or configure the peer IP and MAC address concurrently in each device. After that, this two device will negotiate through two-layer unicast mode.

To configure HA peer IP address (IPv4 or IPv6 address) or mac address, in the global configuration mode, use the following command:

ha peer {**ip** *ip-address* | **ipv6** *ipv6-address*} [**mac** *mac-address*]

- **ip** *ip-address* - Specifies the IPv4 address of HA link interface of peer device.
- **ipv6** *ipv6-address* - Specifies the IPv6 address of HA link interface of peer device.
- **mac** *mac-address* - Specifies the MAC address of HA link interface of peer device.

In the global configuration mode, use **no ha** {**ip** | **ipv6**} to restore the default configuration.



Notes: When device is added to HA cluster and HA function take effective, you can not modify the HA peer ip or mac address .If you want to modify it, execute the command **no ha cluster** firstly.

Specifying the MTU Value of HA link Interface

After specifying the HA link interface, you can continue to specify the MTU value of HA link interface as required. After it is specified, the sender will send the message separately and the receiver will reorganize the message after receiving it when the size of the message exceeds the MTU value of the HA link interface. To configure the MTU value of the HA link interface, in the global configuration mode, use the following command:

ha link mtu *value*

- *value* – Specifies the MTU value of the HA link interface. The default value is 1500.

To cancel the specified MTU value, in the global configuration mode, use the following command: **no ha link mtu**.

Configuring a HA Cluster

After configuring the HA group, HA group interface and HA link interface, you need to add the device to the HA cluster to make the HA function take effective. If there are more than one pair of HA devices in the network, you need to configure different HA cluster IDs, otherwise the MAC addresses may conflict. To configure an HA cluster, in the global configuration mode, use the following command:

ha cluster *cluster-id* [[**peer-mode node** *ID* [**symmetric-routing**]] | **node** *ID*]

- *cluster-id* – Specifies the HA cluster ID. The value varies depending on the HA virtual MAC prefix.
- **peer-mode node** *ID* – Configures the HA Peer mode and specifies the role of this device in the HA cluster. The range is 0 to 1. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is will be in the disabled status.
- **symmetric-routing** - If you enter this parameter, the device will work in the symmetrical routing environment. Note: The symmetrical routing configuration and **ha traffic enable** are mutually exclusive.
- **node** *ID* - Specifies the HA Node value for the device. The values for two devices must be different. The range is 0 to 1. You need to specify the HA node value except for CloudEdge If you do not specify this value for CloudEdge, the devices will obtain the Node ID value by automatic negotiation.

To disable the specified HA cluster, in the global configuration mode, use **no ha cluster** command.

Configuring HA VMAC Prefix

This feature is only supported for CloudEdge. If more than 8 HA clusters in a network segment need to be configured, you can configure the prefix of the HA virtual base MAC address, i.e., the HA virtual MAC prefix, in order to avoid the HA virtual MAC address duplication. When the length of prefix is set to 7 hexadecimal, you can deploy up to 128 HA clusters on the same network segment. When the length of prefix is set to 8 or by default, you can deploy up to 8 HA clusters on the same network segment. After the configuration is complete, the system will prompt the HA virtual MAC range to be generated and the configuration will take effect after reboot. To configure the HA virtual MAC prefix, in the global configuration mode, use the following command:

ha virtual-mac-prefix *prefix-addr*

- *prefix-addr* – Specifies the prefix of the HA base MAC in hexadecimal format. Its length can only be configured as seven or eight. By default, the HA virtual MAC prefix is 0x001C54FF. It should be noted that 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid.

To restore to the default prefix, in the global configuration mode, use **no ha virtual-mac-prefix** command.



Tip: With the HA function enabled, if you want to modify the HA virtual MAC prefix, you may need to disable the HA function first.

Viewing HA VMAC Prefix

To view the current HA virtual MAC prefix and the maximum number of HA clusters that can be configured, use the following command in any mode:

show ha cluster

Configuring HA Base Virtual MAC

To ensure unique HA virtual MAC address and simplify future maintenance, you can assign specific HA virtual MAC addresses by configuring the HA base virtual MAC. This feature is supported only in HA A/P mode and needs to be configured before the HA function is enabled. No device reboot is required for the configuration to take effect.

To configure the HA base virtual MAC, in the global configuration mode, use the following command:

ha base-virtual-mac*mac-address*

- *mac-address* – Specifies he HA base virtual MAC address. Note that 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid. It is recommended that you use the system recommended HA

base virtual MAC address. You can press the Tab key after entering the **ha base-virtual-mac** parameter to view the system recommended HA base virtual MAC address.

To delete the configured HA base virtual MAC address, in the global configuration mode, use **no ha base-virtual-mac** command.



Notes:

- HA virtual prefix and HA base virtual MAC functions are mutually exclusive and the two cannot be configured at the same time.
- With the HA function enabled, if you want to modify the HA base virtual MAC, you may need to disable the HA function first.

Viewing HA Base Virtual MAC

To view the HA base virtual MAC address and the system-recommended HA base virtual MAC address, use the following command in any mode:

show ha base-virtual-mac

Below is a return example:

```
hostname# show ha base-virtual-mac
HA base virtual MAC: 1a1c.5478.3a01
System recommend HA base virtual MAC: 1a1c.5478.3a01
```

Configuring a Management IP

To manage the HA backup device, you need to configure a management IP for the backup device. To configure a management IP address, in the interface configuration mode, use the following command:

manage ip *ip-address*

- *ip-address* - Specifies the management IP address.

Configuring Local Property



Notes: Do not configure the Local attribute on the business interface (interface carrying business traffic). Once configured, the interface will no longer participate in HA information synchronization. All configuration details, session information, and ARP entries associated with this interface will not be synchronized to the backup device, potentially leading to traffic disruption or abnormal network behavior, which could impact business operations. In addition, note that sub-interfaces and Virtual Forward interfaces automatically inherit the Local attribute of their parent interface. For example, if a physical interface is configured with the Local attribute, its sub-interfaces will also inherit this attribute. Therefore, special attention needs to be paid to the Local attribute of the parent interface during configuration.

Sytem supports to configure an editable Local property for all interfaces (except VSwitch) to avoid the duplicate MAC address when managing huge amount of HA devices in the same Layer 2 Network. The sub-interface and virtual forward interface don’ t need to configure Local property, which inherit the primary interface directly. If you configure Local property for an interface , the system will not synchronize this configuration with the backup device. In the interface configuration mode, use the following command:

local

To delete HA Local property, in interface configuration mode, use command **no local**.

Configuring the Layer 3 Port Down-up Function

The Layer 3 port down-up function is enabled by default. When this function is disabled, the following types of physical interfaces do not perform down-up operations when the device is switched from a master device to a backup device for HA switching:

- The physical interface that is bound to a Layer 3 zone.
- The physical interface that belongs to a redundant interface, and the redundant interface is bound to a Layer 3 zone.
- The physical interface that belongs to an aggregate interface, and the aggregate interface is bound to a Layer 3 zone.

To enable or disable the Layer 3 port down-up function, in the global configuration mode, use the following command:

ha l3-port-force-down-up {**enable** | **disable**}

- **enable** - Enable the Layer 3 port down-up function.
- **disable** - Disable the Layer 3 port down-up function.

Manually Synchronizing HA Information

As described in HA synchronization, the system uses batch synchronization to synchronize all the master device information to the backup device when the HA master device election is successful. However, in some cases, the master and backup configuration information may not be synchronized. For example, the configuration order in the backup device is not consistent with that of the master device, there are configurations in the backup device that are not included in the master device, or the configuration of the backup device reaches the capacity limit, resulting in the loss of the configurations that have been synchronized from the master device. In this case, you need to manually perform batch synchronization to synchronize the configuration information of the master and backup devices. When manually synchronizing the configuration, you can further configure the full synchronization function. This function can delete the configuration information of the backup device that is more than that of the master device while batch synchronizing the configuration of the master device, and adjust the configuration order of the backup device to ensure that the configuration information and configuration order of the master and backup devices are consistent.

In some exceptional circumstances, the master and backup configurations may not be synchronized. In such a case you need to manually synchronize the configuration information of the master and backup device. To determine if you need to manually synchronize the HA information, take the following steps:

1. View the relevant configuration information of both master and backup device by using the command **show**.
2. According to the displayed configuration information, determine whether you need to manually synchronize the HA information:

- If the configuration information is consistent, then you don’ t need to synchronize manually;
- If the configuration information is inconsistent, you need to run the corresponding commands to manually synchronize the configuration (for more information about the relevant commands, see table below).



Notes:

- You do not need to manually synchronize the inconsistent local configuration information, such as the interface timeout information.
- For dynamic information, such as session information, you do not need to synchronize the information manually unless the dynamic information is not synchronized properly.
- For some functional modules (policy (without aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, ISP routing, static routing, interface, address book, and service book), the redundant configurations in the backup device can be deleted only if they belong to one of the above functional modules.

Commands to synchronize HA information manually are shown as belows:

HA synchronization information	show command	Manual synchronization command	clear synchronization times command
All static configuration and dynamic data	show ha sync state all	exec ha sync all	-
Configuration information	show configuration	exec ha sync configuration	clear ha sync config

HA synchronization information	show command	Manual synchronization command	clear synchronization times command
File information	**show file**	**exec ha sync file** *filename*	-
ARP table	**show arp**	**exec ha sync rdo arp**	-
DNS configuration information	**show ip hosts**	**exec ha sync rdo dns**	**clear ha sync dns**
DNS rewrite rule information	**show dns-rewrite-rule**	**exec ha sync rdo dns-rewrite**	-
DHCP configuration information	**show dhcp**	**exec ha sync rdo dhcp**	**clear ha sync dhcp**
MAC address table	**show mac**	**exec ha sync rdo mac**	-
PKI configuration information	**show pki key**	**exec ha sync rdo pki**	**clear ha sync pki**
	show pki trust-domain		
MAC address table	**show session**	**exec ha sync rdo session**	-
IPSec VPN information	**show ipsec sa**	**exec ha sync rdo vpn**	**clear ha sync vpn**
	show isakmp sa		
IPSec VPN information	**show scvpn client test**	**exec ha sync rdo scvpn**	**clear ha sync scvpn**
	show scvpn		
	show scvpn host-check-profile		

HA synchronization information	show command	Manual synchronization command	clear synchronization times command
	show scvpn pool		
	show scvpn user-host-binding		
	show scvpn session		
	show auth-user scvpn		
L2TP information	show l2tp tunnel	exec ha sync rdo l2tp	-
	show l2tp pool		
	show l2tp client {tunnel-name *name* [user *username*] | tunnel-id *ID*}		
	show auth-user l2tp [interface *interface-name* | vrouter *vrouter-name* | slot *slot-no*]		
WebAuth information	show auth-user webauth	exec ha sync rdo webauth	-
NTP information	show ntp	exec ha sync rdo ntp	clear ha sync ntp

HA synchronization information	show command	Manual synchronization command	clear synchronization times command
Route information	show ip route	exec ha sync rdo route	clear ha sync route
Multicast routing information	show ha sync statistic mroute	exec ha sync rdo mroute	clear ha sync mroute
	show ha sync state mroute		

HA Full Synchronization

In HA scenarios, after the system performs batch synchronization, if there is still a difference in the configuration information between the master and backup devices, there is configuration information in the backup device that is not included in the master device. In this case, you can use the full synchronization function to delete the configuration information in the backup device that is more than that in the master device, adjust the configuration order of the backup device, and then ensure that the configuration information and configuration order of the master and backup devices are consistent. By default, this function is disabled.

To configure HA full synchronization, in execution mode, use the following command:

exec ha sync configuration full-sync

Notes:

- You can run this command only on the master device of HA.
- For configurations in some functional modules (policy (excluding aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, and ordered address book), if the order of configurations in the backup device is not the same as that of the master device, the system adjusts the order of configurations in

the backup device to be the same as that of the master device when it performs batch synchronization.

- For some functional modules (policy (without aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, ISP routing, static routing, interface, address book, and service book), the redundant configurations in the backup device can be deleted only if they belong to one of the above functional modules.
- When deleting a configuration that the backup device has more than the master device, if the configuration has been referenced by other function modules, it cannot be deleted and needs to be un-referenced before it can be deleted.

Enabling/Disabling Automatic HA Session Synchronization

By default the system will synchronize sessions between HA devices automatically. Session synchronization will generate some traffic, and will possibly impact device performance when the device is overloaded. You can enable or disable automatic HA session synchronization according to the device workload to assure stability.

To enable or disable automatic HA session synchronization, in the global configuration mode, use the following command:

- Enable: **ha sync rdo session**
- Disable: **no ha sync rdo session**

Enabling/Disabling Scheduled Comparison of HA Configurations

After the scheduled comparison of HA configurations is enabled, system will check the HA configurations every 1 hour and record logs if the configuration is found changed. By default, the scheduled comparison of HA configurations is disabled.

To enable or disable the scheduled comparison of HA configurations, in global configuration mode, use the following command:

- Enable: **ha configuration-consistency-check enable**
- Disable: **no ha configuration-consistency-check enable**

Manually Switching Main and Backup Device Status of HA

To switch main and backup device status of HA manually, in any mode, use the following command:

exec ha master switch-over



Notes:

- This command is only supported on the main device of HA.
- This command is only supported in Active-Passive (A/P) mode.
- As the switching operation executes, this device is executing batch synchronization or some Hillstone devices (SG-6000-K9180, SG-6000-X25812, SG-6000-X25803, SG-6000-X10800, SG-6000-X9180 and SG-6000-X8180) are executing batch synchronization of SCM, which will result in failed switching of HA main and backup device status.

Configure the Deployment Mode of HA on Cloudplatform

For virtual firewall CloudEdge, When it is deployed with HA scenario on cloud platform , there are two ways:

- Via HAVIP, you can configure the high availability virtual IP address (HAVIP) on the cloud platform to deploy the HA scenario.
- Via Accesskey , you can configure the access key and secondary IP addresson the cloud platform to deploy the HA scenario.

To enable the "HAVIP " way of CloudEdge's HA deployment, in the global configuration mode , use the following command:

ha cloud-deploy havip enable

To disable the "AccessKey/AppID" way of CloudEdge's HA deployment, in the global configuration mode , use the following command:

ha cloud-deploy havip disable

Specifying the Cloud platform of HA deploying

For CloudEdge , When "AccessKey/AppID" way is configured , you need continue to specify the cloud platform that CloudEdge is deployed， in the global configuration mode , use the following command:

ha cloud-deploy platform { **tencent** | **aliyun** |**aws**}

In the global configuration mode , use the command **no ha cloud-deploy platform** to delete the cloud platform .

Viewing the HA Cloud Deployment Information

For CloudEdge , to view the HA cloud deployment information in any mode, use the following command: :

show ha cloud-deploy

Specifying the AccessKey of Cloud Platform

For CloudEdge , When "AccessKey/AppID" way is configured , you need continue to specify the AccessKey of cloud platform that CloudEdge is deployed， in the global configuration mode , use the following command:

cloud-deploy accesskeyid *key-id* **accesskeysecret** *password*

- *key-id* - Enter the AccessKey or APP ID applied for on the cloud platform.
- *password* - Enter the key password applied for on the cloud platform.

In the global configuration mode , use the command **no cloud-deploy accesskeyid** to delete the configuration of AccessKey.

Checking the Connectivity to Cloud Platform API

For virtual firewall CloudEdge, after configuring the access key and password corresponding to the cloud platform, you can manually check the connectivity with the cloud platform API. In any mode, use the following command:

exec cloud-deploy check cloud-connection

Verifying the Access ID and Password of the Cloud platform

For virtual firewall CloudEdge, after configuring the access key and password corresponding to the cloud platform,you can manually verify whether the access ID and password are correct. In any mode, use the following command:

exec cloud-deploy check accesskey

Viewing the AccessKey of Cloud Platform

For CloudEdge , to view the AccessKey information of Cloud Platform , in any mode, use the following command: :

show cloud-deploy accesskey

Enabling/Disabling Platform Checking of HA devices

For Hillstone CloudEdge virtual firewall, when it is deployed as HA, system will check the platform consistency of HA master and backup device by default. You can disable the checking function in an HA environment for platform upgrade(e.g., VM01 upgraded to VM02). During the upgrade process, the HA device will remain in a negotiated successful state and the user business will not be interrupted. After the upgrade is completed, please enable the chencking again.

To disable the platform checking, in the global configuration mode , use the following command:

ha platform-check disable

To enable the platform checking, in the global configuration mode , use the following command:

ha platform-check enable

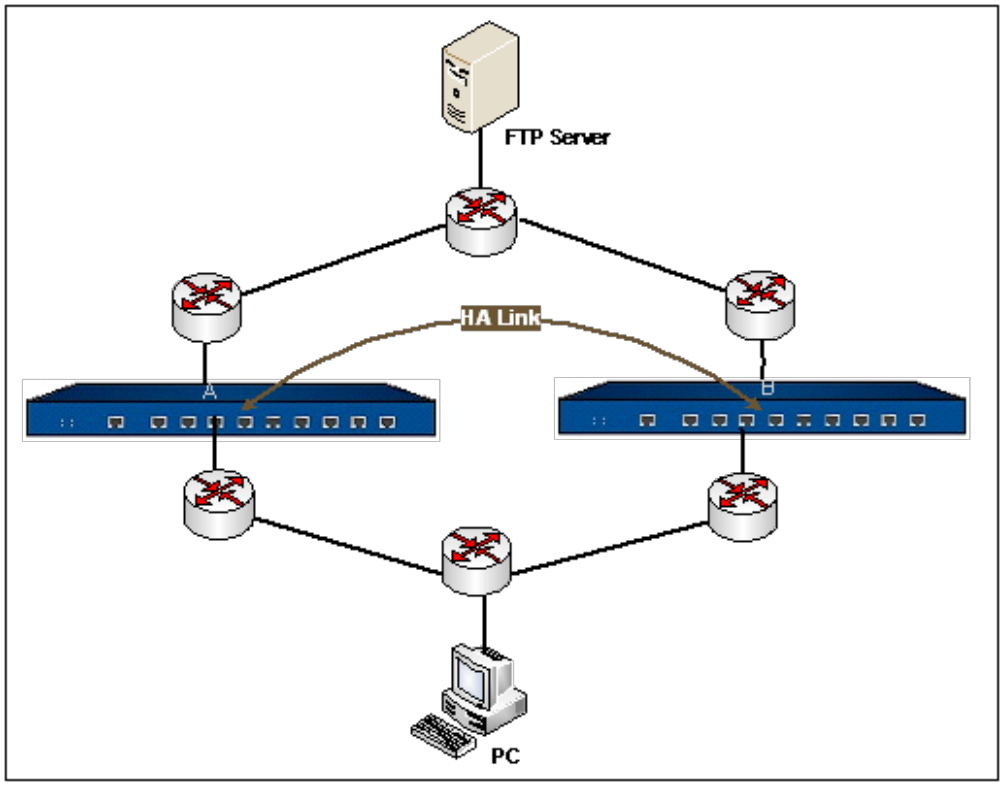
Viewing the Status of HA Platform checking

To view the status of platform checking, in any mode, use the following command:

show ha platform-check status

Configuring HA Traffic

For the HA devices that are deployed in asymmetric routing environment (i.e., inbound and outbound traffic may take different routes), you can enable HA traffic to assure the inbound and outbound packets of a session are processed on the same device, thus avoiding session failure. Figure below illustrates a typical HA traffic application topology.



As shown in the figure above, the left route is from PC to the FTP server by the way of Device A. the righ route is the same start and ending by the way of Device B. the metric value of these two routes are different from each other, making the network an asymmetric route,In addition, the FTP requests from PC are sent to the FTP server via Device A. In order to assure the response packets from the FTP server are returned to PC via Device A, you need to enable HA traffic on both Device A and Device B.

To enable HA traffic, use the following two steps:

1. Configure the two HA device to HA Peer mode;
2. Enable HA traffic.

Enabling HA Traffic

HA traffic is disabled by default. To enable or disable the function, in the global configuration mode, use the following commands:

- To enable: **ha traffic enable**
- To disable: no **ha traffic enable**



Notes:

- After enabling the HA traffic function, the traffic between devices increase. Hillstone recommends you first configure the interface of the data link.
- The symmetrical routing configuration and **ha traffic enable** are mutually exclusive.

Configuring HA Traffic Delay

When processing outbound packets, the device with HA traffic enabled will synchronize packet-related information with the pairing device. If the peer device responses (i.e., inbound packet) before the synchronization is completed, the sessions will not be matched and the response to the request packet will be dropped. To solve this problem, in the transparent mode, you can configure HA traffic delay. The device will wait for the specified delay time so that the synchronization will be completed, and then process inbound packets.

To configure HA traffic delay, in the global configuration mode, use the following commands:

ha traffic delay *num*

- *num* - Specifies the delay time. The value range is 1 to 50 ms. The default value is 3.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic delay

Configuring First Packet Forwarding

In the routing mode, you can configure the first packet forwarding function to ensure that when processing outbound packets, the device will synchronize packet-related information with the pairing device. To configure the first packet forwarding function, use the following command in the global configuration mode:

ha traffic first-packet [**max-size** *num*]

- **max-size** *num* – Specifies the size of the first packet. The unit is byte. The value is 64 to 1024. Without configuring this parameter, the default value is 124.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic first-packet

Configuring First Packet Forwarding Bounce Back

In the routing mode/transparent mode, you can configure the first packet forwarding bounce back function to ensure that when processing outbound packets, the device will synchronize packet-related information with the peer device.

- In the routing mode, the local device synchronizes the outbound packets and packet-related information to the peer HA device. After the peer device completes the session creation, it will return the outbound packets to the local device. After that, the local device performs the next step of forwarding processing.
- In the transparent mode, the local device sends the session synchronization information to the peer HA device, and then continues to send outbound packets. When the peer device completes the session creation, it will return the outbound packets to the local device, and then the local device will perform the next step of forwarding processing.

To configure the first packet forwarding bounce back function, use the following command in the global configuration mode:

ha traffic first-packet-bounce-back [**max-size** *num*]

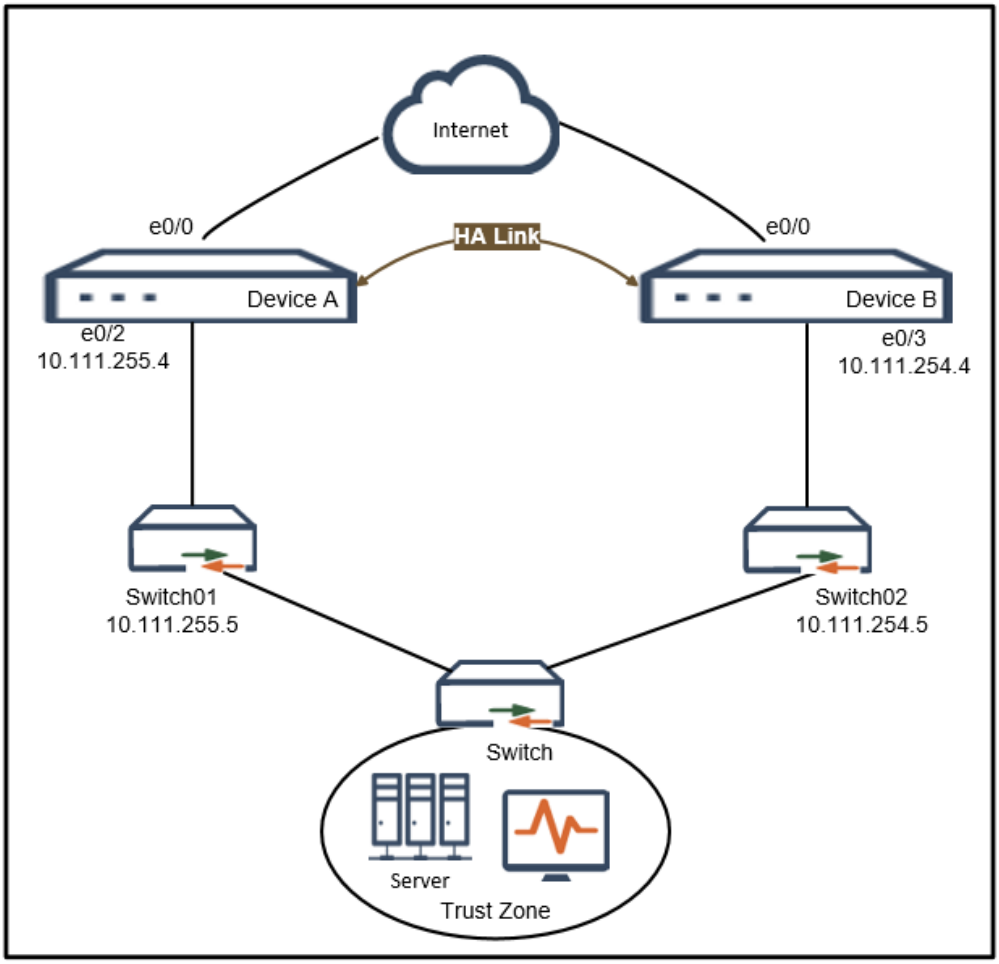
- **max-size** *num* – Specifies the size of the first packet. The unit is byte. The value is 64 to 1024. Without configuring this parameter, the default value is 124.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic first-packet-bounce-back

Configuring HA Route Rematch by Session

In the HA Active-Passive (A/P) mode, you can enable the HA route rematch by session function if the master device and backup device are interconnected with other devices(such as switches) using different interfaces and IP addresses which are not in the same network segment. With this function enabled, the backup device will match the route again for the session synchronized from the master device and find a new egress interface for the route, thus avoiding session failure after HA switchover. Figure below illustrates a typical HA route rematch by session application topology.



As shown in the figure above, Device A and Device B work in HA A/P mode, with Device A as the master and Device B as the backup device:

- Device A connects to Switch01 through interface eth0/2. Interface eth0/3 is not connected. A static route with the destination IP of eth0/2 is configured.
- Device B connects to Switch01 through interface eth0/3. Interface eth0/2 is not connected. A static route with the destination IP of eth0/3 is configured.

When HA switches, Device B becomes the primary device, but the next hop of the route synchronized from Device A is still the IP address of Switch01, causing the session failure. When the HA route rematch by session function is enabled on Device B, Device B will match the route and find the egress interface again for sessions synchronized from Device A, thus avoiding the session failure.

Notes:

- In the above typical scenario, you need to disable the eth0/3 of Device A and the eth0/2 of Device B by using the command **shutdown**.
- The HA session rematch route function supports for Destination Routing, Destination-Interface-Based Routing (DIBR), Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), and Policy-Based Routing (PBR).

The HA session rematch route function is disabled by default. To enable the function, in the global configuration mode, use the following command:

ha session-rematch-route

To disable the HA session rematch route function, in the global configuration mode, use the command **no ha session-rematch-route**.

Viewing HA Configuration

To view the HA configuration information, use the following commands:

- Show the HA cluster configuration information: **show ha cluster**
- Show the HA group configuration information: **show ha group** {**config** | *group-id*}
- Show the HA link status: **show ha link status**
- Show the HA synchronization state: **show ha sync state** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **flow** | **scvpn** | **route** | **mroute** }
- Show the HA traffic status: **show ha traffic**
- Show the HA synchronization statistics: **show ha sync statistic** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **scvpn** | **route**| **mroute** }
- Show the HA protocol statistics: **show ha protocol statiscitc**

- Show the synchronized or unsynchronized HA session information: **show session** {**sync** | **unsync**}
- Show the HA statistics: **show ha flow** [[**slot** *slot-number*] | [**cpu** *cpu-number*]]**statistics**
- Show key information of the HA switchover: **show ha state change info** [**all**]
    - **all** - Show key information for HA switchover of last three times, including HA state change time, HA state change event, HA state change reason, CPU information, memory information, session information and HA interface rate. If this parameter is not specified, the system will show key information for the latest HA switchover.
- Show current status (enable or disable) of the HA route rematch by session function: **show ha session-rematch-route**

Enabling HAVIP function that Alibaba Cloud provides to deploy HA

Only the CloudEdge deployed on Alibaba Cloud supports this function. With this function enabled, vADC will use the HAVIP function that Alibaba Cloud provides to deploy HA. If you use the secondary IP of the interface for HA deployment or do not want to deploy HA, you need to disable this function. To enble/disable HAVIP, in the global configuration mode, use the following command:

- Enable: **ha aliyun-deploy havip enable**
- Disable: **ha aliyun-deploy havip disable**

Configuring the Accesskey of Alibaba Cloud

Only the CloudEdge deployed on Alibaba Cloud supports this function. Specify the AccessKey ID and password of your Alibaba Cloud account.

aliyun accesskeyid *id* **accesskeysecret** *value*

HSVRP

The system supports the Hillstone Virtual Redundant Protocol (HSVRP) function. In peer active-active (A/A) scenarios, if a device fails, traffic that originally flows into the interface of this device will be redirected to another healthy device. This ensures that network communication is not interrupted.

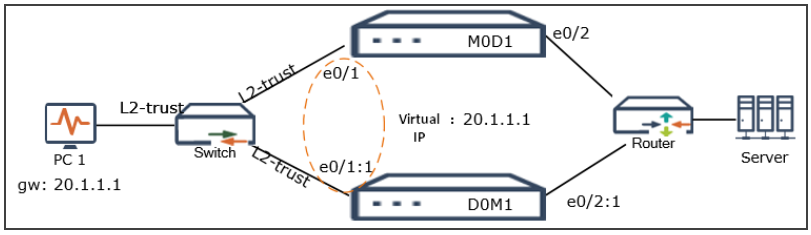
The HSVRP function provides the HSVRP group, which consists of a group of interfaces on two HA devices. The virtual IP address of the HSVRP group takes effect on the primary interface first. In other words, traffic that accesses the virtual IP address flows into the primary interface of the HSVRP group. If the device where the primary interface belongs fails, traffic will be redirected to the secondary interface on another device. This avoid network communication interruptions.

Typical Scenario

HSVRP is usually deployed in HA peer mode. In the following scenario, HA group 0 of the M0D1 device is at the active status and HA group 1 of the D0M1 device is at the disabled status. HA group 1 of the D0M1 device is at the active status and HA group 0 of the D0M1 device is at the disabled status. The eth0/1 and eth0/1:1 interfaces are service forwarding interfaces of HA group 0 and group 1 respectively. After the HSVRP function is configured, the virtual IP address of the HSVRP group takes effect on eth0/1 first. If M0D1 fails, the virtual IP address takes effect on eth0/1:1 and redirects traffic that accesses eth0/1 to eth0/1:1. This ensures that the business of HA group 0 is not affected.

In the following scenario, an HSVRP group is configured and the virtual IP address of the HSVRP group is 20.1.1.1. The virtual IP address is referenced by the eth0/1 and eth0/1:1 interfaces and takes effect on eth0/1 first. The gateway of a PC over the internal network is destined for the virtual IP address (20.1.1.1). When the PC accesses the server:

- If M0D1 and D0M1 are running as normal, the virtual IP address (20.1.1.1) takes effect on eth0/1 and access traffic is redirected by M0D1.
- If M0D1 fails, the virtual IP address (20.1.1.1) takes effect on eth0/1:1 and D0M1 takes over M0D1 to redirect access traffic.



Basic Concepts

HSVRP Group

HSVRP group is a virtual entity that has a virtual IP address and a virtual MAC address. In HA scenarios, after an HSVRP group is configured, the group does not take effect until referenced by a group of interfaces on HA devices.

Referencing an HSVRP Group by an Interface

After an interface references an HSVRP group, the virtual IP address of the HSVRP group takes effect. One interface can reference up to two HSVRP groups. If an interface references two HSVRP groups, the interface needs to be used as the primary interface of an HSVRP group and the secondary interface of another HSVRP group.

If the interface is used as the primary interface of an HSVRP group, the virtual IP address of the HSVRP group takes effect on the interface first. If the interface is used as the secondary interface of an HSVRP group, the virtual IP address of the HSVRP group takes effect on the interface only when the device where the primary interface of the HSVRP group belongs fails.

For example, in peer A/A scenarios, M0D1 uses eth0/1 as the service forwarding interface and D0M1 uses eth0/1:1 as the service forwarding interface. Two HSVRP groups hsvrp 1 and hsvrp 2 configured with a virtual IP address are created.

- **Example 1**: The eth0/1 and eth0/1:1 interfaces reference only hsvrp 1. The eth0/1 interface is used as the primary interface of hsvrp 1 and the eth0/1:1 interface is used as the secondary interface of hsvrp 1.

  In this case, the virtual IP address of hsvrp 1 takes effect on eth0/1, which receives traffic

that accesses the virtual IP address. The eth0/1:1 interface is in the backup state. The virtual IP address of hsvrp 1 takes effect on eth0/1:1 and eth0/1:1 starts taking over traffic of eth0/1 only when M0D1 fails.

- **Example 2**: The eth0/1 and eth0/1:1 interfaces reference both hsvrp 1 and hsvrp 2. The eth0/1 interface is used as the primary interface of hsvrp 1 and the secondary interface of hsvrp 2. The eth0/1:1 interface is used as the secondary interface of hsvrp 1 and the primary interface of hsvrp 2.

  In this case, the virtual IP address of hsvrp 1 takes effect on eth0/1 and the virtual IP address of hsvrp 2 takes effect on eth0/1:1. That is, eth0/1 receives traffic that accesses the virtual IP address of hsvrp 1 and eth0/1:1 receives traffic that accesses the virtual IP address of hsvrp 2 within the same period. The eth0/1 and eth0/1:1 interfaces serve as a backup for each other.

  - If M0D1 fails, eth0/1:1 takes over traffic of eth0/1. Traffic that accesses the virtual IP address of both hsvrp 1 and hsvrp 2 reaches eth0/1:1.
  - If D0M1 fails, eth0/1 takes over traffic of eth0/1:1. Traffic that accesses the virtual IP address of both hsvrp 1 and hsvrp 2 reaches eth0/1.

HSVRP Group Status

The system determines the interface on which the virtual IP address of an HSVRP group takes effect based on the status of the HSVRP group. This interface processes traffic that accesses the virtual IP address. Only one interface takes effect at a time. If the device where this interface belongs fails, the interface on another device takes over traffic of the faulty device to ensure business continuity in the network.

An HSVRP group can be in the active or inactive state. If the status of the HSVRP group on the interface is active, it indicates that the HSVRP group takes effect on this interface, which processes traffic that accesses the virtual IP address. If the status of the HSVRP group on the interface is inactive, it indicates that the HSVRP group does not take effect on this interface and another interface processes traffic that accesses the virtual IP address. If the status of the HSVRP

group on an interface is active, the status of the same HSVRP group on another interface is inactive at the same time.

The status of an HSVRP group on an interface is determined by whether the interface is the primary interface of the HSVRP group and whether the device where the interface belongs runs as normal:

- If the device where the primary interface belongs runs as normal, the status of the HSVRP group on the primary interface is active. Otherwise, the status of the HSVRP group on the secondary interface is active.
- If the device where the primary interface belongs recovers from a failure, the status of the HSVRP group on the primary interface changes from inactive to active.

When the status of the HSVRP group on the interface changes from inactive to active, the interface uses the virtual IP address and virtual MAC address of the HSVRP group to send gratuitous ARP packets, redirects traffic that accesses the virtual IP address to itself, and then forwards the traffic.

Configuring HSVRP

- Creating an HSVRP Group
- Configuring the Virtual IP Address of an HSVRP Group
- Viewing an HSVRP Group
- Referencing an HSVRP Group by an Interface

Creating an HSVRP Group

You can create up to 255 HSVRP groups. To create an HSVRP group, use the following command in global configuration mode:

hsvrp id *id*

- *id* - Specifies the ID of the HSVRP group. Valid values: 1 to 255. For example, **hsvrp id 1** and **hsvrp id 2** indicates different HSVRP groups. After the command is executed, you will enter the configuration mode of the HSVRP group.

In global configuration mode, use the **no hsvrp id** *id* command to delete a specified HSVRP group.



Notes: Before you delete an HSVRP group, you need to cancel the reference to the HSVRP group by interfaces.

Configuring the Virtual IP Address of an HSVRP Group

The IP address of an HSVRP group and the IP address of the interface to which the HSVRP group is bound can belong to the same network segment or different network segments. To configure the virtual IP address of an HSVRP group, use the following command in HSVRP group configuration mode:

ip address {*A.B.C.D* | *A.B.C.D/M*}

- *A.B.C.D* | *A.B.C.D/M* - Specifies the IP address of the HSVRP group.
    - If you specify the IP address in the *A.B.C.D* format, the subnet mask is 255.255.255.255. In this case, the specified IP address and the IP address of the interface to which the HSVRP group is bound needs to belong the same network segment.
    - If you specify the IP address in the *A.B.C.D/M* format, the specified IP address and the IP address of the interface to which the HSVRP group is bound needs to belong different network segments.

In HSVRP group configuration mode, use the **no ip address** [*A.B.C.D* | *A.B.C.D/M*] command to cancel the configuration.

ipv6 address {*X:X:X:X::X* | *X:X:X:X::X/M*}

- *X:X:X:X::X* | *X:X:X:X::X/M* - Specifies the IPv6 address of the HSVRP group.
    - If you specify the IPv6 address in the *X:X:X:X::X* or *X:X:X:X::X/128* format, the specified IPv6 address and the IPv6 address of the interface to which the HSVRP group is bound need to belong the same network segment.
    - If you specify the IPv6 address in the *X:X:X:X::X/M* (M is not equal to 128) format, the specified IPv6 address and the IPv6 address of the interface to which the HSVRP group is bound need to belong different network segments.

In HSVRP group configuration mode, use the **no ipv6 address** command to cancel the configuration.



Tips: After you configure the virtual IP address of an HSVRP group, the system automatically generates the virtual MAC address corresponding to the HSVRP group based on the HSVRP group ID. The generated virtual MAC address is in the format of 00-00-5E-00-01-id, in which "id" indicates the hexadecimal HSVRP group ID. For example, the virtual MAC address of **hsvrp 17** is 00-00-5E-00-01-11.

Viewing an HSVRP Group

To view an HSVRP group, use the following command in any configuration mode:

show hsvrp [**id** *id*]

- **id** *id* - Specifies the ID of the HSVRP group whose information you want to view, including the virtual IP address, virtual MAC address, primary interface name, secondary interface name, and the name of the interface on which the virtual IP address takes effect.

Referencing an HSVRP Group by an Interface

In peer mode, to ensure that the interface address of the M0D1 or D0M1 device is still reachable when the device fails, the interface needs to reference an HSVRP group. After the interface references a configured HSVRP group and provides the IP address of the HSVRP group externally, traffic that accesses the IP address of the HSVRP group will reach this interface and be processed by the device where this interface belongs.

The following types of interfaces can reference an HSVRP group: physical interface, aggregate interface, redundant interface, VSwitch interface, or subinterface of preceding interfaces.

To reference an HSVRP group for an interface, in global configuration mode, use the following command to go to the interface configuration mode of the interface:

interface *interface-name*

- *interface-name* - Specifies the interface name and you will enter the configuration mode of the interface.

In interface configuration mode, use the following command to reference a configured HSVRP group for the interface:

hsvrp id *id* {**primary** | **secondary**}

- *id* - Specifies the ID of the HSVRP group.
- **primary** - Sets the interface to the primary interface of the HSVRP group. If both devices in peer A/A mode run as normal, the referenced HSVRP group is in the active state on the interface.
- **secondary** - Sets the interface to the secondary interface of the HSVRP group. If both devices in peer A/A mode run as normal, the referenced HSVRP group is in the inactive state on the interface.

In interface configuration mode, use the **no hsvrp id** *id* {**primary** | **secondary**} command to cancel the reference to the HSVRP group.



Notes:

- The IP address of an interface cannot be the same as the virtual IP address of the referenced HSVRP group.
- After an interface references an HSVRP group, you can still use the IP address of the interface itself. However, we recommend that you use the IP address as the management IP address instead of as the IP address of other service forwarding interfaces.
- If an interface is used as a primary interface and secondary interface respectively and is bound to two HSVRP groups, the IP address of these two HSVRP groups needs to belong to the same network segment.
- If an HSVRP group needs to be referenced, the IP address of the interface needs to be a static IP address configured manually, which cannot be obtained dynamically.
- If an interface needs to reference an HSVRP group, the interface cannot be configured with the management IP address or have the local attribute enabled, and the secondary IP address of the interface cannot be the same as the IP address of the referenced HSVRP group.
- After an interface references an HSVRP group, you can configure only static routes for network devices connected to the interface and cannot use dynamic routing protocols.

VRRP

Virtual Router Redundancy Protocol (VRRP) is a network layer protocol that serves as a high-availability solution. When the default gateway of network fails, the VRRP function can switch

business traffic to the backup device in a timely manner to implement redundant backup of the gateway and ensures reliable network communication.

VRRP includes two versions, VRRPv2 and VRRPv3. VRRPv2 supports IPv4 VRRP, while VRRPv3 supports both IPv4 VRRP and IPv6 VRRP. The current StoneOS system version supports only VRRPv3 and specifically supports IPv4 VRRP.

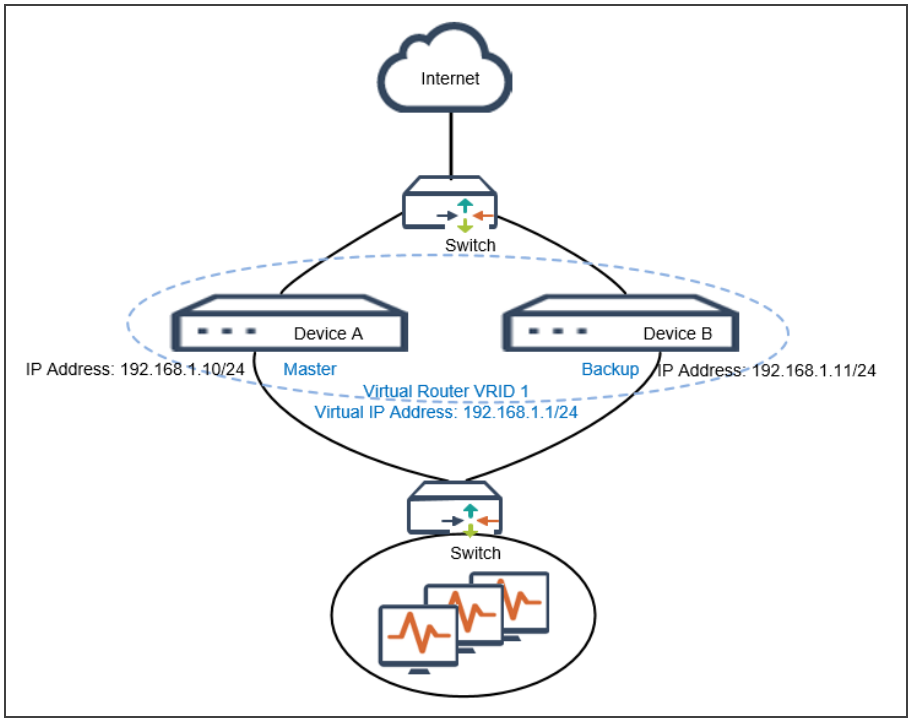


Notes:

- The VRRP function cannot be used together with the HA function.
- The VRRP function adopts the standard VRRP protocol, allowing for mutual negotiation with other manufacturer's devices that support the standard VRRP protocol.
- The VRRP function does not support configuration synchronization or session synchronization. It only provides redundant backup in case of gateway failures.

Basic Principle and Concept

VRRP enables multiple physical gateway devices to form a virtual router and sets the IP address of the virtual router to the default gateway address. Hosts within the LAN communicate with the external network through the virtual router. Packets of the virtual router are forwarded by one of the physical gateway devices in the virtual router. If this physical gateway device fails, VRRP uses an election algorithm to select a device from the remaining physical gateways to take over the failed device.



The following concepts are involved in VRRP:

- **Virtual Router**: Also known as a VRRP backup group, it consists of a master device and one or more backup devices, functioning as a virtual router to the external network. As shown in the figure above, Device A and Device B form a virtual router.
- **Virtual Router ID (VRID)**: It is used to identify the virtual router. In the figure above, the VRID for the virtual router composed of Device A and Device B is 1.
- **Virtual Router Master**: The device within the virtual router that is used to forward packets. As shown in the figure above, Device A is the master device.
- **Virtual Router Backup**: The device that can take over packet forwarding in case the master device fails. As shown in the figure above, Device B is the backup device.
- **Virtual IP Address**: The IP address of the virtual router. As shown in the figure above, the virtual IP address for the virtual router composed of Device A and Device B is 192.168.1.1/24.

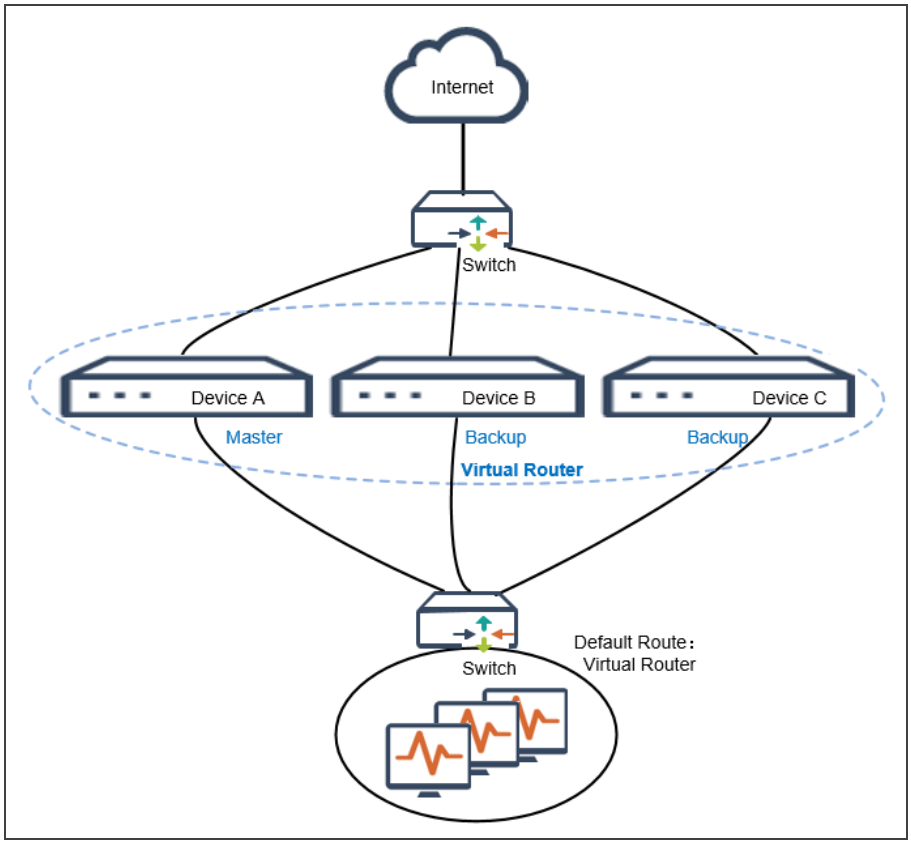
- **IP Address Owner**: If a device within a VRRP backup group has the same interface IP address as the IP address of the virtual router, the device is called IP address owner, whose priority remains 255 as long as it is in normal working condition, indicating that it is the master device.
- **Virtual MAC Address**: A virtual router has a virtual MAC address. The format of the virtual MAC address is "00-00-5E-00-01-VRID". Typically, when responding to ARP requests, the virtual MAC address is used instead of the actual MAC address of the interface. As shown in the figure above, the VRID for the virtual router composed of Device A and Device B is 1, so the MAC address for this VRRP backup group is 00-00-5E-00-01-01.
- **Priority**: Used for VRRP election, where the device with a higher priority is elected as the primary device. The priority value ranges from 1 to 254, with higher values indicating higher priorities. The priority value of 255 is reserved for the IP address owner.
- **Preempt Mode**: If the mode of a device within the VRRP backup group is set to preempt, it will become the master device once its priority is higher than that of the current master device. The previous master device will then become the backup device. If a device is set to non-preempt mode, even if its priority is higher than that of the master device, it can take over as the master device only when the current master fails.

Scenario

VRRP is used in two scenarios: master-backup redundancy and load balancing.

Master-Backup Redundancy

The master-backup redundancy scenario of VRRP involves a virtual router, which consists of a master device and one or more backup devices. The master device is used to forward packets. When the master device fails, a new master device is elected from the backup device based on priority. The new master device takes over the previous one and continues forwarding packets.

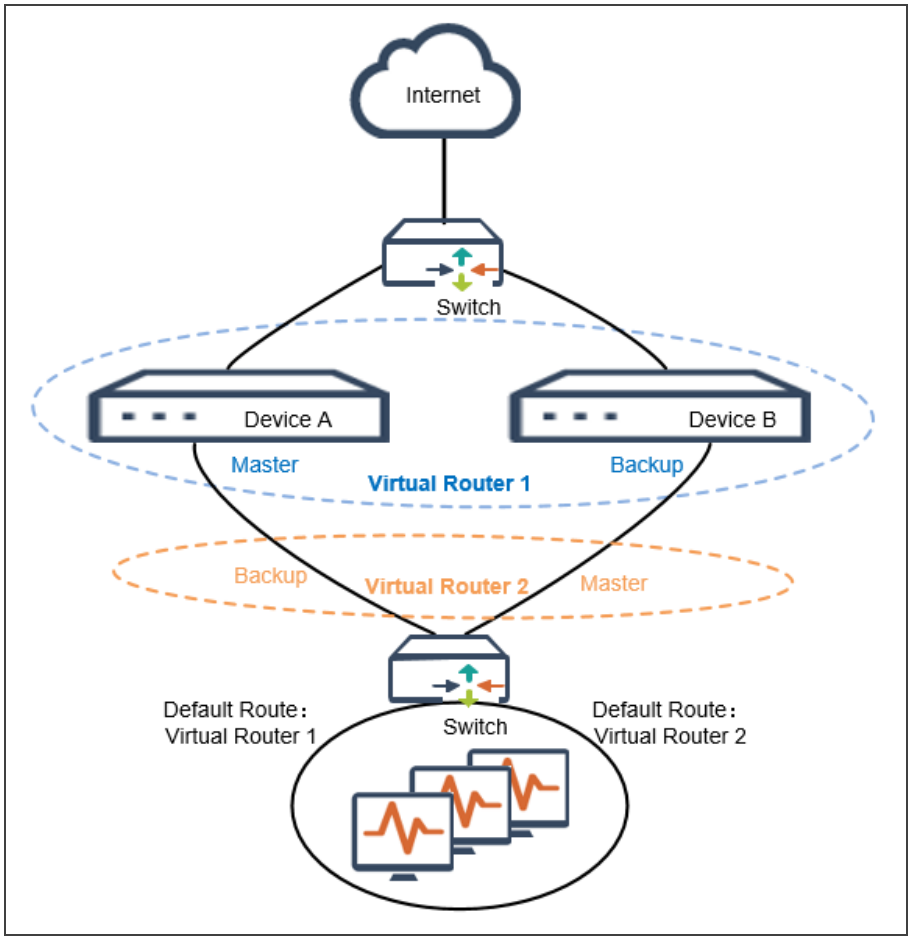


As shown in the figure above, Device A, Device B, and Device C form a virtual router. Device A acts as the master device to forward packets. Device B and Device C function as backup devices and do not forward packets. Device A periodically sends VRRP advertisement messages to notify Device B and Device C that it works properly. If Device A fails, the system will select a new master device from Device B and Device C based on priority to act as the gateway to continue forwarding packets.

Load Balancing

The load balancing scenario involves two or more virtual routers, where multiple virtual routers simultaneously act as gateways. You can assign different virtual routers as gateways for different hosts, enabling load balancing.

In the load balancing scenario, a single device can join multiple VRRP backup groups. By setting different priorities, the device can act as the master device in one backup group and as a backup device in other backup groups.



As shown in the figure above, Device A and Device B form two virtual routers, Virtual Router 1 and Virtual Router 2. In Virtual Router 1, Device A is the master device and Device B is the backup device. In Virtual Router 2, Device A is the backup device and Device B is the master device. Some hosts in the LAN use Virtual Router 1 as their gateway, and others use Virtual Router 2 as their gateway. Both Virtual Router 1 and Virtual Router 2 handle traffic, implementing load balancing of business traffic. If one of the virtual routers fails, all traffic will be processed by the virtual router that works properly, and this ensures mutual backup.

Configuring VRRP

To use the VRRP function, take the following steps:

1. Configure the VRRP backup group. To do this, you need to configure the virtual IP address of the VRRP backup group, specify the preempt mode and priority of devices in the backup

group, and configure the interval at which VRRP advertisement messages are sent.

2. Bind the VRRP backup group to interface.

Configuring the VRRP Backup Group

To configure the VRRP backup group, in global configuration mode, use the following command:

vrrp group *group-id*

- *group-id* - Specifies the ID of the VRRP backup group, which needs to be an integer from 1 to 255.

After the command is executed, the system enters the VRRP backup group configuration mode. In global configuration mode, use the **no vrrp group** *group-id* command to delete the specified VRRP backup group.



Notes: You can create up to 12 VRRP backup groups.

Configuring the Virtual IP Address of the VRRP Backup Group

To configure the virtual IP address of the VRRP backup group, in VRRP backup group configuration mode, use the following command:

virtual-ip *ip-address*

- *ip-address* - Specifies the virtual IP address of the VRRP backup group.

In VRRP backup group configuration mode, use the **no virtual-ip** command to delete the specified virtual IP address of the VRRP backup group.



Notes:

- You can configure only one virtual IP address for a VRRP backup group.
- Each virtual IP address of VRRP backup group needs to be unique.

Configuring the Preempt Mode

If the mode of a device within the VRRP backup group is set to preempt, it will become the master device once its priority is higher than that of the current master device. The previous master device will then become the backup device. If a device is set to non-preempt mode, even if its priority is higher than that of the master device, it can take over as the master device only when the current master fails. When you configure the preempt mode, you can also specify the delayed time to allow the backup device to upgrade to the master device after the specified delayed time. To configure the preempt mode, in VRRP backup group configuration mode, use the following command:

preempt [**delay** *delay-time*]

- **delay** *delay-time* - Specifies the delayed time, which ranges from 0 to 3,600 seconds. The default value is 0.

In VRRP backup group configuration mode, use the **no preempt** command to restore to the non-preempt mode.

Specifying the Priority

The priority specified in this command is used for VRRP election. In a VRRP backup group, the device with a higher priority is elected as the master device, where a greater value indicates a higher priority. To specify the priority for device, in VRRP backup group configuration mode, use the following command:

priority *number*

- *number* - Specifies the priority, which needs to be an integer from 1 to 254. The default value is 100.

In VRRP backup group configuration mode, use the **no priority** command to restore the priority to the default value.

Configuring the Interval of Sending VRRP Advertisement Messages

The master device in the VRRP backup group sends VRRP advertisement messages periodically to notify the backup devices of its operational status. If backup devices do not receive VRRP

advertisement messages within the Master Down interval, a VRRP election will be triggered to select a new master device.

The calculation of the Master Down interval is determined by the formula: 3 * Interval of sending VRRP advertisement messages + Skew_Time. Skew_Time is calculated as follows: ((256 - priority of the device in the backup group) * Interval of sending VRRP advertisement messages) / 256.

To configure the interval at which VRRP advertisement messages are sent, in VRRP backup group configuration mode, use the following command:

advertise-interval *interval-value*

- *interval-value* - Specifies the interval at which VRRP advertisement messages are sent, which ranges from 1 to 40 seconds. The default value is 1.

In VRRP backup group configuration mode, use the **no advertise-interval** command to restore the interval to the default value.

Bind the VRRP Backup Group to Interface

The VRRP backup group takes effect only after bound to an interface, which can be a physical interface, physical sub-interface, aggregate interface, aggregate sub-interface, redundant interface, or redundant sub-interface. To bind the configured VRRP backup group to the interface, in interface configuration mode, use the following command:

vrrp group *group-id*

- *group-id* - Specifies the ID of the configured VRRP group.

In interface configuration mode, use the **no vrrp group** *group-id* command to disassociate the specified VRRP backup group from the interface.



Notes:

- A VRRP backup group can only be bound to an interface. At most two VRRP backup groups can be bound to the same interface.

- The logical interface bound to a VRRP backup group can be deleted only after the interface is unbound.
- Before binding a VRRP backup group to an interface, configure an IP address for the interface and a virtual IP address for the VRRP backup group. The IP address of the of the interface and the virtual IP address of the VRRP backup group need to fall into the same network segment.
- After the VRRP backup group is bound to an interface, you need to unbind the VRRP backup group before deleting or editing the IP address of the interface.
- You cannot modify the virtual IP address of the VRRP backup group bound to an interface.
- A VRRP backup group cannot be bound to an interface that is configured with DHCP or management IP address.
- If the virtual IP address of the VRRP backup group is the same as the primary IP address of the bound interface, the priority of the device where the interface resides is 255, the highest priority.

Configuring the Checksum Calculation Method for VRRP Messages

The system calculates the checksum of VRRP messages to check whether the VRRP messages are valid. By default, the system does not carry a pseudo header when calculating the checksum of VRRP messages. You can configure the system to carry a pseudo header when calculating the checksum of VRRP messages. To do this, in global configuration mode, use the following command:

vrrp checksum-method with pseudo-header

In global configuration mode, use the **no vrrp checksum-method with pseudo-header** command to restore to the default calculation method.



Notes: When negotiating VRRP with devices from other manufactures, make sure that the checksum calculation method of VRRP messages is the same as that of devices from the other manufactures.

Viewing Information about VRRP Backup Group

To view information about VRRP backup group, in any mode, use the following command:

- **show vrrp all**: displays all information about VRRP backup group, including the ID of the VRRP backup group, interface to which the VRRP backup group is bound, active/standby status of the device, virtual IP address, virtual MAC address, interval at which VRRP advertisement messages are sent, priority, the status of the preempt mode, Master Down interval, the IP address and priority of the master device, the interval at which the master device sends VRRP advertisement messages.
- **show vrrp all brief**: displays all information about VRRP backup group in a brief list.
- **show vrrp interface** *interface-name*: displays all information about VRRP backup group bound to the specified interface, including the VRRP backup group ID, the interface to which the VRRP backup group is bound, active/standby status of the device, virtual IP address, virtual MAC address, interval at which VRRP advertisement messages are sent, priority, the status of the preempt mode, Master Down interval, the IP address and priority of the master device, the interval at which the master device sends VRRP advertisement messages.
- **show vrrp interface** *interface-name* **brief** : displays all information about VRRP backup group bound to the specified interface in a brief list.
- **show vrrp group** *group-id*: displays information about the specified VRRP backup group, including the VRRP backup group ID, the interface to which the VRRP backup group is

bound, active/standby status of the device, virtual IP address, virtual MAC address, interval at which VRRP advertisement messages are sent, priority, the status of the preempt mode, Master Down interval, the IP address and priority of the master device, the interval at which the master device sends VRRP advertisement messages.

- **show vrrp group** *group-id* **brief** : displays information about the specified VRRP backup group in a brief list.

Twin-mode HA

Introduction

Currently , data centers providing important data information and office services in many industries. In order to improve the reliability, companies generally build two or more data centers, and the extended mode of L2 (DCI: Data Center Interconnection) is used for inter-connections between two data centers. Two data centers running independently, providing business services and mutual backup, constitute a redundant data center.

The Hillstone devices are deployed in the data center under the routing mode, used to check traffic and isolated by policy across different regions. Because of the DCI, the asymmetric L3 traffic that across the data center and different regions may occurs (i.e., inbound and outbound traffic may take different routes), the policy isolation will not take effect. To resolve this problem, system provides the Twin-mode HA function. This function will optimizes the traffic forwarding, ensuring the business continuity and efficiency of redundant data centers.



Notes:

- Currently, only some devices (All platforms of X series, E3960 and above platforms of E series and A3000 and above platforms of A series) support the function.
- Before configuring Twin Mode, make sure you have already installed Twin-mode License。
- Currently, only the IP address and peer IP address of the twin-mode HA A/P link interface supports IPv6.
- You must enable HA function before enable the Twin-mode HA function, and the devices must in Active-Passive (A/P) mode.



- In twin-mode A/P mode or twin-mode A/A mode, you must configure the same HA cluster ID for the data center.

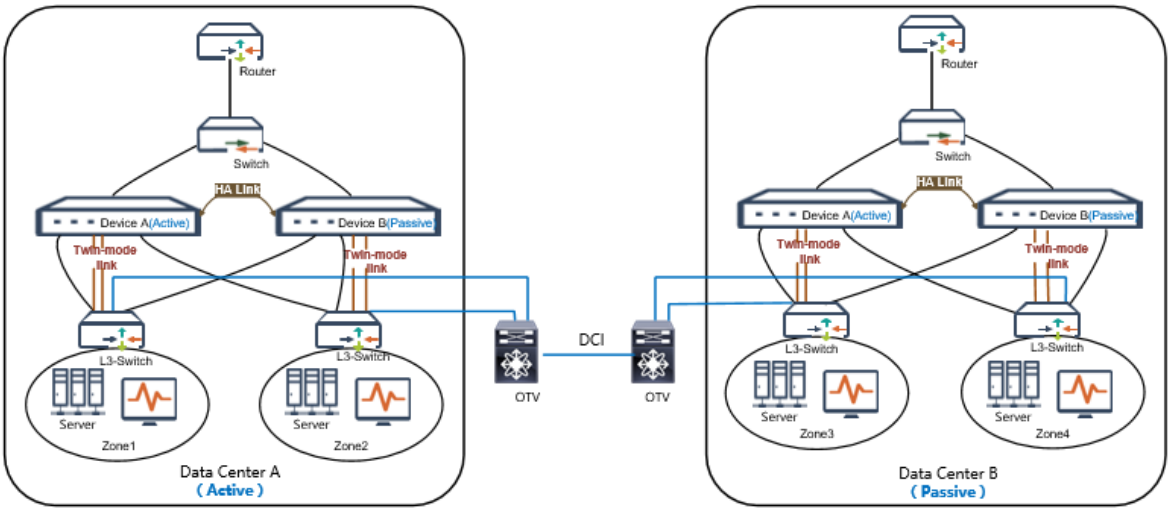
Currently, The system supports functions for Twin-mode HA listed in Table below. For more details and configuration, see relevant section.

Function			
Application Layer Gateway (ALG)	Interface	High Availablity (HA)	Routing
Application Layer Identification and Control	System Management	Log	Virtual System (VSYS)
Network Address Translation (NAT)	Monitor	Report	SNMP
Attack Defense	Firewall		

Twin-mode HA Deployment Scenarios

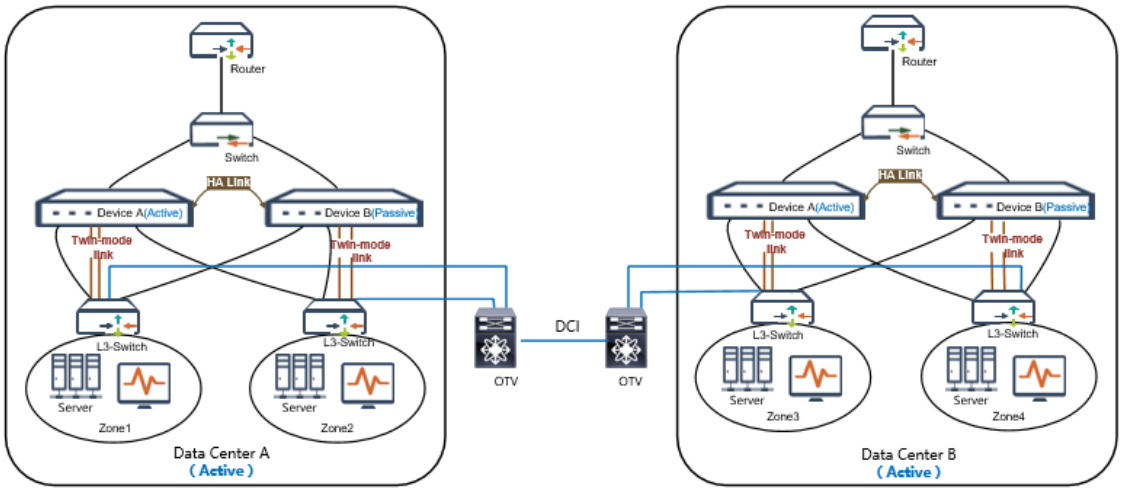
There are three kinds of typical L2TP twin-mode deployment scenarios:

- Active-Passive（A/P）deployment scenarios



As shown in the figure above, configure two data center to form an HA group, with one data center acting as a master device and the other acting as its backup device. When the master data center fails, the backup data center will be promoted to master and take over its work to forward packets. The Hillstone devices are deployed on each data center (you can use 3 straight series deployment or deploy the device in the gateway location), and make up the HA A/P mode.

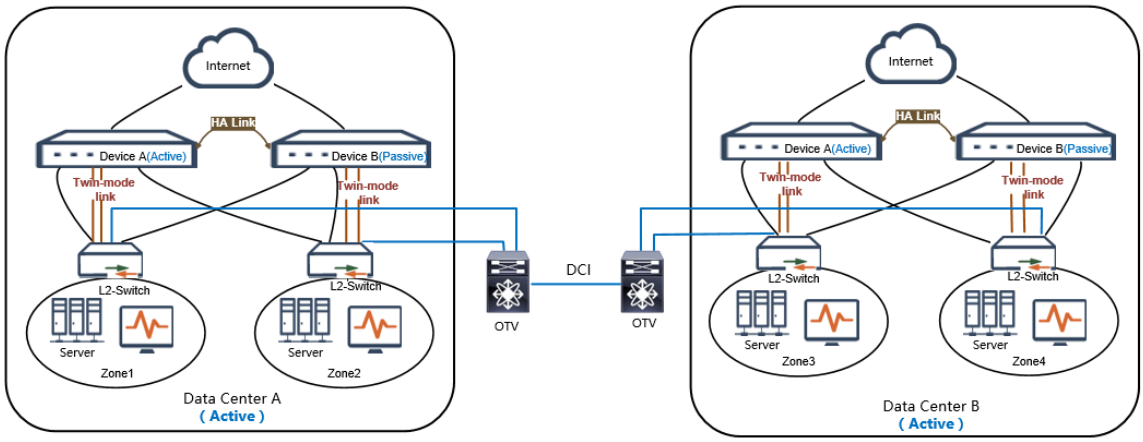
- Active-Active（A/A）deployment scenarios



As shown in the figure above, the two data centers perform their own tasks simultaneously,

and monitor the operation status of each other. When one data center fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. The Hillstone devices are deployed on each data center and make up the HA A/P mode. Through Twin-mode HA function, the problem of asymmetric L3 traffic that across the data center and different regions is solved.

- Gateway deployment scenarios: This deployment scenarios is a special Active-Active （A/A） deployment scenarios.



As shown in the figure above, the Hillstone devices are deployed in the data center as a gateway and make up the HA A/P mode. The two data centers consist of twin-mode A/A mode, and backup each other. Since the extended device of L2 filters the same IP address and MAC address of the data center gateway, this problem is solved by deploying the gateway mode and configuring the twin-mode HA gateway function.

Twin-mode HA Synchronization

To ensure the backup device can take over the work of the master data center when it fails, the master data center will synchronize its information with the backup data center. In different deployment modes, the system supports different synchronous mode and synchronous information types.

In twin-mode HA A/P mode, the types of information that can be synchronized includes:

- IPv4 configuration information
- IPv4/IPv6 session information

- IPv4 ARP tabel
- IPv4 pinhole
- IPv4 track information
- IPv4/IPv6 dynamic route information
- IPv4 NTP information
- IPv4 signature file
- IPv6 ND neighbor information
- IPv6 PMTU entries

In twin-mode HA A/A mode, the system supports two synchronous mode: Part synchronization and No synchronization. About configuration steps, refer to Specifying the deployment mode and synchronization mode. The types of information that can be synchronized includes:

- IPv4 configuration information (Policy/Service Book/Address Book/IPS/AV/URL/Schedule)
- IPv4 session information
- IPv4 pinhole
- IPv4 signature file

Configuring Twin-mode HA

The Twin-mode HA need to be configured in the Twin-mode configuration mode. To enter the Twin-mode configuration mode, in the global configuration mode, use the following command:

twin-mode

After executing the command, the system will enter the Twin-mode configuration mode.

In the Twin-mode configuration mode, you can perform the following configurations:

- Specifying the deployment mode and synchronization mode for Twin-mode HA
- Specifying the Node
- Specifying the Priority
- Configuring the Preempt Mode
- Specifying the Hello Interval
- Specifying the Hello Threshold
- Configuring Twin-mode HA Link
- Enabling / Disabling Twin-mode HA



Notes:

- Before configuring the twin-modefunction, you should install the Twin-mode License first.
- The deployment mode, node value, link must be specified.

Specifying the deployment mode and synchronization mode

Currently, supports two deployment modes for Twin-mode HA: A/A mode and A/P mode. The system supports two synchronization mode: Part synchronization and No synchronization. In the Twin-mode configuration mode, use the following command:

mode {**active-active** [**no-sync** | **part-sync**] | **active-passive** }

- **active-active** [**no-sync** | **part-sync**] – Specifies the deployment mode is A/A mode.
- **no-sync** - Specifies the synchronization mode is no synchronization.
- **part-sync** - Specifies the synchronization mode is part synchronization mode. About specific

synchronization information content, refer to Twin-mode HA Synchronization

- **active-passive** – Specifies the deployment mode is A/P mode.

To cancel the specified deployment mode, in the Twin-mode configuration mode, use the following command:

no mode

Specifying the Node

To distinguish the data center, you can use the value of Node to mark the data center. To specify the Node, in the global configuration mode, use the following command:

node *node-ID*

- *node-ID* – Specifies the Node. The range is 0 to 1.

To cancel the specified Node, in the Twin-mode configuration mode, use the following command:

no node



Notes:

- You must specify the different Node for each data center.
- User needs to restart the device to make it take effect after modifying the Node.

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device of data center. To specify the priority, in the Twin-mode configuration mode, use the following command:

priority *number*

- *number* – Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the Twin-mode configuration mode, use the following command:

no priority



Tip: When the priorities are identical, the device with Node 0 will be priorized.

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the Twin-mode configuration mode, use the following command:

preempt [*delay-time*]

- *delay-time* – Specifies the delay time. The value range is 1 to 600 seconds. The default value is 3.

To cancel the preempt mode, in the Twin-mode configuration mode, use the following command:

no preempt

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the Twin-mode configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* – Specifies the interval for sending heartbeats. The value range is 1 to 10 seconds. The default value is 1s.

To restore to the default Hello interval, in the Twin-mode configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device's heartbeat fails. To specify the Hello threshold, in the Twin-mode configuration mode, use the following command:

hello threshold *value*

- *value* – Specifies the Hello threshold value. The value range is 5 to 255. The default value is 10.

To restore to the default Hello threshold, in the Twin-mode configuration mode, use the following command:

no hello threshold

Configuring Twin-mode HA Link

There are two types of Twin-mode HA links, control Link and data Link. Currently, system only support to specify the physical interfaces and aggregation interfaces as a Twin-mode HA link interface.

You need to specify the Twin-mode HA link interface first, and then specify the IP address and peer IP address of the interface.

Specifying a Twin-mode HA Link Interface

To specify a Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link { **control** | **data** } **interface** *interface-name*

- **control** | **data** – Specifies the Twin-mode HA link type.
- *interface-name* – Specifies the name of the interface.

To delete the specified Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

no link { **control** | **data** } **interface** *interface-name*



Notes:

- Data link interface does not allow specifying on the X-series device panel interface ethernet0/0- ethernet0/3.
- Control Link and Data Link can specify up to two interfaces.
- When asymmetric data traffic is larger, it is recommended that users use two data links or using a aggregate interface to ensure sufficient bandwidth for transmitting data traffic.

Specifying the IP Address of Twin-mode HA link Interface

After the Twin-mode HA link interface is specified, to configure the IPv4 or IPv6 address of the Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link {**ip** | **ipv6**} *ip-address netmask*

- **ip** | **ipv6** – Specifies the IP address of the Twin-mode HA link interface. It can be an IPv4 (**ip**) or IPv6 (**ipv6**)address.
- *ip-address netmask* – Specifies the IPv4 address and the netmask or the IPv6 address prefix and the prefix length of the Twin-mode HA link interface.

To cancel the specified IP address, in the Twin-mode configuration mode, use the following command:

no link {**ip** | **ipv6**}

Specifying the Peer IP Address

The peer IP supports both IPv4 or IPv6 address. To configure the peer IP address, in the Twin-mode configuration mode, use the following command:

peer-ip {**ip** | **ipv6**} *ip-address*

- **ip** | **ipv6** – Specifies the IP address of the peer. It can be an IPv4 (**ip**) or IPv6 (**ipv6**)address.
- *ip-address* – Specifies the IPv4 address or the IPv6 address of the peer. You can configure up to two peer IP adresses.

To cancel the specified peer IP address, in the Twin-mode configuration mode, use the following command:

no peer-ip



Notes:

- Currently, only the IP address and peer IP address of the twin-mode HA A/P link interface supports IPv6 configurations.
- The type of the IP address and the peer address of the twin-mode HA A/P link interface must be the same, such as IPv4 or IPv6.

Enabling/Disabling Twin-mode HA

By default the Twin-mode HA function is disabled. To enable or disable Twin-mode HA, in the Twin-mode configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

Specifying the Forwarding Mode of Asymmetric Traffic

For the asymmetric traffic, Twin-mode HA provides two forwarding mode: tunnel mode and layer 2 tunnel mode.

- Tunnel Mode: The encapsulated package will be sent to the peer data center through Data Link, after the traffic was de-encapsulated , the peer data center will transfer it. By default, the forwarding mode is tunnel mode.
- Layer 2 Tunnel Mode: The MAC address of the packet is modified as the virtual MAC (VMAC) address which corresponds to its interface of peer data center, the traffic is forwarded through layer 2 tunnel. With this mode, the user needs to enable the layer 2 tunnel forwarding mode at all business interfaces of the device.

To enable the layer 2 tunnel forwarding mode, in the interface configuration mode, , use the following command:

twin-mode-l2-tunnel-enable

To restore to the default forwarding mode, in the interface configuration mode, use the following command:

no twin-mode-l2-tunnel-enable



Notes: The forwarding mode must be specified. The two modes cannot be mixed, otherwise the function is not effective.

Configuring Twin-mode HA First Packet Forwarding Bounce Back

In twin-mode HA Active-Active （A/A） deployment scenarios, you can configure the first packet forwarding bounce back function. With this function enabled, the local device sends the new session synchronization information and the first packet that triggered the new session to the peer device successively. When the peer device completes the session creation, it will return the received first packet to the local device, and then the local device will perform the next step of forwarding processing, thus solving the problem of packet loss caused by reply packet not finding

the session due to the untimely session synchronization of the peer device in the asymmetric routing environment.

To configure the Twin-mode first packet forwarding bounce back function, use the following command in the Twin-mode configuration mode:

first-packet-bounce-back [**max-size** *num*]

- **max-size** *num* – Specifies the size of the first packet. The unit is byte. The value is 64 to 1024. Without configuring this parameter, the default value is 124.

To cancel the above configurations, use the following command in the Twin-mode configuration mode:

no first-packet-bounce-back

Configuring Twin-mode HA Gateway

In the gateway deployment scenarios, because the extended device of L2 filters the same IP address and MAC address of the data center gateway, the asymmetric traffic blocked. In order to avoid this problem, you needs to enable the twin-mode gateway function, and configure gateway interface IP address for sending the ARP request message, the system will take this IP address as the source of IP, Twin-mode virtual MAC (VMAC) as the source MAC address to send the ARP request message, and forward the data traffic with Twin-mode virtual MAC (VMAC) address as the source address, so as to solve the problem of asymmetric traffic.

To enable the twin-mode gateway function and configure gateway interface IP address for sending the ARP request message, in the interface configuration mode, use the following command:

twin-mode-gateway sender-ip *ip-address*

- *ip-address* – Specifies the gateway interface IP address for sending the ARP request message. This IP address must be in the same network segment as the IP address of the gateway interface.

To disable this function and delete the specified IP address, in the interface configuration mode, use the following command:

no twin-mode-gateway sender-ip *ip-address*



Notes: The gateway interface IP for sending ARP request messages of both data centers must be different.

Configuring the Switching Mode of Twin-mode HA Session State

In the twin-mode HA A/A mode, system supports two switching modes of twin-mode HA session state, including unidirectional switching and bidirectional switching.

- Unidirectional switching: When a link of access extranet server fails in the data center, the system will quickly switch the inactive twin-mode HA session state to the active state, and ensure that the traffic will not be interrupted.
- Bidirectional switching: When you need to modify the traffic forwarding path of data center, you can use this switching mode, the system will quickly switch the inactive twin-mode HA session state to the active state, so as to optimize the traffic paths.

To configure the switching mode of twin-mode HA session state, in the Flow configuration mode, use the following command:

twin-mode-sess-owner-change {**follow-init-direction** | **follow-two-direction**}

- **follow-init-direction** – Unidirectional switching, when the traffic hits the upstream traffic of the inactive session, the system will switch the session state.
- **follow-two-direction** – Bidirectional switching, when the traffic hits both the upstream and downstream traffic of the inactive session, the system will switch the session state.

To disable this function, in the Flow configuration mode, use the following command:

no twin-mode-sess-owner-change



Tip: To enter the flow configuration mode, in the global configuration mode, use the command **flow**.

Manually Synchronizing Twin-mode HA Configuration Information

In some exceptional circumstances, the master and backup configurations of data center may not be synchronized. In such a case you need to manually synchronize the twin-mode HA configuration information of the master and backup data center. To determine if you need to manually synchronize the twin-mode HA information, take the following steps:

1. View the relevant configuration information of both master and backup datacenter by using the command **show twin-mode configuration difference** on the master device.
2. According to the displayed configuration information, determine whether you need to manually synchronize the twin-mode HA information:

- If the configuration information is consistent, then you don't need to synchronize manually;
- If the configuration information is inconsistent, you need to run the command**exec twin-mode sync configuration**to manually synchronize the configuration.



Notes: The command **exec twin-mode sync configuration** can only be executed on the master HA device of the master data center.

Viewing/Clearing the Transfer Packet Count of Twin-mode HA

To view the transfer packet count of Twin-mode HA, in any mode, use the following command:

show twin-mode-counter

To clear the transfer packet count of Twin-mode HA, in any mode, use the following command:

clear twin-mode-counter

Viewing Twin-mode HA Configuration

To view the Twin-mode HA configuration information, use the following commands:

- Show the Twin-mode HA configuration information: **show twin-mode configuration**
- Show the Twin-mode HA link information: **show twin-mode link**
- Show the Twin-mode HA peer status: **show twin-mode peer**
- Show the Twin-mode HA status: **show twin-mode status**

Examples of HA

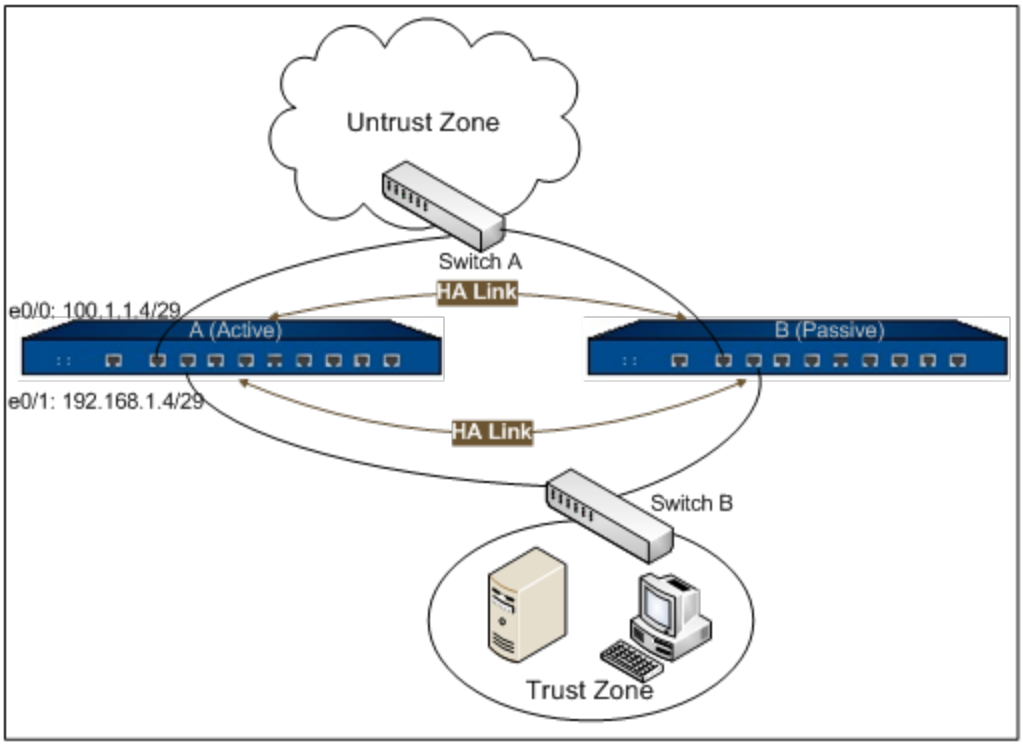
This section describes three HA configuration examples:

- Example 1: configuration example of HA in A/P mode
- Example 2: configuration example of HA Peer A/A mode and HA traffic

Example 1: Example of HA in A/P Mode

Requirement

To goal is use two Hillstone devices, which are of the same hardware platform, firmware version, and license, to a form an HA cluster in Active-Passive mode. In addition, the two devices are using the same interface to connect to the network. The network topology is shown below:



Configuration Steps

Step 1: Configure the interfaces and policy rules on Device A:

Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 100.1.1.4/29
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.4/29
hostname(config-if-eth0/1)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure a track object which is used for tracking the status of interface of the master device, and if the interface ethernet0/0 fails, the device will implement failover:

```
hostname(config)# track trackobj1
hostname(config-trackip)# interface ethernet0/0 weight 255
hostname(config-trackip)# exit
hostname(config)#
```

Step 3: Configure an HA group:

Device A

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

Device B

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)#
```

Step 4: Configure HA link interfaces and enable the HA function:

Device A

```
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 10.10.1.1/24
hostname(config)#
```

Device B

```
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 10.10.1.2/24
hostname(config)#
```

Step 5: Configure an HA cluster to enable HA:

Device A

```
hostname(config)# ha cluster 1
```

Device B

```
hostname(config)# ha cluster 1
```

Step 6: Configure the management IPs of the master device and backup device after synchronization:

Device A

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.253
```

Device B

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.254
```

Step 7: Configure a track object on Device B, and if the interface ethernet0/0 on Device B fails, the device will implement failover:

Device B

```
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

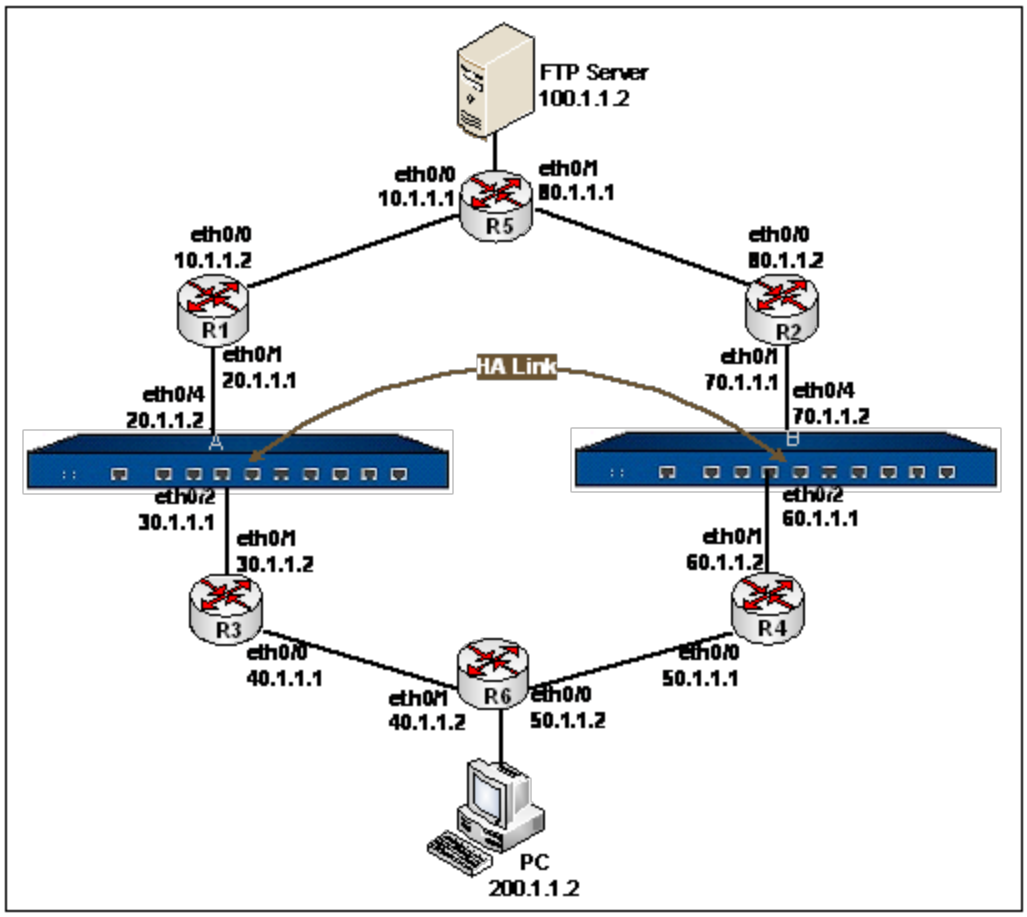
After the above configuration, the system will select Device A as the master device for forwarding traffic. Device B acts as the backup device. Device A will synchronize its configuration information and status to Device B. When Device A fails and cannot forward traffic, or the ethernet0/0 of Device A is disconnected, Device B will switch to the master device without interrupting user's communication, and continue to forward the traffic.

Example 2: Example of HA Peer Mode and HA Traffic

Requirement

This section describes how to configure HA Peer mode and HA traffic in asymmetrical routing environment. Before configuring, make sure the two Hillstone devices that will adopt HA Peer mode are using the same hardware platform, firmware version, license, and the interfaces that are connected to the network belong to the same security zone.

After completing the configuration, both of the two devices enable HA traffic. When PC requests any virus file in zip format from the FTP server, this function can assure the inbound and out-bound packets will be processed on Device A, and related logs will also be generated on Device A. The network topology is shown below:



Configuration Steps

The following steps omit the configuration of interfaces and zones, and only focus on the configuration of HA Peer mode and HA traffic.

Step 1: Configure HA Peer mode and HA link interfaces:

Device A

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 10.10.1.1/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha group 0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# exit
hostname(config)# ha cluster 1 peer-mode node 0
Confirm: If you set HA peer mode, the system need reboot by administrator, continue? [y]/n: y
hostname(config)#
```

Device B

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 10.10.1.2/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha group 0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# exit
hostname(config)# ha cluster 1 peer-mode node 1
Confirm: If you set HA peer mode, the system need reboot by administrator, continue? [y]/n: y
hostname(config)#
```

Step 2: Enable HA traffic:

Device A

```
hostname(M0D1) (config)# ha traffic enable
hostname(M0D1) (config)#
```

Device B

```
hostname(D0M1) (config)# ha traffic enable
hostname(D0M1) (config)#
```

Step 3: Configure the asymmetric routing environment. Assume that all routers use the OSPF protocols and you have set the default metric and cost:

Device A

```
hostname(M0D1) (config) # ip vrouter trust-vr
hostname(M0D1) (config-vrouter)# router ospf
hostname(M0D1) (config-router) # router-id 1.1.1.1 local
hostname(M0D1) (config-router) # network 20.1.1.1/24 area 0
hostname(M0D1) (config-router) # network 30.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 60.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 70.1.1.1/24 area 0
hostname(M0D1) (config-router)# exit
hostname(M0D1)(config-vrouter)# exit
hostname(M0D1) (config)# interface eth0/2
hostname(M0D1) (config-if-eth0/2)# zone trust
hostname(M0D1) (config-if-eth0/2)# ip address 30.1.1.1/24
hostname(M0D1) (config-if-eth0/2)# exit
hostname(M0D1) (config)# interface eth0/2:1
hostname(M0D1) (config-if-eth0/2:1)# zone trust
hostname(M0D1) (config-if-eth0/2:1)# ip address 60.1.1.1/24
```

```
hostname(M0D1) (config-if-eth0/2:1)# exit
hostname(M0D1) (config)# interface eth0/4
hostname(M0D1) (config-if-eth0/4)# zone trust
hostname(M0D1) (config-if-eth0/4)# ip address 20.1.1.2/24
hostname(M0D1) (config-if-eth0/4)# exit
hostname(M0D1) (config)# interface eth0/4:1
hostname(M0D1) (config-if-eth0/4:1)# zone trust
hostname(M0D1) (config-if-eth0/4:1)# ip address 70.1.1.2/24
hostname(M0D1) (config-if-eth0/4:1)# exit
hostname(M0D1) (config)#
```

Device B

```
hostname(D0M1) (config)# ip vrouter trust-vr
hostname(D0M1) (config-vrouter)# router ospf
hostname(D0M1) (config-router)# router-id 1.1.1.2 local
```

Step 4: Configure a track object to monitor the status of ethernet0/1 on R3. If the interface fails, all the sessions will be switched to Device B:

Device A

```
hostname(M0D1) (config)# track track1
hostname(M0D1) (config-trackip)# ip 30.1.1.2 interface eth0/2
hostname(M0D1) (config-trackip)# exit
hostname(M0D1) (config)# ha group 0
hostname(M0D1) (config-ha-group)# monitor track track1
hostname(M0D1) (config-ha-group)# exit
```

Step 5: Configure an AV profile on Device A and bind to the security zone:

Device A

```
hostname(M0D1) (config)# av-profile av
```

```
hostname(M0D1) (config-av-profile)# protocol-type ftp action log-only
hostname(M0D1) (config-av-profile)# file-type zip
hostname(M0D1) (config-av-profile)# exit
hostname(M0D1) (config)# zone untrust
hostname(M0D1) (config-zone-untrust)# av enable av
hostname(M0D1) (config-zone-untrust)# exit
```

Chapter 7 IPv6

System supports IPv6 (Internet Protocol Version 6). Compared with IPv4, IPv6’ s noticeable advantages include larger address space, simplified header, flexible header expansion and options, hierarchical address allocation, automatic stateless address allocation, data security supported by IPsecIPSec header, stronger QoS management support, etc.

StoneOS is dual-stack firmware that supports both IPv4 and IPv6. It also supports tunneling technique (the latest version supports manual IPv6 tunnel) for IPv6 communication.

This chapter describes IPv6 configuration of StoneOS, including:

- Configuring an IPv6 address
- Configuring IPv6 NDP
- Configuring IPv6 system management
- Configuring IPv6 SNMP
- Configuring IPv6 debugging
- Configuring an IPv6 route
- Configuring IPv6 DNS
- Configuring PMTU
- Configuring an IPv6 policy rule
- Configuring IPv6 ALG
- NDP protection
- Configuring an IPv6 6to4 tunnel
- Configuring an IPv6 4to6 tunnel
- Configuring NAT-PT

- Configuring NAT64 and DNS64
- IPv6 configuration examples



Notes: All the IPv6-related functions in the current firmware version support multiple VRs, i.e.,system support the default VR trust-vr.

Configuring an IPv6 Address

Hillstone devices support dual stacks, so the interfaces can support IPv4 and IPv6 addresses simultaneously. By default only IPv4 is enabled. To enable IPv6 on an interface, in the interface configuration mode, use the following command:

ipv6 enable

After enabling IPv6 on the interface, the system will also generate a link-local unicast IPv6 address for the interface.

To disable IPv6 and delete the link-local address allocated to the interface automatically, use the command **no ipv6 enable**. However, if the interface is configured with other IPv6 options, this command is not allowed.

For example, to enable IPv6 on ethernet0/1, use the following command:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ipv6 enable
```

After enabling IPv6 on an interface, you can configure the following IPv6 options for the interface:

- Specifying a global IPv6 address
- Specifying address auto-config
- Specifying an EUI-64 address
- Specifying a link-local address

- Specifying an IPv6 MTU
- Viewing IPv6 Configuration

Specifying a Global IPv6 Address

Typically the global IPv6 address specified for an interface follows the format of IPv6 address prefix/prefix length. Besides, the system also supports the format of IPv6 general prefix, i.e., an address consisting of general prefix and sub-prefix. The general prefix need to be configured in the global configuration mode, and can be referenced when users are specifying an address for an interface. To specify a global IPv6 unicast address for an interface, in the interface configuration mode, use the following command:

ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*}

- *ipv6-address* – Specifies the IPv6 address prefix.
- *Mask* – Specifies the prefix length. The value range is 1 to 128.
- *general-prefix-name* – Specifies the name of general prefix.
- *sub-prefix/Mask* – Specifies the sub-prefix.

Suppose the name of general prefix is test-prefix, the IPv6 address prefix is 2002:ae3:1111::/48, the sub-prefix is 0:0:0:2222::1/64, then the command **ipv6 address test-prefix 0:0:0:2222::1/64** will specify the IPv6 address 2002:ae3:1111:2222::1/64 for the interface.

To cancel the specified global IPv6 unicast address, use the following commands:

no ipv6 address (cancels all the IPv6 addresses on the interface)

no ipv6 address {*ipv6-address/Mask* | *general-prefix-name sub-prefix/Mask*} (cancels the specified IPv6 address on the interface)

Configuring an IPv6 General Prefix

The system supports IPv6 and 6to4 general prefix. The 6to4 general prefix follows the format of 2002:a:b::/48, where a:b is a hexadecimal address translated from the IPv4 address of the referenced interface (specified by interface-name). To configure an IPv6 general prefix, in the global configuration mode, use the following command:

ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

- *prefix-name* – Specifies the name of general prefix.
- *X:X:X:X::X/M* – Specifies the IPv6 address prefix for the general prefix.
- **6to4** – Specifies to use 6to4 general prefix.
- *interface-name* – Specifies the interface referenced by the 6to4 general prefix (references the IPv4 address of the interface).

To delete the specified IPv6 general prefix, in the global configuration mode, use the following command:

no ipv6 general-prefix *prefix-name* {*X:X:X:X::X/M* | **6to4** *interface-name*}

To view the IPv6 general prefix defined in the system, in any mode, use the following command:

show ipv6 general-prefix

Specifying Address Auto-config

In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. To specify address auto-config, in the interface configuration mode, use the following command:

ipv6 address autoconfig [**default**]

- **default** – If the interface is configured with a default router, this option will generate a default route to the default router.

To cancel address auto-config, in the interface configuration mode, use the following command:

no ipv6 address autoconfig

Specifying an EUI-64 Address

To specify an IPv6 address that uses EUI-64 interface ID, in the interface configuration mode, use the following command:

ipv6 address *ipv6-address/Mask* **eui-64**

- *ipv6-address* – Specifies the IPv6 address prefix.
- *Mask* – Specifies the prefix length. The value range is 1 to 128. If the length value is not larger than 64, the last 64 bits of the address will use the generated interface ID; if the length value is larger than 64, the last (128-prefix) bits of the address will use the generated interface ID.

To cancel the specified EUI-64 address, in the interface configuration mode, use the command:

no ipv6 address *ipv6-address/Mask* **eui-64**

Specifying a Link-local Address

Link-local address is used for communication between adjacent nodes of a single link, for example, communication between hosts when there is no router on the link. By default the system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one. To specify a link-local for an interface, in the interface configuration mode, use the following command:

ipv6 address *ipv6-address* **link-local**

- *ipv6-address* – Specifies an IPv6 address.

To cancel the specified link-local address (and restore to the default link-local address), in the interface configuration mode, use the command **no ipv6 address** *ipv6-address* **link-local**.

Specifying an IPv6 MTU

To specify an IPv6 MTU for an interface, in the interface configuration mode, use the following command:

ipv6 mtu *value*

- *value* – Specifies the MTU value. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (The max MTU may vary on different platforms.). If the Jumbo

Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Jumbo Frame.

To restore to the default MTU, in the interface configuration mode, use the command **no ipv6 mtu**.

Viewing IPv6 Configuration

To view IPv6 configuration of an interface, in any mode, use the following command:

show ipv6 interface [*interface-name*] [**prefix**]

- *interface-name* – Shows IPv6 configuration of the specified interface. If this parameter is not specified, the system will show all the interfaces which are enabled with IPv6.
- **prefix** – Shows IPv6 prefix of the specified interface.

Configuring IPv6 Neighbor Discovery Protocol

NDP (Neighbor Discovery Protocol) is a basic component of IPv6. This protocol operates on the link layer, and is responsible for looking for other nodes on the link, determining link layer addresses of other nodes, looking for available routers and maintaining information of other reachable nodes. Except for IPv4 ARP, router discovery and redirection functions of ICMP, NDP also provides more advanced functions, e.g., detection mechanism for unreachable neighbors.

StoneOS supports the following NDP configurations:

- Configuring DAD
- Specifying reachable time
- Configuring RA parameters
- Specifying a RA interval
- Specifying RA lifetime
- Specifying DRP

- Configuring RA suppress on LAN interfaces
- Adding/Deleting static IPv6 neighbor cache

Configuring DAD

This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving an NS packet, if any other host on the link finds the address of the NS requester is duplicated, it will send an NA (Neighbor Advertisement) packet advertising the address is already in use, and then the NS requester will mark the address as Duplicate, indicating the address is an invalid IPv6 address.

The configuration of DAD includes specifying NS packets attempts times and interval.

To specify NS packet attempts times for an interface, in the interface configuration mode, use the following command:

ipv6 nd dad attempts *times*

- *times* – Specifies NS packet attempts times. The value range is 0 to 20. The default value is 1. Value 0 indicates DAD is not enabled on the interface. If the system does not receive any NA response packet after sending NS packets for the attempts times, it will verify the IPv6 address is the unique available address.

To restore to the default attempts time, in the interface configuration mode, use the command **no ipv6 nd dad attempts**.

To specify an NS packet interval for an interface, in the interface configuration mode, use the following command:

ipv6 nd ns-interval *interval*

- *interval* – Specifies an interval for sending NS packets. The value range is 1000 to 3600000 milliseconds. The default value is 1000.

To restore to the default NS packet interval, in the interface configuration mode, use the command **no ipv6 nd ns-interval**.

Specifying Reachable Time

After sending an NS packet, if the interface receives acknowledge from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time. To configure reachable time, in the interface configuration mode, use the following command:

ipv6 nd reachable-time *time*

- *time* – Specifies reachable time. The value is 0 to 3600000 milliseconds. The default value is 30000.

To restore to the default value, in the interface configuration mode, use the command **no ipv6 nd reachable-time**.

Specifying RA Parameters

Routers send RA (Router Advertisement) packets periodically to advertise availability information and link/Internet parameters, including address prefix, recommended hop limit value, local MTU, auto-config type flag used by the node, DNS configuration options, etc.

Specifying a Hop Limit

Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface. To specify a hop limit, in the interface configuration mode, use the following command:

ipv6 nd hoplimit *number*

- *number* - Specifies the hop limit. The value range is 0 to 255. The default value is 64.

To restore to the default hop limit, in the interface configuration mode, use the following command:

no ipv6 nd hoplimit

Advertising MTU

You can specify whether to include MTU in RA packets sent on device interfaces and advertise to other routers. By default MTU is advertised. To specify to advertise MTU, in the interface

configuration mode, use the following command:

ipv6 nd adv-linkmtu

To specify not to advertise MTU, in the interface configuration mode, use the following command:

no ipv6 nd adv-linkmtu

Specifying DNS Configuration Options

You can specify to include DNS configuration options in RA packets sent on device interfaces and advertise to IPv6 hosts. IPv6 hosts that receive DNS configuration options can perform automatic DNS configuration. DNS configuration options include:

- RDNSS (Recursive DNS Server) configuration option: This option contains the IP addresses of recursive DNS servers. IPv6 hosts use recursive DNS servers for DNS name resolution.
- DNSSL (DNS Search List) configuration option: This option is a list of DNS suffix domain names. IPv6 hosts searches for short, unqualified domain names from this list when they perform DNS query .



Notes: DNS configuration options can only be configured on layer 3 interfaces.

To specify the RDNSS configuration option, in the interface configuration mode, use the following command:

ipv6 nd ra dns server {**suppress** | *ipv6-address***lifetime** {**infinite** | *rdnss-life*}}

- **suppress** - After this parameter is configured, RA packets sent on the specified interface no longer deliver the RDNSS configuration option.
- *ipv6-address* - Specifies the IP addresses of the recursive DNS server.
- **lifetime** {**infinite** | *rdnss-life*} - Specifies the valid time of the RDNSS configuration option. If **infinite** is specified, the option will be valid permanently. If *rdnss-life* is configured, the value range is 0 to 4294967295 seconds.

To cancel the specified RDNSS configuration option, in the interface configuration mode, use the following command:

no ipv6 nd ra dns server {**suppress** | *ipv6-address*}

To specify the DNSSL configuration option, in the interface configuration mode, use the following command:

ipv6 nd ra dns search-list {**suppress** | *list* **lifetime** {**infinite** | *dnssl-life*}}

- **suppress** - After this parameter is configured, RA packets sent on the specified interface no longer deliver the DNSSL configuration option.
- *list* - Specifies the list of DNS suffix domain names.
- **lifetime** {**infinite** | *dnssl-life*} - Specifies the valid time of the DNSSL configuration option. If **infinite** is specified, the option will be valid permanently. If *dnssl-life* is configured, the value range is 0 to 4294967295 seconds.

To cancel the specified DNSSL configuration option, in the interface configuration mode, use the following command:

no ipv6 nd ra dns search-list {**suppress** | *list*}

Specifying an Auto-config Type Flag

You can notify the connected hosts whether to obtain IP addresses and other configuration parameters via auto-config method (e.g., DHCP) by specifying an auto-config type flag in the RA packets. To specify to obtain IP addresses via auto-config, in the interface configuration mode, use the following command:

ipv6 nd managed-config-flag

To cancel the above configuration, in the interface configuration mode, use the command **no ipv6 nd managed-config-flag**.

To specify to obtain other configuration parameters other than IP addresses via auto-config, in the interface configuration mode, use the following command:

ipv6 nd other-config-flag

To cancel the above configuration, in the interface configuration mode, use the command **no ipv6 nd other-config-flag**.

Specifying an IPv6 Prefix and Parameters

RA packets will advertise the IPv6 prefix of interface. You can also specify the IPv6 prefix to be advertised, and configure its related parameters. In the interface configuration mode, use the following command:

ipv6 nd prefix {*ipv6-prefix/M* | **default**} [**no-advertise** | [*valid-lifetime preferred-lifetime* [**off-link** | **no-autoconfig**]]] | [**at** *valid-date* [*preferred-date* [**off-link** | **no-autoconfig**]]]

- *ipv6-prefix/M* – Specifies the IPv6 prefix and its length to be advertised.
- **default** – Specifies the default parameter for all the prefixes.
- **no-advertise** – Do not advertise IPv6 prefix in RA packets.
- *valid-lifetime* – Specifies valid lifetime for the IPv6 prefix. The value range is 0 to 4294967295 seconds. The default value is 2592000 (30 days).
- *preferred-lifetime* – Specifies the preferred lifetime for the IPv6 prefix. The default value is 604800 (7 days). The preferred lifetime should not be larger than the valid lifetime.
- **off-link** – Specifies off-link status for the prefix, i.e., the node that receives the RA packets will not write the prefix to its own routing table; if the prefix already exists in the routing table, the node will delete it.
- **no-autoconfig** – Advertises the host that receives the packets not to use the prefix as an IPv6 auto-configured address.
- *valid-date* – Specifies a valid date for the prefix, i.e., the prefix is only valid before the date. The format is MM/DD/YYYY HH:MM, such as 09/20/2010 09:30.
- *preferred-date* – Specifies a preferred valid date for the prefix. The format is MM/DD/YYYY HH:MM. This date must be earlier than the valid date.

To cancel the above IPv6 prefix parameters, in the interface configuration mode, use the following command:

no ipv6 nd prefix {*ipv6-prefix/M* | **default**}

Specifying a RA Interval

RA interval refers to the interval at which interface sends RA packets. This interval should not be larger than the lifetime of RA packets configured via CLI. To reduce the possibility of sending RA packets simultaneously with other routers on the same link, the system usually select a random number between the maximum and minimum interval as the actual RA interval. To configure a RA interval, in the interface configuration mode, use the following command:

ipv6 nd ra interval *max-interval* [*min-interval*]

- *max-interval* – Specifies the maximum interval. The value range is4 to 1800 seconds. The default value is 600.
- *min-interval* – Specifies the minimum interval. The value range is 3 to 1350 seconds. The minimum interval should not be larger than 75% of the maximum interval and must be larger than 3. If this parameter is not specified, the system will use 1/3 of the maximum interval as the minimum interval.

To restore to the default RA interval, in the interface configuration mode, use the following command:

no ipv6 nd ra interval

Specifying RA Lifetime

RA lifetime refers to the valid time during which the router is used as the default router of the interface. To specify RA lifetime, in the interface configuration mode, use the following command:

ipv6 nd ra lifetime *time*

- *time* – Specifies RA lifetime. The value range is 0 to 9000 seconds. The default value is 1800. Value 0 indicates the router is not the default route of the interface. For other values other than 0, the value should not be smaller than the RA interval.

To restore to the default RA lifetime, in the interface configuration mode, use the following command:

no ipv6 nd ra lifetime

Specifying DRP

DRP is the abbreviation for Default Router Preference. When a node receives an equal-cost route from different routers, it will select a preferred router based on DRP. To specify DRP, in the interface configuration mode, use the following command:

ipv6 nd router-preference {**high** | **medium** | **low**}

- **high** – Specifies DRP as high.
- **medium** – Specifies DRP as medium.
- **low** – Specifies DRP as low.

To restore to the default value, in the interface configuration mode, use the following command:

no ipv6 nd router-preference

Configuring RA Suppress on LAN Interfaces

By default FDDI interfaces with IPv6 unicast route configured will send RA packets automatically, and interfaces of other types will not send RA packets. To configure RA suppress on a LAN interface, in the interface configuration mode, use the following command:

ipv6 nd ra suppress

The above command will disable the interface to transfer RA packets. To re-enable the interface to transfer RA packets, in the interface configuration mode, use the following command:

no ipv6 nd ra suppress

Adding/Deleting a IPv6 Neighbor Cache Entry

IPv6 neighbor cache entries, key for unicast address connections, are a group of entries that store a single neighbor's information respectively. To view IPv6 neighbor cache entries in the system, in any mode, use the following command:

show ipv6 neighbor [**interface** *interface-name* | **slot** *slot-num* | **static** | **vrouter** *vr-name* | *ipv6-address* | **generic**]

- *interface-name* – Shows IPv6 neighbor cache entries of the specified interface.
- *ipv6-address* – Shows IPv6 neighbor cache entries of the specified address.
- **slot** *slot-num* – Shows IPv6 neighbor cache entries of the specified slot. Only for some devices (X series, K9180 and K6580 devices).
- **vrouter** *vr-name* – Shows IPv6 neighbor cache entries of the specified VRouter.
- **static** – Shows static IPv6 neighbor cache entries.
- **generic** – Shows statistics of neighbor cache entries.

To add a static IPv6 cache entry, in the global configuration mode, use the following command:

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* – Specifies the IPv6 address.
- *interface-name* – Specifies the name of interface.
- *mac-address* – Specifies the MAC address corresponding to the IPv6 address.

To delete a static IPv6 cache entry, in the global configuration mode, use the following command:

clear ipv6 neighbor [*ipv6-address*] [**vrouter** *vr-name*]

- *ipv6-address* – Deletes the IPv6 neighbor entry of the specified address.
- **vrouter** *vr-name* – Deletes the IPv6 neighbor cache entries of the specified VRouter.

IPv6 System Management

StoneOS supports FTP, TFTP, HTTP and HTTPS protocols for IPv6, i.e., it allows you to visit FTP and TFTP servers by IPv6 addresses; besides it also allows you to visit its WebUI by the IPv6 address. HTTP and HTTPS services for IPv4 and IPv6 share the same protocol port number.

You can export the following objects to the IPv6 address of an FTP or TFTP server: configuration file, system firmware, license, partial logs (alarm, event, security), PKI certificate, SSL VPN user-host binding list and URL database. In the execution mode, use the following commands:

- To export the configuration file: **export configuration** {{**startup** | **backup**} *number*} **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address* [**vrouter** *vrouter-name*]} [*file-name*]
- To export the system firmware: **export image** *name* **to** {**ftp server** *ipv6-address* [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the license: **export license** *name* **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export logs: **export log** { **event** | **security**} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the PKI certificate: **export pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the SSL VPN user-host binding list: **export scvpn user-host-binding to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]
- To export the URL database: **export urlfilter-database to** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} [*file-name*]

You can import the following objects from the IPv6 address of an FTP or TFTP server: application signature database, configuration file, custom firmware for SSL VPN and WebAuth webpage, system firmware, ISP file, license, PKI certificate, SSL VPN user-host binding list and URL database. In the execution mode, use the following commands:

- To import the application signature database: **import application-signature from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the configuration file: **import configuration from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the customized picture for SSL VPN or WebAuth webpage: **import customize** {**scvpn • To import the license:** | **webauth**} **from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the system firmware: **import image from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the ISP file: **import ispfile from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the license: **import license from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the PKI license: **import pki** *trust-domain-name* {**cacert** | **cert** | **pkcs12** *password*} **from**{**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*
- To import the SSL VPN user-host binding list: **import scvpn user-host-binding from** {**ftp server** *ipv6-address* [**user** *username* **password** *string*] | **tftp server** *ipv6-address*} *file-name*



Tip: For more detailed information about the command parameters, see related chapters.

Configuring IPv6 SNMP

StoneOS allows you to view the general IPv6-related MIB information via SNMP. The configuration of SNMP IPv6 includes:

- Configuring an IPv6 management host
- Configuring an IPv6 trap destination host
- Creating an SNMPv3 user (IPv6 remote management host)



Tip: For more information about the SNMP configuration, see "Configuring SNMP" of "System Management".

Configuring an IPv6 Management Host

To configure an IPv6 management host, in the global configuration mode, use the following command:

snmp-server ipv6-host {*host-name* | *ipv6-address*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *host-name* | *ipv6-address* – Specifies hostname or IPv6 address of the management host.
- **version** [*1* | *2c*] – Specifies the SNMP version as SNMP v1 or SNMP v2C.
- **community** *string* – Specifies the community string. The length is 1 to 31 bits. The community string is a password between the management and proxy processes; therefore, SNMP packets with inconsistent community strings will be dropped. This parameter only applies for SNMP v1 and v2C.
- **ro** | **rw** – Specifies a privilege for the community string. ro stands for read-only, and such a community string can only read information in the MIB; **rw** stands for read-write, and such a community string can not only read but also modify information in the MIB. This parameter is

optional. By default the privilege is **ro**.

- **version** *3* – Specifies the SNMP version as SNMP v3.

To delete the specified IPv6 management host, in the global configuration mode, use the command **no snmp-server ipv6-host** {*host-name* | *ipv6-address*}.

Configuring an IPv6 Trap Destination Host

You can configure an IPv6 destination host that is used to receive SNMP trap packets. To configure an IPv6 trap destination host, in the global configuration mode, use the following command:

snmp-server ipv6-trap-host *ipv6-address* [**ipv6-source-ip** *ipv6-address*] {**version** {1 | 2c} **community** *string* | **version 3 user** *user-name* **engineID** *string* } [**port** *port-number*]

- **ipv6-trap-host***ipv6-address* – Specifies the hostname or IPv6 address of the trap destination host.
- **ipv6-source-ip** *ipv6-address* - Specifies the source IPv6 address that sends SNMP trap packets.
- **version** {1 | 2c} – Specifies to send trap packets via SNMPv1 or SNMPv2C.
- **community** *string* – Specifies the community string for SNMPv1 or SNMPv2C.
- **version 3** – Specifies to send trap packets via SNMPv3.
- **user** *user-name* – Specifies the SNMPv3 username.
- **engineID** *string* – Specifies engine ID of the trap destination host.
- **port** *port-number* – Specifies the port number of the destination host that receives trap packets. The value range is 1 to 65535. The default value is 162.

To delete the specified trap destination host, in the global configuration mode, use the command **no snmp-server ipv6-trap-host** *ipv6-address* [**ipv6-source-ip**].



Notes: In the HA environment, the backup device does not synchronize with the source IP address (**ipv6-source-ip**) configured in the primary device for sending SNMP trap packets. To specify the source IPv6 address for the added IPv6 trap host to send SNMP trap packets, you can use the **snmp-server ipv6-trap-host** *ipv6-address* **ipv6-source-ip** *ipv6-address* command in the backup device.

Creating an SNMPv3 User

To configure an SNMPv3 user, in the global configuration mode, use the following command:

snmp-server user *user-name* **group** *group-name* **v3** {**remote** *remote-ip* | **ipv6-remote** *ipv6-address*} [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* – Specifies the username. The length is 1 to 31 characters.
- **group** *group-name* – Specifies a user group defined in the system for the user.
- **remote** *remote-ip* – Specifies the IP address of the remote management host.
- **ipv6-remote** *ipv6-address* – Specifies the IPv6 address of the remote management host.
- **auth-protocol** {**md5** | **sha**} – Specifies the authentication protocol as MD5 or SHA. If this parameter is not specified, the default security level will be no authentication and no encryption.
- *auth-pass* – Specifies the authentication password. The length is 8 to 40 characters.
- **enc-protocol** {**des** | **aes**} – Specifies the encryption protocol as DES or AES.
- *enc-pass* – Specifies the encryption password. The length is 8 to 40 characters.

The system supports up to 25 users. To delete the specified user, in the global configuration mode, use the command **no snmp-server user** *user-name*.

Configuring IPv6 Debugging

System supports ping to an IPv6 address. To ping an IPv6 address, in any mode, use the following command:

ping ipv6 *ipv6-address* [**count** *number*] [**size** *number*] [**source** {*ipv6-address* | *interface-name*}] [**timeout** *time*] [**vrouter** *vr-name*]

- *ipv6-address* – Specifies the destination address to which ping packets are sent.
- **count** *number* – Specifies the number of ping packets. The value range is 1 to 65535. The default value is 5.
- **size** *number* – Specifies the size of ping packets. The length is 28 to 65535 bytes.
- **source** {*ipv6-address* | *interface-name*} – Specifies the source address where ping packets originate. It can be either an IP address or an interface.
- **timeout** *time* – Specifies timeout for ping packets. The value range is 0 to 3600 seconds. The default value is 0, i.e., never timeout.
- **vrouter** *vr-name* – Specifies the VRouter that sends ping packets.

Configuring IPv6 Routing

StoneOS supports IPv6 DBR, SBR, SIBR and DIBR. To configure an IPv6 static route, you need to enter the VRouter configuration mode. In the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of VRouter, and enter the VRouter configuration mode.

Configuring an IPv6 DBR Entry

To add an IPv6 DBR entry, in the VRouter configuration mode, use the following command:

ipv6 route *ipv6-address/M* {**null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]} [*distance-value*] [**name** *name*][**weight** *weight-value*] [**description***description*] [**track***track-name*]

- *ipv6-address/M* – Specifies the segment of the destination address.
- **null0**- Specifies the Null0 interface.
- *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*] – Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* – Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* – Specifies the name of router.
- *weight-value* – Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description***description* - Specifies the description of router. The range is 1 to 63.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add multiple DBR entries.

To delete the specified IPv6 DBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route *ipv6-address/M* { **null0** | *ipv6-address* | **vrouter** *vrouter-name* | *interface-name* [*ipv6-address*]}

Configuring an IPv6 SBR Entry

To add an IPv6 SBR entry, in the VRouter configuration mode, use the following command:

ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*] [**description***description*] **track***track-name*

- *ipv6-address/M* – Specifies the segment of the source address.
- **null0** – Specifies the Null0 interface.
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* – Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* – Specifies the name of router.
- *weight-value* – Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description***description* - Specifies the description of router. The range is 1 to 63.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add multiple SBR entries.

To delete the specified IPv6 SBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route source *ipv6-address/M* { **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name*}

Configuring an IPv6 SIBR Entry

To add an IPv6 SIBR entry, in the VRouter configuration mode, use the following command:

ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* | *interface-name*| **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*] [**description***description*] [**track***track-name*

- *interface-name* – Specifies the ingress interface of the routing entry.
- **null0**- Specifies the Null0 interface.
- *ipv6-address/M* – Specifies the segment of the source address.
- *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* – Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* – Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* – Specifies the name of router.
- *weight-value* – Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description***description* - Specifies the description of router. The range is 1 to 63.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add multiple SIBR entries.

To delete the specified IPv6 SIBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route source in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* }

Configuring an IPv6 DIBR Entry

To add an IPv6 DIBR entry, in the VRouter configuration mode, use the following command:

ipv6 route in-interface*interface-name ipv6-address/M* { **null0** | *ipv6-address* | *interface-name*| **vrouter** *vrouter-name* } [*distance-value*] [**name** *name*] [**weight** *weight-value*] [**description***description*] [**track***track-name*]

- *interface-name* – Specifies the ingress interface of the routing entry.
- **null0**- Specifies the Null0 interface.
- *ipv6-address/M* – Specifies the segment of the source address.
- *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* – Specifies the next hop which can be a gateway address (*ipv6-address*) , VRouter（**vrouter** *vrouter-name*） or an interface (*interface-name*).
- *distance-value* – Specifies the administration distance of the route. This parameter is used to determine the precedence of the route. The smaller the value is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route is invalid.
- *name* – Specifies the name of router.
- *weight-value* – Specifies the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
- **description***description* - Specifies the description of router. The range is 1 to 63.
- **track***track-name* – Specify the name of a created track object. When the track fails, the route will be invalid.

Repeat the above command to add multiple DIBR entries.

To delete the specified IPv6 DIBR entry, in the VRouter configuration mode, use the following command:

no ipv6 route in-interface *interface-name ipv6-address/M* { **null0** | *ipv6-address* | *interface-name* | **vrouter** *vrouter-name* }

Viewing IPv6 Routing Information

To view IPv6 routing information, in any mode, use the following commands:

- To view DBR information: **show ipv6 route static** [**vrouter** *vr-name*]
- To view SBR information: **show ipv6 route source** [**vrouter** *vr-name*]
- To view SIBR information: **show ipv6 route source in-interface** *interface-name*
- To view connected route information: **show ipv6 route connected** [**vrouter** *vr-name*]
- To view routing information of the specified destination address: **show ipv6 route** *ipv6-address/[M]* [**vrouter** *vr-name*]
- To view IPv6 routes statistics: **show ipv6 route summary** [**vrouter** *vr-name*]
- To view IPv6 FIB information: **show ipv6 fib** [**source** | **source in-interface** *interface-name* | *ipv6-address/[M]* | **summary**] [**vrouter** *vr-name*]

Configuring RIPng

RIPng (RIP next generation) is an extension to the RIP-2 in IPv4. Most concepts of RIP are applicable to RIPng.

Compared with RIP, RIPng modifies following items:

- UDP port: Uses the UDP port 521 to send and receive routing information.
- Multicast address: Uses FF02::9 as the multicast address of the RIPng router in the local-link address range.
- Prefix length: The destination address uses prefix length of 128 bits.
- Next-hop address: Use the 128 bits IPv6 address.

- Source address: Uses the link-local address FE80::/10 as the source address to send RIPng routing information update packets.

RIPng configuration includes basic options, redistribute, passive IF, network and distance. Besides, you also need to configure RIP parameters for different interfaces, including split horizon and poison reverse.

Basic Options

The basic options of RIPng configuration include metric, distance, information originate and timer (update interval, invalid time, and flush time). You can configure RIPng protocol for different VRouter respectively. The basic options of RIPng must be configured in the RIPng routing configuration mode. To enter the RIPng routing configuration mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

ipv6 router rip (enters the RIPng routing configuration mode, and at the same time enables the RIPng function on the device. Each RIPng process is individual and you can create one RIPng process in a VRouter.)

To disable the RIPng function, in the VRouter configuration mode, use the command **no ipv6 router rip**.

Specifying a Default Metric

RIPng measures the distance to the destination network by counting the number of hops. This distance is known as metric. The metric from a router to a directly connected network is 1, and increments by 1 for every additional router between them. The maximum metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed. To specify the default metric, in the RIPng routing configuration mode, use the following command:

default-metric *value*

- *value* – Specifies the default metric value. The value range is 1 to 15. If no value is specified, the value of 1 will be used.

To restore the metric value to 1, in the RIPng routing configuration mode, use the command **no default-metric**.

Specifying a Default Distance

To specify the default distance for RIPng, in the RIPng routing configuration mode, use the following command:

distance *distance-value*

- *distance-value* – Specifies the default administration distance value. The value range is 1 to 255. If no value is specified, the value of 120 will be used.

To restore to the distance value of 120, in the RIPng routing configuration mode, use the command **no distance**.

Specifying a Timer

The timers you can configure for RIPng include update interval, invalid time, holddown time and flush time, as described below:

- Update interval: Specifies the interval at which all RIPng routes will be sent to all the neighbors. The default value is 30 seconds.
- Invalid time: If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The default value is 180 seconds.
- Flush time: StoneOS will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the flush time ends, it will be deleted from the RIPng information database. The default value is 240 seconds.

To modify the above three timers, in the RIPng routing configuration mode, use the following command:

timers basic *interval-time invalid-time flush-time*

- *interval-time* – Specifies the update interval time. The value range is 0 to 16777215 seconds. The default value is 30.
- *invalid-time* – Specifies the invalid time. The value range is 1 to 16777215 seconds. The default value is 180.
- *flush-time* – Specifies the flush time. The value range is 1 to 16777215 seconds. The default value is 120.

To restore to the default timer value, in the RIPng routing configuration mode, use the command **no timers basic**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers with RIPng enabled. By default RIPng will not redistribute the default route. To configure the default information originate, in the RIPng routing configuration mode, use the following commands:

- Redistribute: **default-information originate**
- Do not redistribute: **no default-information originate**

Configuring Redistribute

RIPng allows you to introduce information from other routing protocols (IPv6 BGP, connected, static, OSPFv3 and IS-IS) and redistribute the information. To configure the redistribute metric, in the RIP routing configuration mode, use the following commands:

redistribute {**bgp** | **connected** | **static** | **ospf** | **isis**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf** – Specifies the protocol type: IPv6 BGP (**bgp**), connected route (**connected**), static route (**static**) , OSPFv3 (**OSPF**) or IS-IS (**isis**).
- **metric** *value* – Specifies a metric value for the redistribute. The value range is 1 to 15. If the value is not specified, the system will use the default metric configured by the command **default-metric** *value*.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the RIPng routing configuration mode, use the command **no redistribute** {**bgp** | **connected** | **static** | **ospfv3** | **isis**}.

Configuring a Network

You can configure some networks so that only the interfaces within the specified networks can receive and send RIPng update. To configure a network, in the RIPng routing configuration mode, use the following command:

network {*interface-name* | *X:X:X:X::X/M*}

- *interface-name* – Specified the interface name. This interface is located at the network that you want to specify.
- *X:X:X:X::X/M* – Specifies the IPv6 address of the network.

Repeat the above command to configure more networks.

To delete the specified network, in the RIPng routing configuration mode, use the command **no network** {*interface-name* | *X:X:X:X::X/M*}.

Configuring a Passive IF

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the RIPng routing configuration mode, use the following command:

passive-interface *interface-name*

- *interface-name* – Specifies the interface as a passive interface.

Repeat the above command to configure multiple passive interfaces.

To cancel the specified passive interface, in the RIP routing configuration mode, use the command **no passive-interface** *interface-name*.

Configuring Split Horizon

When using split horizon, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent. To enable or disable split horizon, in the interface configuration mode, use the following commands:

- Enable: **ipv6 rip split-horizon**
- Disable: **no ipv6 rip split-horizon**

Configuring Poison Reverse

When using poison reverse, RIPng will send the poison messages to all neighbor routers, including the router whose sends the poison message, and will not obey the split horizon rule. This poison message advertise the invalid route. To configure the poison reverser function , use the following command in the interface configuration mode:

- Enable: **ipv6 rip poison-reverse**
- Disable: **no ipv6 rip poison-reverse**

Viewing RIPng Information

To view the RIPng information, in any mode, use the following command:

show ipv6 rip

To view the RIPng route information, in any mode, use the following command:

show ip route rip [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the RIP router information of the specified VRouter.

When a Hillstone device is running RIPng, it will own a RIPng route database which can store all routing entries for all the reachable networks. The routing entry information includes destination address, next hop, metric, source, and timer information. To view the RIPng database information, in any mode, use the following command:

show ipv6 rip database [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – Shows the RIPng information of the specified VRouter.

Configuring OSPFv3

OSPFv3 is the third version of Open Shortest Path First and it mainly provides the support of IPv6.

The similarities between OSPFv3 and OSPFv2 are as follows:

- Both protocols use 32 bits Router ID and Area ID
- Both protocols use the Hello packets, DD (database description) packets, LSR (link state request) packets, LSU (link state update) packets, and LSAck (link state acknowledgment) packets.
- Both protocols use the same mechanisms of finding neighbors and establishing adjacencies.
- Both protocols use the same mechanisms of LSA flooding and aging

The differences between OSPFv3 and OSPFv2 are as follows:

- OSPFv3 runs on a per-link basis and OSPFv2 is on a per-IP-subnet basis.
- OSPFv3 supports multiple instances per link.
- OSPFv3 identifies neighbors by Router ID, and OSPFv2 identifies neighbors by IP address.

You can configure the OSPFv3 protocol for each VRouter respectively. Configuring OSPFv3 includes the following options:

- Configuring a Router ID
- Configuring the virtual link for an area
- Configuring the default metric
- Configuring the default administrative distance
- Configuring the default information originate

- Configuring the interface area and instance
- Configuring redistribute
- Configuring a passive interface
- Configuring the timer for an interface
- Configuring the router priority for an interface
- Configuring the link cost for an interface
- Configure the MTU check for an interface
- Disabling or Enabling OSPFv3
- Configure the network type for an interface
- Configuring encryption and authentication for an area
- Configuring encryption and authentication on an interface

The basic options of OSPFv3 protocol must be configured in the OSPFv3 routing mode. To enter the OSPFv3 routing mode, in the global configuration mode, use the following commands:

ip vrouter *vrouter-name* (enters the VRouter configuration mode)

ipv6 router ospf [*process-id*] (enters the OSPFv3 routing configuration mode, and at the same time enables OSPFv3 on the device.)

- *process-id* - Specifies the OSPFv3 process ID. If not specified, process 1 will be used by default. Each OSPFv3 process is individual, and has its own link state database and the related OSPFv3 routing table. Each VRouter supports up to four OSPFv3 processes, and multiple processes maintain a routing table together. Each OSPFv3 process can redistribute OSPFv3 routes from other OSPFv3 processes, as well as routes from other IPv6 routing protocols (static, connected, IPv6BGP, RIPng and ISISv6).

When specifying multiple OSPFv3 processes, note the following matters:

- When multiple OSPFv3 processes generate routes with the same destination network, if their administrative distances and metrics are the same, the process that generates the route first will be prioritized. Besides, ECMP is not supported across multiple OSPFv3 processes.
- When other routing protocols attempt to redistribute OSPFv3 routes, only the routing information of process 1 will be redistributed.

To disable OSPFv3, in the VRouter configuration mode, use the command **no ipv6 router ospf**.

Configuring a Router ID

Each router running OSPFv3 protocol must be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPFv3 domain, represented in the form of an IP address. To configure a Router ID for the Hillstone device that is running OSPFv3 protocol, in the OSPF routing mode, use the following command:

router-id *A.B.C.D* [**local**]

- *A.B.C.D* – Specifies the Router ID used by OSPFv3 protocol, in form of an IP address.
- **local** - Specifies the Router ID as a local configuration. This kind of configuration is applicable to HA Peer mode, and is not synchronized to HA configuration. By default the router ID is not a local configuration.

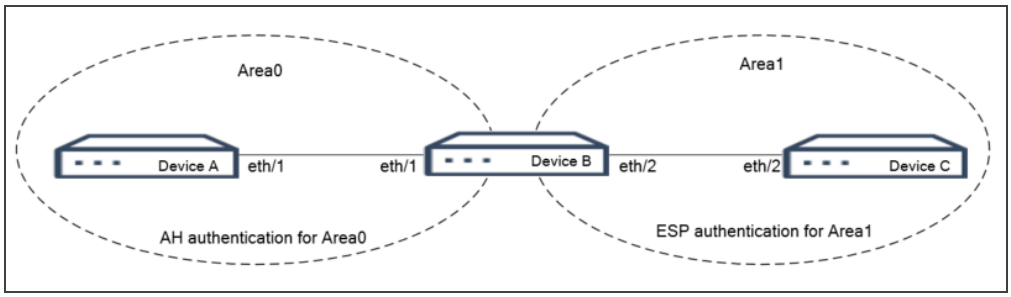
Enabling Encryption and Authentication for an Area and on an Interface

OSPFv3 can use IPsec Authentication Header (AH) and IPSec Encapsulating Security Payload (ESP) header capabilities to achieve encryption and authentication between neighbor devices. You can enable encryption and authentication for an OSPFv3 area and on an interface within the OSPFv3 area.

- When you need to protect all OSPFv3 packets in an area, you can enable encryption and authentication for this area. In this case, all devices in this area needs to be configured the same encryption and authentication policy, including the authentication method, SIP value,

authentication algorithm, authentication key, etc.

- When you need to protect OSPFv3 packets of a specified interface within an area, you can enable encryption and authentication on this interface. In this case, the interface of the directly connected neighbor needs to be configured with the same encryption and authentication policy, including the authentication method, SIP value, authentication algorithm, authentication key, etc.



Take note of the following rules for the Cryptographic Authentication function of the OSPFv3 route:

- If the Cryptographic Authentication function is enabled in an area and disabled for all interfaces in this area, the encryption and authentication policy of the area is applied to these interfaces.
- If the Cryptographic Authentication function is enabled for both an interface and the area where the interface belongs and the authentication types of the interface and the area are different and the authentication method of the interface is neither AH NULL nor ESP NULL, the encryption and authentication policy of the interface takes effect.
- If the Cryptographic Authentication function is enabled for the area where the interface belongs and the authentication types of the interface and the area are different and the authentication method of the interface is NULL, the encryption and authentication policy of the area is applied to the interface. For example, if the area where the interface belongs is configured with AH authentication and the interface is configured with ESP NULL, the encryption and authentication policy of this area is applied to this interface.

- If the Cryptographic Authentication function is enabled for the area where the interface belongs and the authentication types of the interface and the area are the same but the authentication method of the interface is NULL, no encryption and no authentication is performed on packets on this interface. For example, if the area where the interface belongs is configured with ESP authentication and the interface is configured with ESP NULL, no encryption and no authentication are performed on packets on this interface.
- Both the interface and the area where the interface belongs can be configured with one authentication method.

Enabling AH Authentication for an Area

To enable AH authentication for an area, use the following command in OSPFv3 routing mode:

area { *id* | *A.B.C.D* } **authentication ipsec spi***spi-id* {**md5** | **sha1**} *authentication-key*

- *id* | *A.B.C.D* − Specifies the area ID of OSPFv3, which can be a 32-bit digital number, or an IP address.
- *spi-id* − Specifies the Security Parameter Index (SPI) value. Valid values: 256 to 4294967295. The receiver authenticates received packets by using the SPI value.
- *authentication-key* − Specifies the authentication key in the hexadecimal string format in the OSPFv3 area. The authentication algorithms include MD5 and SHA1.

In OSPFv3 routing mode, use the **no area** { *id* | *A.B.C.D* } **authentication ipsec spi***spi-id* command to disable AH authentication for a specified area.

Enabling AH Authentication on an Interface

To enable AH authentication on an interface, use the following command in interface configuration mode:

ipv6 ospf authentication {**ipsec spi***spi-id* {**md5** | **sha1**} *authentication-key* | **null**}

- *spi-id* – Specifies the SPI value. Valid values: 256 to 4294967295. The receiver authenticates received packets by using the SPI value.
- *authentication-key* – Specifies the authentication key of the corresponding authentication algorithm in the hexadecimal string format. The authentication algorithms include MD5 and SHA1.
- **null** – Specifies that no AH authentication is enabled on the interface., which is applicable to the scenario where AH authentication is enabled for an area but is disabled for packets of the interface within this area.

In interface configuration mode, use the **no ipv6 ospf authentication** {**ipsec spi***spi-id* | **null**} command to cancel the configuration.

Enabling ESP Authentication for an Area

To enable ESP authentication for an area, use the following command in OSPFv3 routing mode:

area { *id* | *A.B.C.D* } **encryption ipsec spi***spi-id***esp** {**3des***encryption-key* | **aes-cbc** {**128** | **192** | **256**} *encryption-key* | **des***encryption-key* | **null**} {**md5** | **sha1**} *authentication-key*

- *id* | *A.B.C.D* – Specifies the area ID of OSPFv3, which can be a 32-bit digital number, or an IP address.
- *spi-id* – Specifies the SPI value. Valid values: 256 to 4294967295. The receiver authenticates received packets by using the SPI value.
- *encryption-key* – Specifies the encryption key of the corresponding encryption algorithm in the hexadecimal string format. The encryption algorithms include DES, 3DES, AES-128, AES-192, and AES-256. **null** indicates that no encryption algorithm is specified and ESP provides only the authentication function.
- *authentication-key* – Specifies the authentication key of the corresponding authentication algorithm in the hexadecimal string format. The authentication algorithms include MD5 and SHA1.

In OSPFv3 routing mode, use the **no area** { *id* | *A.B.C.D* } **encryption ipsec spi***spi-id* command to disable ESP encryption and authentication of a specified area.

Enabling ESP Authentication on an Interface

To enable ESP authentication on an interface, use the following command in interface configuration mode:

ipv6 ospf encryption { **ipsec spi***spi-id***esp** {**3des***encryption-key* | **aes-cbc** {**128** | **192** | **256**} *encryption-key* | **des***encryption-key* | **null**} {**md5** | **sha1**} *authentication-key* | **null**}

- *spi-id* – Specifies the SPI value. Valid values: 256 to 4294967295. The receiver authenticates received packets by using the SPI value.
- *encryption-key* – Specifies the encryption key of the corresponding encryption algorithm in the hexadecimal string format. The encryption algorithms include DES, 3DES, AES-128, AES-192, and AES-256. **null** indicates that no encryption algorithm is specified and ESP provides only the authentication function.
- **null** – Specifies that no ESP authentication is enabled on the interface., which is applicable to the scenario where ESP authentication is enabled for an area but is disabled for packets of the interface within this area.

In interface configuration mode, use the **no ipv6 ospf encryption** {**ipsec spi***spi-id* | **null**} command to cancel the configuration.

Configuring the Virtual Link for an Area

Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. To configure virtual link parameters and its timer parameters, in the OSPFv3 routing mode, use the following command:

area { *id* | *A.B.C.D* } **virtual-link** *A.B.C.D*

- *id | A.B.C.D* – Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
- *A.B.C.D* – Specifies the Router ID that is used as a virtual link router.

Configuring the Default Metric

The default metric configured here will take effect if the redistributed route has no configured metric. To specify the default metric for OSPFv3, in the OSPFv3 routing configuration mode, use the following command:

default-metric *value*

- *value* – Specifies the default metric value. The value range is 1 to 16777214.

To restore to the original metric value, in the OSPFv3 routing configuration mode, use the command **no default-metric**.

Configuring the Default Administrative Distance

You can configure the default administrative distance according to the route type. To configure the default administrative distance, in the OSPFv3 routing configuration mode, use the following command:

distance {*distance-value* | **ospf** [**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- *distance-value* – You can configure the default administrative distance according to the route type. To configure the default administrative distance, in the OSPFv3 routing configuration mode, use the following command:
- **intra-area** *distance-value* – Specifies the administrative distance value of the intra-area route. The default value is 110 and the value ranges from 1 to 255.
- **inter-area** *distance-value* – Specifies the administrative distance value of the inter-area route. The default value is 110 and the value ranges from 1 to 255.

- **external** *distance-value* – Specifies the administrative distance value of the external route. The default value is 110 and the value ranges from 1 to 255.

To restore to the value of 110, in the OSPFv3 routing configuration mode, use the command **no distance ospf**.

Configuring the Default Information Originate

You can specify if the default route will be redistributed to other routers. To configure the default information originate, in the OSPFv3 routing configuration mode, use the following command:

default-information originate [**always**] [**type** {1 | 2}] [**metric** *value*]

- **always** – When using **always**, OSPFv3 of this router unconditionally generates and redistributes the default route. If there is no default route in the current router, it will generate a route whose next hop is the router itself. Without using always, the router will not redistribute the default route if it has no one.
- **type** {1 | 2} – Specifies the type of the external route associated with the default route that is sent to OSPFv3 routing area. 1 refers to type1 external route, 2 refers to type2 external route.
- **metric** *value* – Specifies the metric value for the default route that will be sent. If no default metric value is specified by this command or by the command **default-metric** *value*, then OSPFv3 will use the value of 20. The value range is 0 to16777214.

To restore to the value of 20, in the OSPFv3 routing configuration mode, use the command **no default-information originate**.

Configuring the Interface Area and Instance

To specify the area and instance that the interface belongs to, in the OSPFv3 routing configuration mode, use the following command:

ipv6 ospf *process-id* **area** { *A.B.C.D* | *id*} {**instance** *id*}

- *process-id* – Specifies the ID of the OSPFv3 process that the interface belongs to. The default value is 1.
- **area** { *A.B.C.D* | *id*} – Specifies the area ID that the interface belongs to. The area ID is in form of a 32-bit digital number, or an IP address.
- **instance** *id* – Specifies the instance ID that the interface belongs to. To establish the neighbor relationship, interfaces must belong to the same instance. The value ranges from 0 to 255. The default value is 0.

To cancel the area and instance configuration, in the OSPFv3 routing configuration mode, use the command **no ipv6 ospf area** { *A.B.C.D* | *id*}.

Configuring Redistribute

OSPFv3 allows you to introduce information from other routing protocols (IPv6 BGP, connected, static , IS-IS and RIPng) and redistribute the information. You can set the metric and type of the external route for the redistribute. To configure the redistribute, in the OSPFv3 routing configuration mode, use the following command:

redistribute {**bgp** | **connected** | **static** | **isis** |**ripng** | **ospfv3***process-id*} [**type** {**1** | **2**}] [**metric** *value*] [**route-map***name*]

- **bgp** | **connected** | **static** | **isis** | **ripng** – Specifies the protocol type which can be IPv6 BGP (**bgp**), connected route (connected), static route (**static**) or OSPFv3 (**OSPF**).
- **ospfv3** *process-id* - Specifies the process ID of the redistributed OSPFv3 route.
- **type** {**1** | **2**} – Specifies the type of the external route. 1 refers to type1 external route, 2 refers type2 external route.
- **metric** *value* – Specifies a metric value for the redistribute. The value range is 0 to 16777214. If the value is not specified, the system will use the default OSPFv3 metric configured by the command **default-metric** *value*.

- **route-map***name* - Specifies the route map used to filter redistribute information. For more information about route map, see "Route Map" on Page 541.

Repeat the above command to redistribute a different type of routes.To cancel the redistribute of specified route, in the OSPF routing configuration mode, use the command

no redistribute {**bgp** | **connected** | **static** | **isis** | **rip**}.

Configuring a Passive Interface

You can configure some interfaces to only receive but not to send data. This kind of interfaces is known as a passive interface. To configure a passive interface, in the interface configuration mode, use the following command:

ipv6 ospf passive

Repeat the above command to configure more passive interfaces.

To cancel the specified passive interface, in the interface configuration mode, use the command **no ipv6 ospf passive**.

Configuring the Timer for an Interface

There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets.

To specify the interval for sending Hello packets for an interface, in the interface configuration mode, use the following command:

ipv6 ospf hello-interval *interval*

- *interval* – Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. If the OSPFv3 interface chooses the point-to-multipoint network type, the default value is 30.

To restore to the default interval, in the interface configuration mode, use the command **no ipv6 ospf hello-interval**.

If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent

routers. To configure the dead interval for an interface, in the interface configuration mode, use the following command:

ipv6 ospf dead-interval *interval*

- *interval* – Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If the OSPFv3 interface chooses the point-to-multipoint network type, the default value is 120.

To restore to the default dead interval, in the interface configuration mode, use the command **no ipv6 ospf dead-interval**.

To specify the LSA retransmit interval for an interface, in the interface configuration mode, use the following command:

ipv6 ospf retransmit-interval *interval*

- *interval* – Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5.

To restore to the default retransmit interval, in the interface configuration mode, use the command **no ipv6 ospf retransmit-interval**.

ipv6 ospf transmit-delay *interval*

- *interval* – Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.

To restore to the default transmit delay, in the interface configuration mode, use the command **no ipv6 ospf transmit-delay**.

Configuring the Router Priority for an Interface

The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and send the received link information. To specify the router priority for an interface, in the interface configuration mode, use the following command:

ipv6 ospf priority *level*

- *level* – Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router. If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.

To restore to the default priority, in the interface configuration mode, use the command **no ipv6 ospf priority**.

Configuring the Link Cost for an Interface

You can use one of the following methods to configure the link cost for an interface:

- Specify the cost directly
- Specify the bandwidth reference value and OSPFv3 computes the cost automatically based on the bandwidth reference value

To specify the cost directly, use the following command in the interface configuration mode:

ipv6 ospf cost *cost-value*

- *cost-value* – Specifies a cost value. The value range is 0 to 16777214.

To cancel the configuration, use **no ipv6 ospf cost**.

To compute the cost according to the specified bandwidth reference value, specify the bandwidth of the interface in the OSPFv3 configuration mode:

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – Specifies the bandwidth reference value. The unit is Mbps, and the default value is 100. The value ranges from 1 to 4294967. The cost equals to the value of dividing interface bandwidth by the bandwidth reference value.

To restore the bandwidth reference value to the default value, use **no auto-cost reference-bandwidth**.

Configuring the MTU Check for an Interface

OSPFv3 uses DBD packets to check whether the interface MTU set is matched or not between the neighbors. If the MTU set is not matched, the neighbors cannot establish the adjacency. You can modify the MTU set to solve this issue. For the interfaces whose MTU set cannot be modified, you can ignore the MTU check.

To ignore the MTU check, use the following command in the interface configuration mode:

ipv6 ospf mtu-ignore

Use the no form to restore the MTU check:

no ipv6 ospf mtu-ignore

Configuring the Network Type for an Interface

In OSPFv3, the network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. To configure the network type of an interface, in the interface configuration mode, use the following command:

ipv6 ospf network {**point-to-point** | **point-to-multipoint**}

- **point-to-point** – Specifies the network type of an interface as the point-to-point type.
- **point-to-multipoint** - Specifies the network type of an interface as the point-to-multipoint type.

To set the network type as the default broadcast type, use the following command:

no ipv6 ospf network

Disabling or Enabling OSPFv3

Disable OSPFv3 protocol on interface, in the interface configuration mode, use **ipv6 ospf shutdown**.

Enable OSPFv3 protocol on interface, in the interface configuration mode, use **no ipv6 ospf shutdown**.

Viewing OSPFv3 Information

To view the OSPFv3 routing information of the Hillstone device, in any mode, use the following command:

show ipv6 ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* - Shows the OSPF route information of the specified VRouter name. If the VRouter is not specified, system will only show the protocol information of the trust-vr.
- **process** *process-id* - Shows the protocol information of the OSPFv3 with the specified process ID. If the process ID is not specified, system will show the protocol information of all OSPFv3 processes in the VRouter.

To view the OSPFv3 protocol’ s database information of the Hillstone device, in any mode, use the following commands:

show ipv6 ospf database

show ipv6 ospf database {**inter-router** | **external** | **network** | **router** | **inter-prefix** | **link** | **intra-prefix**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **inter-router** – Shows the LSAs originated by ABRs and these LSAs are flooded throughout the LSA's associated area. Each inter-router LSA describes a route to ASBR.
- **external** – Shows the LSAs originate by ASBRs and these LSAs are flooded throughout the AS (except Stub and NSSA areas). Each external LSA describes a route to another AS.
- **network** – Shows the LSAs of the network. These LSAs are originated for broadcast and NBMA networks by the designated router. This LSA contains the list of routers connected to the network, and is flooded throughout a single area only.
- **router** – Shows the LSAs of the router. These LSAs are originated by all routers. This LSA describes the collected states of the router's interfaces to an area, and is flooded throughout a single area only.

- **inter-prefix** – Shows the LSAs originated by ABRs and these LSAs are flooded throughout the LSA's associated area. Each inter-prefix LSA describes a route with IPv6 address prefix to a destination outside the area, yet still inside the AS (an inter-area route).
- **link** – Shows the LSAs originated by a router. This link LSA is originated for each link and it has link-local flooding scope. Each link LSA describes the IPv6 address prefix of the link and link-local address of the router.
- **intra-prefix** - Shows the LSAs that contains IPv6 prefix information on a router, stub area or transit area information, and it has area flooding scope. The intra-prefix LSAs were introduced because router LSAs and network LSAs contain no address information now.
- *A.B.C.D* - Shows the IP address of link status ID.
- **adv-router** *A.B.C.D* – Shows the LSAs of the specified router.
- **self-originate** - Only shows self-originated LSAs (from local router).
- *vrouter-name* - Specifies the VRouter name. If the VRouter is not specified, system will only show the database information of all OSPFv3 processes in the trust-vr.
- **process** *process-id* - Shows the database information of the OSPFv3 with the specified process ID. If the process ID is not specified, system will show the database information of all OSPFv3 processes in the VRouter.

To view the OSPF interface information, in any mode, use the following command:

show ipv6 ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF neighbor information, in any mode, use the following command:

show ip ospf neighbor [*A.B.C.D* | **detail**][**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF border router information, in any mode, use the following command:

show ipv6 ospf border-routers [*A.B.C.D*][**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPF route information, in any mode, use the following command:

show ip ospf route [*X:X:X:X::X/M* [**vrouter** *vrouter-name*] [**process** *process-id*]

To view the OSPFv3 virtual links information, in any mode, use the following command:

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

Configuring IPv6 BGP

BGP-4 was designed to carry only IPv4 routing information, and other network layer protocols such as IPv6 are not supported. To support multiple network layer protocols, IETF extended BGP-4 by introducing multiprotocol BGP (MP-BGP). MP-BGP for IPv6 is called IPv6 BGP. IPv6 BGP uses the extension attribute of BGP to achieve the goal of using BGP in IPv6 network and it has the same messaging and routing mechanisms as BGP.

To configure the following items, see "Configuring BGP" of "Routing".

- Configuring a peer/peer group
- Configuring equal cost multipath routing
- Configuring a timer
- Configuring MD5 authentication
- Disabling a peer/peer group
- Configuring EBGP multihop
- Configuring description
- Configuring a peer timer

This section introduces the following configurations:

- Configuring IPv6 unicast route
- Activating a connection
- Sending community path attributes to a peer/peer group
- Specifying Upper Limit of Prefixes

Entering the IPv6 Unicast Routing Configuration Mode

To configure the settings of IPv6 unicast route, you must enter into the IPv6 unicast routing configuration mode. Execute the following command in the BGP instance configuration mode:

address-family ipv6 unicast

Configuring IPv6 Unicast Route Redistribute

IPv6 BGP supports IPv6 unicast route redistribute. It allows users to introduce information from other routing protocols (connected, IS-IS, static, OSPFv3 and RIPng) and redistribute the information. To configure the redistribute metric, in the IPv6 unicast routing configuration mode, use the following command:

redistribute {**ospf** | **isis**| **connected** | **static** | **rip**} [**metric** *value*] [**route-map***name*]

- **ospf** | **isis**| **connected** | **static** | **rip** – Specifies the protocol type which can be connected route (**connected**), IS-IS (**isis**), static route (**static**), RIPng (**rip**) or OSPFv3 (**ospf**).
- **metric** *value* – Specifies the redistribute metric value. The value range is 0 to 4294967295.
- **route-map***name* - Specifies the route map used to filter redistribute information. For more information about route map, see "Route Map" on Page 541.

Repeat the above command to redistribute different types of protocols.

To cancel the redistribute of the specified protocol, in the IPv6 unicast routing configuration mode, use the following command:

no redistribute {**ospf** | **isis**| **connected** | **static** | **rip**}

Activating a BGP Connection

By default, the IPv6 BGP connection between the configured BGP peer or peer group and the device is activated. You can de-activate or re-activate the IPv6 BGP connection. To activate the IPv6 BGP connection, in the IPv6 unicast routing configuration mode, use the following command:

neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **activate**

- *X:X:X:X::X | A.B.C.D | peer-group* – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.

To de-activate the IPv6 BGP connection to the specified BGP peer or peer group, in the IPv6 unicast routing configuration mode, use the following command:

no neighbor {*X:X:X:X::X | A.B.C.D | peer-group*} **activate**

Sending Community Path Attributes to a Peer/Peer Group

To configure the upper limit of prefixes that can be received from IPv6 peer/peer group, use the following command in the IPv6 unicast routing configuration mode:

neighbor {*X:X:X:X::X | A.B.C.D | peer-group*} **send-community** {**standard** | **extended** | **both**}

- {*X:X:X:X::X | A.B.C.D | peer-group*} – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.
- **standard** | **extended** | **both** – Specifies the type of the communities path attributes. There are three types: **standard** means the standard communities path attributes, **extended** means the extended communities path attributes, and **both** means both of the communities path attributes and extended communities path attributes.

Use the following command to cancel the above configurations:

no neighbor {*X:X:X:X::X | A.B.C.D | peer-group*} **send-community**

Specifying Upper Limit of Prefixes

To configure the upper limit of prefixes that can be received from IPv6 peer/peer group, use the following command in the IPv6 unicast routing configuration mode:

neighbor {*X:X:X:X::X | A.B.C.D | peer-group*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

- {*X:X:X:X::X | A.B.C.D | peer-group*} – Specifies the IPv4/IPv6 address of the peer or the name of the peer group.

- *maximum* - Specifies the upper limit of prefixes that can be received from IPv6 peer/peer group.
- *threshold* – Specifies the threshold that will trigger the generation of log information. The default value is 75, and it ranges from 1 to 100.
- **restart** *restart-interval* – After the received prefixes reaches the threshold, the connection to the peer will be disconnected and the connection will be re-established after the specified interval here. The unit is minute and the value ranges from 1 to 65535.
- **warning-only** – After the received prefixes reaches the threshold, the system generates the corresponding log information.

Use the no form to cancel the above configurations:

no neighbor {*X:X:X:X::X* | *A.B.C.D* | *peer-group*} **maximum-prefix**

Viewing BGP Routing Information

To view the routing information of the entire IPv6 BGP routing table, in any mode, use the following command:

show ip bgp ipv6 unicast {*X:X:X:X::X/Mask* | **vrouter** *vrouter-name*}

- *X:X:X:X::X/Mask* – Shows the IPv6 BGP routing information of the specified network.
- *vrouter-name* - Shows the IPv6 BGP routing information of the specified VRouter.

To view the status parameters of all BGP connections, including the prefix, path, attribute, etc., in any mode, use the following command:

show ip bgp ipv6 unicast summary [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the IPv6 BGP routing information of the specified VRouter.

To view the BGP peer status, in any mode, use the following command:

show ip bgp ipv6 unicast neighbor [*X:X:X:X::X* | *A.B.C.D*] [**vrouter** *vrouter-name*]

- *X:X:X:X::X | A.B.C.D* – Shows the BGP peer status of the specified IPv4/IPv6 address.
- *vrouter-name* - Shows the IPv6 IPv6 BGP routing information of the specified VRouter.

Configuring IPv6 Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet, and specify the next hop of the packets which match the policy. System supports to configure PBR rules using IPv6 address.

To configure the following items, see Policy-based Route in StoneOS_CLI_User_Guide_Routing:

- Editing a PBR Rule
- Enabling/Disabling a PBR Rule
- Moving a PBR Rule
- Applying a PBR Rule

Creating a PBR Policy

To create a PBR policy, in the global configuration mode, use the following command:

pbr-policy *name*

- *name* – Specifies the name of the PBR policy. The length is 1 to 31 characters. If the policy exists, the system will directly enter the PBR policy configuration mode.

To delete the specified PBR policy, use the command **no pbr-policy** *name*.

Creating a IPv6 PBR Rule

To create a IPv6 PBR rule, in the PBR policy configuration mode, use the following command:

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name | A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id* – Specifies the ID of the new PBR rule. The value range is 1 to 255. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in its corresponding PBR policy.
- **before** *rule-id* | **after** *rule-id* | **top** – Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the new rule at the end of all the rules.
- *src-addr* – Specifies the source address which should be an entry defined in the address book. The address should be IPv6 address.
- *dst-addr* – Specify the destination address which should be an entry defined in the address book. The address should be IPv6 address.
- *service-name* – Specifies the name of the service. service-name should be the service defined in the service book.
- *application-name* – Specifies the name of the application. application-name should be the application defined in the application book.
- **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} – Specifies the next hop. *interface-name* is the name of egress interface, or local-address. *A.B.C.D* is the IP address of the next hop, **vrouter** *vrouter-name* is a VRouter, and **vsys** *vsys-name* is the name of VSYS.
- **weight** *value* – Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, the system will distribute the traffic in proportion to the corresponding weight.
- **track** *track-object-name* – Specifies the track object for the next hop. If the track object fails, the PBR rule will fail as well. For more information about track object, see "Configuring a Track Object" in "System Management".

To delete the specified rule, in the PBR policy configuration mode, use the following command:

no match-v6 id *rule-id*

In addition, you can also use the following command in PBR policy configuration mode to create a PBR rule ID, and then in the PBR policy rules configuration mode, further configure other relevant parameters of the PBR rule:

match-v6 [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* – Specifies the ID of the new PBR rule. If no ID is specified, the system will automatically assign an ID. The rule ID must be unique in the whole system. However, the PBR rule ID is not related to the matching sequence.
- **top** | **before** *rule-id* | **after** *rule-id* – Specifies the position of the PBR rule. The new PBR rule can be located before a rule (**before** *rule-id*), after a rule (**after** *rule-id*) or at the top of all the rules (**top**). By default, the system will put the newly created rule at the end of all the rules.

Configuring IPv6 IS-IS

The IS-IS routing protocol (Intermediate System-to-Intermediate System intra-domain routing information exchange protocol) supports multiple network protocols, including IPv6. The IS-IS routing protocol that supports IPv6 is named IPv6 IS-IS routing protocol. In the IPv6 network environment, you can configure the IPv6 IS-IS routing protocol to realize the connectivity between IPv6 networks.

To configure the following items, see Configuring IS-IS in StoneOS_CLI_User_Guide_Routing:

- Configuring the router type
- Configuring the interface type
- Configuring the network as point-to-point type
- Configuring the NET address
- Configuring the metric style
- Configuring the parameters for Hello packets

- Configuring the priority for DIS election
- Configuring the passive interface
- Configuring the parameters for LSP packets
- Configuring the hostname mappings
- Configuring the authentication methods
- Configuring the interface authentication

This section introduces the following configurations:

- Enabling IPv6 IS-IS at interfaces
- Configuring the interface metric
- Entering into the IPv6 unicast routing configuration mode
- Configuring the default route advertisement
- Configuring the administrative distance
- Configuring redistribute
- Configuring the overload bit
- Configuring the SPF calculation interval
- Configuring Multiple-Topology routing
- Viewing IPv6 IS-IS information

Enabling IPv6 IS-IS at interfaces

By default, the IPv6 IS-IS function is disabled at the interface. After creating an IS-IS process at the current router, proceed to enable the IPv6 IS-IS function at the interface. Use the following command in the interface configuration mode:

isis ipv6 enable

Use the **no isis ipv6 enable**command to disable the IPv6 IS-IS function at the interface.

Configuring the Interface Metric

The metric is used to calculate the cost to the destination network via the selected link. To configure the metric of the link where the interface locates in IPv6 network, use the following command in the interface configuration mode:

isis ipv6 metric *value* [**level-1** | **level-2**]

- *value* – Configure the metric value of the link that the interface locates. The value ranges from 1 to 16777214 and the default value is 10.
- **level-1** | **level-2** – Use level-1 to configure the metric value for Level-1 routes. Use level-2 to configure the metric value for Level-2 routes. Without specifying level-1 or level-2, the metric value is effective for both Level-1 and Level-2 routes.

Use the **no isis ipv6 metric** command to restore the metric value to the default one.

Entering into the IPv6 Unicast Routing Configuration Mode

To configure the settings for IPv6 IS-IS unicast route, you must enter into the IPv6 unicast routing configuration mode. Execute the following commands to enter into this configuration mode:

ip vrouter *vrouter-name* – In the global configuration mode, execute this command to enter into the VRouter configuration mode.

router isis – Enter into the IS-IS routing configuration mode and create the IS-IS process. The IS-IS processes in each VRouter are independent.

address-family ipv6 unicast - Enter into the IPv6 unicast routing configuration mode.

Configuring the Default Route Advertisement

The default IPv6 route in the introduced routing information will not be used by the routers. To advertise the default IPv6 route in the routing domain, in the IS-IS IPv6 unicast routing configuration mode, use the following command:

default-information originate

If there is a default route in the router with the above command configured, the IS-IS process in this router will advertise this route via Level-2 LSPs.

To cancel the default IPv6 route advertisement, use the **no default-information originate** command.

Configuring the Administrative Distance

To configure the administrative distance of the IPv6 IS-IS route, use the following command in the IS-IS IPv6 unicast routing configuration mode:

distance *distance-value*

- *distance-value* – Specify the administrative distance. The value ranges from 1 to 255. The default value is 115.

To restore the value to the default one, use the **no distance** command.

Configuring Redistribute

IPv6 IS-IS allows you to introduce routing information from other routing protocols (connected, static, OSPFv3, IPv6 BGP and RIPng) and redistribute the information. To configure the redistribute and the corresponding metric, in the IS-IS IPv6 unicast routing configuration mode, use the following commands:

redistribute {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *value*] [**metric-type** {**external** | **internal**}]

- **connected** | **static** | **ospf** | **bgp** | **rip** – Specifies the protocol type which can be **connected**, **static**, **OSPF**(OSPFv3), **bgp**(IPv6 BGP), or **rip**(RIPng).
- **level-1** | **level-1-2** | **level-2** – Specifies the level for the introduced route, including the level-1 route (**level-1**), level-2 route (**level-2**), and both levels (**level-1-2**).
- **metric** *value* – Specifies a metric value for the introduced route. The value range is 0 to 4294967296. The default value is 0. When the metric type of the router is narrow, the metric value of the introduced route cannot exceed 63.

- **metric-type** {**external** | **internal**} – If you select the external metric type (**external**), the metric value will be the sum of the value configured in **metric** *value* and 64. If you select the internal metric type (**internal**), the metric value will be the one you configured in the **metric** *value* command. The default option is internal.

To cancel the redistribute configurations, use the **no redistribute** {**connected** | **static** | **ospf** | **bgp** | **rip**} [**level-1** | **level-1-2** | **level-2**] command.

Configuring the Overload Bit

If a router is lack of resources, its LSDB might be inaccurate or incomplete. You can configure the overload bit for this router, which will suppress the advertisement of the introduced routes. The routes introduced from other routing protocol will not be advertised. And this reduces the number of packets that are forwarded via this router. However, the packets whose destination is the directly connected network of this router or the packets whose destination is within the same routing domain, can be forwarded to this router as before. To configure the overload bit for the router, use the following command in the IS-IS IPv6 unicast routing configuration mode:

set-overload-bit suppress external

To cancel the overload bit configuration, use the command **no set-overload-bit**.

Configuring the SPF Calculation Interval

If the LSDB changes, the router will re-calculate the SPF. To configure the SPF calculation interval for IPv6 IS-IS, use the following command in the IPv6 IS-IS unicast routing configuration mode:

spf-interval *value* [**level-1** | **level-2**]

- *value* – Specify the SPF calculation interval. The value ranges from 1 to 120. The default value is 10. The unit is second.

- **level-1** | **level-2** – Enter **level-1** to specify the SPF calculation interval for level-1 SPFs only, and enter **level-2** to specify the SPF generation interval for level-2 SPFs only. If you enter no parameter, the configured interval value will be used for both level-1 SPFs and level-2 SPFs.

Use the **no spf-interval**command to restore the value to the default one.

Configuring Multiple-Topology Routing

When using IPv6 IS-IS, the device supports both unique topology routing and multiple-topology routing. When using unique topology routing, the device calculates the mixed routing for both IPv4 topo and IPv6 topo.

When using multiple-topology routing, the device will perform the SFP calculation for IPv4 topo and IPv6 topo individually, and generate the routing information individually.

By default, the system uses the unique topology routing. To enable the multiple-topology routing, first change the metric type to wide in the IS-IS routing configuration mode by using the **metric-style wide** command. Then perform the following command in the IS-IS IPv6 unicast routing configuration mode:

multi-topology

To disable the multiple-topology routing, use the command **no multi-topology**.

Viewing IPv6 IS-IS Information

To show the routing information of the IPv6 IS-IS, use the following command in any mode:

show isis ipv6 route

To show the IS-IS process and corresponding information, use the following command in any mode:

show isis [**vrouter** *vrouter-name*]

- *vrouter-name* - Show the information of the specified vrouter.

To show the link state database, use the following command in any mode:

show isis database [**detail**] [**vrouter** *vrouter-name*]

- **detail** – Show the detailed information.
- *vrouter-name* - Show the information of the specified vrouter.

To show the IS-IS interface information, use the following command in any mode:

show isis interface [*interface-name*]

Configuring IPv6 Static Multicast Routing

By default the IPv6 multicast route is disabled. To enable or disable the IPv6 multicast route, in the VRouter configuration mode, use the following commands:

- Enable: **ipv6 multicast-routing**
- Disable: **no ipv6 multicast-routing**

Configuring an IPv6 Static Multicast Route Entry

To create an IPv6 static multicast route entry, in the VRouter configuration mode, use the following command:

ipv6 mroute *X.X.X.X::X X.X.X.X::X* [**iif** *interface-name*] [**eif** *interface-name*]

- *X.X.X.X::X X.X.X.X::X* - Specifies the multicast source address and multicast address. The first *X.X.X.X::X* is the IPv6 address of the multicast source, and the second *X.X.X.X::X* is the IPv6 multicast address.
- **iif** *interface-name* - Specifies an ingress interface. You can specify up to two ingress interfaces.
- **eif** *interface-name* - Specifies an egress interface. You can specify up to four egress interfaces.

To delete the specified IPv6 static multicast route entry, in the VRouter configuration mode, use the following command:

no ipv6 mroute *X.X.X.X::X X.X.X.X::X*

Specifying an Ingress/Egress Interface

You can configure an ingress or egress interface for the existing IPv6 static multicast route entry. Each multicast route entry can have up to two ingress interfaces, and up to 32 egress interfaces. The options of ingress and egress interface must be configured in the IPv6 static multicast route configuration mode. To enter the IPv6 static multicast route configuration mode, in the VRouter configuration mode, use the following command:

ipv6 mroute *X.X.X.X::X X.X.X.X::X*

- *X.X.X.X::X X.X.X.X::X* - Specifies the multicast source address and multicast address. The first *X.X.X.X::X* is the IPv6 address of the multicast source, and the second *X.X.X.X::X* is the IPv6 multicast address.

To specify an ingress and egress interface for the existing IPv6 static multicast routing entry, in the IPv6 static multicast route configuration mode, use the following command:

- Specify an ingress interface: **iif** *interface-name*
- Specify an egress interface: **eif** *interface-name*

Repeat the above command to configure multiple ingress or egress interfaces.

To delete the configured ingress or egress interface for the existing IPv6 static multicast routing entry, in the VRouter configuration mode, use the command **no ipv6 mroute** *X.X.X.X::X X.X.X.X::X* {[**iif** *interface-name*] [**eif** *interface-name*]}. Or in the IPv6 static multicast route configuration mode, use the following command:

- Delete an ingress interface: **no iif** *interface-name*
- Delete an egress interface: **no eif** *interface-name*

Viewing IPv6 Multicast Route Information

To view the IPv6 multicast route information, in any mode, use the following command:

show ipv6 mroute [*X.X.X.X::X X.X.X.X::X* | **summary**] [**vrouter** *vr-name*]

- **show ipv6 mroute** - Shows all the IPv6 multicast route information.
- *X.X.X.X::X X.X.X.X::X* - Shows the multicast route information of the specified multicast source address and multicast address. The first *X.X.X.X::X* is the IPv6 address of the multicast source, and the second *X.X.X.X::X* is the IPv6 multicast address.
- **summary** - Shows the summary of IPv6 multicast route.
- **vrouter** *vr-name* - Shows the IPv6 multicast route information of the specified VRouter.

Viewing IPv6 Multicast FIB Information

To view the IPv6 multicast FIB information, in any mode, use the following command:

show ipv6 mfib [*X.X.X.X::X X.X.X.X::X* | **summary**] [**vrouter** *vr-name*]

- **show ipv6 mfib**- Shows all the IPv6 multicast FIB information.
- *X.X.X.X::X X.X.X.X::X* - Shows the multicast FIB information of the specified multicast source address and multicast address. The first *X.X.X.X::X* is the IPv6 address of the multicast source, and the second *X.X.X.X::X* is the IPv6 multicast address.
- **summary** - Shows the summary of IPv6 multicast FIB.
- **vrouter** *vr-name* - Shows the IPv6 multicast FIB information of the specified VRouter.

Configuring IPv6 BFD

BFD (Bidirectional Forwarding Detection) is a unified detection mechanism for the entire network, which is used to fast detect and monitor the forwarding and connection status of the link and the IP route. To enhance the network performance, the protocol neighbor must have the ability to detect the communication failures quickly. Thus, the backup communication can be established to restore the communication in time.

BFD creates sessions between two routers for monitoring the bidirectional forwarding path between these two routers, which provides services for the upper level protocol, for example, routing protocol. BFD does not have the discovering mechanism and upper level protocol will notify BFD to create sessions with specifies objects. If no BFD packets are received from the peer during the detection period after creating sessions, BFD will notify the upper-level service and the upper-level service will execute the corresponding operations.

In the current StoneOS, BFD can integrate with IPv4 static route, IPv6 static route, OSPF route, OSPFv3 route, and BGP route. Thus, StoneOS can realize the detection of the forwarding and connection status on the link that runs IPv4 static route, IPv6 static route, OSPF route, OSPFv3 route, and BGP route.

To configure the following items, see Configuring BFD in StoneOS_CLI_User_Guide_Routing:

- Configuring the BFD detection methods
- Configuring the BFD session parameters
- Enabling/Disabling the Echo function
- Specifying the interval of receiving Echo packets
- Configuring BFD multi-hop detection

This section introduces the following configurations:

- Configuring the source IP address of the Echo packets
- Integrating BFD with the IPv6 static route
- Integrating BFD with the OSPFv3 route
- Viewing IPv6 BFD session information

Configuring the Source IP Address of the Echo Packets

A large number of ICMP redirection packets sent from the peer leads to the network congestion. To avoid the network congestion, you can configure the source IP address of the Echo packets.

To configure the source IPv6 address, use the following command in the global configuration mode:

bfd echo-source-ipv6 *echo-src-address*

- *echo-src-address* – Specifies the source IPv6 addresses of the BFD Echo packets.

To delete the configured source IPv6 address, use the following command in the global configuration mode: **no bfd echo-source-ipv6**.

Integrating BFD with the IPv6 Static Route

To integrate BFD with the IPv6 static route and enable the BFD detection function for the specified next hop, use the following command in the VRoute configuration mode:

ipv6 route *ipv6-address/M interface-name nexthop-ipv6-address* **bfd**

- *ipv6-address/M* – Specifies the network address of the IPv6 static route.
- *interface-name nexthop-ipv6-address* – Specifies the IPv6 address of the next-hop interface. The address type is Link-local.
- **bfd** – Enables the BFD detection function for the specified next hop.

To cancel the integration, use the following command in the VRouter configuration mode:

no ipv6 route *ipv6-address/M interface-name nexthop-ipv6-address* **bfd**

Integrating BFD with the OSPFv3 Route

By integrating BFD with the OSPFv3 route, the system realizes the quick link detection which has higher performance than the Hello detection mechanism of the OSPFv3 protocol. With the integration, OSPFv3 protocol improves its convergence performance.

To integrate BFD with the OSPFv3 rout and enable the BFD detection function on the specified interfaces that corresponds to the OSPFv3 route, use the following command in the interface configuration mode:

ipv6 ospf bfd

To cancel the integration, use the following command in the interface configuration mode:

no ipv6 ospf bfd

Viewing IPv6 BFD Session Information

To view the IPv6 BFD session information, use the following command in any mode:

show bfd session [**interface** *interface-name* | **neighbor***X:X:X:X::X* | **detail**]

- **interface** *interface-name* - Show the information of the BFD sessions of the specified interface.
- *X:X:X:X::X* – Specify IPv6 address of the neighbor router. The address type is Link-local.
- **detail** – Show the detailed information of the BFD sessions of all routers.

Configuring IPv6 DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IPv6 addresses and related network parameters for subnets automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

Hillstone devices support IPv6 DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: A Hillstone device's interface can be configured as a DHCP client and obtain IP addresses from the DHCP server.
- DHCP server: A Hillstone device's interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: A Hillstone device's interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

Hillstone devices are designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Client

You can configure an interface of the device as the DHCP client that obtains IPv6 address from the DHCP server. The DHCP client should be configured in the interface configuration mode. The configuration includes:

- Obtaining an IPv6 address via DHCP
- Releasing and renewing the IPv6 address

Obtaining an IPv6 address via DHCP

To enable the interface to obtain an IPv6 address via DHCP, in the interface configuration mode, use the following command:

ipv6 address dhcp [**rapid-commit**]

- **ipv6 address dhcp** – Enable the interface to obtain an IP address via DHCP.
- **rapid-commit** – Specifying this option can help fast get IPv6 address from the server. You need to enable both of the DHCP client and the server's Rapid-commit function.

To cancel the configuration, in the interface configuration mode, use the command **no ipv6 address dhcp**.

Releasing and Renewing the IPv6 Address

The interface that has obtained a dynamic IPv6 address via DHCP can release and renew its IPv6 address. To release and renew the IPv6 address, in the interface configuration mode, use the following commands:

- Release: **dhcpv6-client ip release**
- Renew: **dhcpv6-client ip renew**

To view the DHCP IPv6 address information allocated to an interface, in the interface configuration mode, use the following command:

show dhcpv6-client interface *interface-name*

Configuring a DHCP Server

The Hillstone devices can act as a DHCP server to allocate IP addresses for the DHCP clients in the subnets. The DHCP server should to be configured in the DHCP server configuration mode. To enter the DHCP server configuration mode, in the global configuration mode, use the following command:

dhcpv6-server pool *pool-name*

- *pool-name* – Specifies the name of the DHCP address pool.

After executing the above command, the system will create a new DHCP address pool and enter the DHCP server configuration mode of the address pool; if the specified address pool exists, the system will directly go to the DHCP server configuration mode.

To delete the specified address pool, in the global configuration mode, use the command **no dhcpv6-server pool** *pool-name*.

The DHCP server functions you can configure include:

- Basic configuration of the DHCP address pool
- Binding the address pool to an interface

Basic Configuration of the DHCP Address Pool

This section describes how to configure DHCP address pool.

Configuring an IP Range

You need to specify the IP range used for external allocation. To specify the IP range of the address pool, in the DHCP server configuration mode, use the following command:

address prefix *ipv6-address/prefix-length* [**lifetime** {*valid-lifetime* | **infinite**} | {*preferred-lifetime* | **infinite**}]

- *ipv6-address/prefix-length* – Specifies the IPv6 address prefix and prefix length.
- *valid-lifetime* – Specifies the lifetime of the address.
- **infinite** – If specified the parameter, the address will be valid permanently.
- *preferred-lifetime* – Specifies the preferred lifetime for the IPv6 address. The preferred lifetime should not be larger than the valid lifetime.

To cancel the specified IP range, in the DHCP server configuration mode, use the command **no address prefix**.

Configuring Domain Name for the DHCP Client

To configure domain name for the DHCP client, in the DHCP server configuration mode, use the following commands:

domain *domain-name*

- *domain-name* – Specifies the domain name.

To cancel the configured domain name, in the DHCP server configuration mode, use the command **no domain**.

Configuring DNS Servers for the DHCP Client

To configure DNS servers for the DHCP client, in the DHCP server configuration mode, use the following commands:

dns-server {**use-system** | [*ipv6-address1*] [*ipv6-address2*]}

- **use-system** - Use the DNS server configured in the system as the DNS server of the client. If the system has configured more than two DNS servers, you can use the first two DNS servers as the DNS servers of the client.
- *ipv6-address1* – Specifies the IP address of the primary DNS server.
- *ipv6-address2* – Specifies the IP address of the alternative DNS server.

To cancel the configured DNS, WINS server and domain name, in the DHCP server configuration mode, use the command **no dns-server**.

Binding the Address Pool to an Interface

If the address pool is bound to an interface, the interface will run DHCP server based on the configuration parameters of the address pool. To bind the address pool to an interface, in the interface configuration mode, use the following command:

dhcpv6-server enable pool *pool-name* [**rapid-commit**] [**preference** *preference*]

- *pool-name* – Specifies the address pool defined in the system.
- **rapid-commit** – Specifying this option can help fast get IPv6 address from the server. You need to enable both of the DHCP client and the server's Rapid-commit function.
- **preference** *preference* – Specifies the priority of the DHCP server. The range should be from 0 to 255. The bigger the value is, the higher the priority is.

To disable the DHCP server on the interface, in the interface configuration mode, use the command **no dhcpv6-server enable**.

Configuring a DHCP Relay Proxy

The Hillstone device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client. The DHCP relay proxy should be configured in the interface configuration mode. The configurations include:

- Specifying the IP address of the DHCP server
- Enabling DHCP relay proxy on an interface

Enabling DHCP Relay Proxy on an Interface

To enable DHCP relay proxy on an interface, in the interface configuration mode, use the following command:

dhcpv6-relay enable

To disable the specified DHCP relay proxy, in the interface configuration mode, use the command **no dhcpv6-relay enable**.

Specifying the IP Address of the DHCP Server

To specify the IP address of the DHCP server, in the interface configuration mode, use the following command:

dhcpv6-relay server *ipv6-address* [**interface** *interface-name*]

- *ip-address* – Specifies the IP address of the DHCP server.
- **interface** *interface-name* – If the DHCP server is specified as link-local address, you need to specify the egress interface name.

To cancel the specified IP address, in the interface configuration mode, use the command **no dhcpv6-relay server** *ipv6-address* [**interface** *interface-name*].

Viewing DHCP Configuration Information

In any mode, use the following command to view DHCP configuration information:

- **show dhcpv6 duid**: Shows device's IPv6 UID information.
- **show dhcpv6 interface**: Shows all the interfaces information which enabling DHCP IPv6.
- **show dhcpv6-client interface** *interface-name*: Shows the interface information which enabling DHCP client IPv6.
- **show dhcpv6-server binding** *pool-name*: Shows the binding relationship between DHCP server and client.
- **show dhcpv6-server pool** *pool-name*: Shows the address pool information of the DHCP server.

Configuring IPv6 DNS

StoneOS supports IPv6 DNS for the translation between domain names and IPv6 addresses. IPv6 introduces new DNS records to resolve IPv6 addresses and translate domain names to IPv6 addresses.



Notes: This section only describes IPv6-related configurations. For more information about DNS and its configurations, see "DNS" of "Firewall".

Configuring a IPv6 DNS Proxy Rule

The configuration of IPv6 DNS proxy rule includes:

- Creating a DNS proxy rule
- Configuring the Filtering Condition of a DNS Proxy rule
- Specifying the Action of a DNS Proxy Rule
- Configuring DNS Proxy Servers

- Modifying/Deleting the Descriptions of a Proxy Rule
- Enabling/Disabling a DNS Proxy Rule



Tip: This section only describes the configuration of DNS proxy filtering condition for IPv6 (IPv6 DNS source address, IPv6 DNS destination address) and IPv6 DNS proxy server configuration. Other configurations are the same as the IPv4 DNS proxy configuration. For details, see Configuring a DNS Proxy in Firewall in the StoneOS_CLI_User_Guide_Firewall.

Specifying IPv6 Source Address

You can specify the source address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. To add or delete the source address of DNS request, in DNS proxy rule configuration mode, use the following command:

- Add the IPv6 source address of the address entry type： **src-addr** { *ipv6-addr-name* | *ipv6-any*}
- Delete the IPv6 source address of the address entry type: **no src-addr** { *ipv6-addr-name* | *ipv6-any*}
- Add the IPv6 source address of the IP member type: **src-ip** *ipv6-address/netmask*
- Delete the IPv6 source address of the IP member type: **no src-ip***ipv6-address/netmask*
- Add the IPv6 source address of the IP range type:**src-range** *min-ipv6-address max-ipv6-address*
- Delete the IPv6 source address of the IP range type :**no src-range***min-ipv6-address min-ipv6-address*

Specifying IPv6 Destination Address

You can specify the IPv6 destination address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple destination address filtering conditions.To add or delete the destination address of request, in DNS proxy rule configuration mode, use the following command:

- Add the IPv6 destination address of the address entry type: **dst-addr** { *ipv6-addr-name* | **ipv6-any** }
- Delete the IPv6 destination address of the address entry type:**no dst-addr** { *ipv6-addr-name* | *ipv6-any* }
- Add the IPv6 destination address of the IP member type: **dst-ip***ipv6-address/netmask*
- Delete the IPv6 destinaion address of the IP member type:**no dst-ip** *ipv6-address/netmask*
- Add the IPv6 destination address of the IP range type:**dst-range***min-ipv6-address max-ipv6-address*
- Delete the IPv6 destination address of the IP range type: **no dst-range***min-ipv6-address max-ipv6-address*

Configuring IPv6 DNS Proxy Servers

When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers. You can specify up to six DNS server and you can configure the interface and preferred properties for the DNS server as needed. When you configure multiple DNS servers, the DNS server with preferred property will be selected for domain name resolution. If no preferred server is specified, the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin; Except for the two DNS servers, which means that you only have a regular DNS server, then select this kind of DNS servers in a round robin.To add a DNS proxy server, in the DNS proxy rule configuration mode, use the following command:

name-server*server-ipv6-address* [**vrouter***vrouter-name*] [**egress-interface** *interface-name*][**preferred**]

- *server-ipv6-address* – Specifies the IPv6 address of the DNS proxy.
- *vrouter-name* – Specifies a VRouter for the DNS proxy.
- *interface-name* – Specifies the outgoing interface for sending DNS proxy requests.
- **preferred** – Specifies the DNS proxy 4dserver as the preferred server, and a DNS proxy rule can only specify one server as the preferred server.

To delete the DNS proxy server, in the DNS proxy rule configuration mode, use the command **no name-server***server-ipv6-address* [**vrouter** *vrouter-name*]

Configuring IPv6 DNS Servers

IPv6 DNS servers are used for domain name resolution. To configure IPv6 DNS servers, in the global configuration mode, use the following command:

ipv6 name-server *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*]

- *ipv6-address1* – Specifies the IPv6 address of DNS server. You can configure up to six DNS servers by one or multiple commands, i.e., running command **ipv6 name-server 2002:ae3:1111:2222::1 2001:0db8::3** and running commands **ipv6 name-server 2002:ae3:1111:2222::1** and **ipv6 name-server 2001:0db8::3**make no difference.
- **vrouter** *vr-name* – Specifies the VRouter the IPv6 DNS server belongs to.

To cancel the specified IPv6 DNS servers, in the global configuration mode, use the command **no ipv6 name-server** *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*] [**vrouter** *vr-name*].

Configuring an IPv6 DNS Proxy Server List

IPv6 DNS proxy server list contains mapping entries for domain names and corresponding IPv6 DNS servers. The list contains up to six mapping entries. To add a mapping entry to the IPv6 DNS proxy server list, in the global configuration mode, use the following command:

ipv6 dns-proxy domain {*domain-suffix* | **any**} **name-server** {**use-system** | *ipv6-address1* [*ipv6-address2*] ... [*ipv6-address6*]} [**vrouter** *vr-name*]

- *domain-suffix* | **any** – Specifies the suffix of domain name that is used to match the domain names in IPv6 DNS requests. any indicates any suffix.
- **name-server** {**use-system** | *server-ip1* [*server-ip2*] ... [*server-ip6*]} – Specifies IPv6 addresses for DNS servers. The servers can either be device's built-in IPv6 DNS server (**use-system**) or specified IPv6 addresses (*ipv6-address1* [*ipv6-address2*] ⋯ [*ipv6-address6*]). You can specify up to six IP addresses for IPv6 DNS servers.
- **vrouter** *vr-name* – Specifies the VRouter the IPv6 DNS server belongs to.

To delete the specified mapping entry, in the global configuration mode, use the command **no ipv6 dns-proxy domain** {*domain-suffix* | **any**} [**vrouter** *vr-name*].

For example, to add a mapping entry whose suffix is com and IP address of IPv6 DNS server is 2010::1, use the following command:

```
hostname(config)# ipv6 dns-proxy domain com name-server 2010::1
```

Enabling/Disabling IPv6 DNS Proxy

The IPv6 DNS proxy on interfaces is disabled by default. To enable IPv6 DNS proxy on an interface, in the interface configuration mode, use the following command:

dns-proxy

To disable DNS proxy, in the interface configuration mode, use the command **no dns-proxy**.

Adding a Static IPv6 DNS Mapping Entry

To add a static IPv6 DNS mapping entry to the cache manually, in the global configuration mode, use the following command:

ipv6 host *host-name* {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} [**ttl** *ttl-time*] [**vrouter** *vr-name*]

- *host-name* – Specifies the hostname. The length is 1 to 255 characters.
- {*ipv6-address1* [*ipv6-address2*] ... [*ipv6-address8*]} – Specifies the IPv6 addresses of the host. You can specify up to eight IPv6 addresses.
- *ttl-time* – Specifies the TTL value, which is the survival time of the IPv6 DNS mapping entry cache on the device. When the device has enabled the DNS proxy function and the DNS request initiated by the client matches the DNS proxy rule, if the DNS request hits the local cache, the TTL value set in the local cache will be returned to the client, and the cache will be deleted from the client if the TTL value is exceeded. The range is 60 to 86400 seconds.
- **vrouter** *vr-name* – Specifies the VRouter the host belongs to.

To delete the specified static IPv6 DNS mapping entry, in the global configuration mode, use the command **no ipv6 host** *host-name* [**vrouter** *vr-name*].

Clearing a Dynamic IPv6 DNS Mapping Entry

To clear a dynamic IPv6 DNS mapping entry manually, in the execution mode, use the following command:

clear ipv6 host [*host-name* [**vrouter** *vr-name*]]

- *host-name* – Clears IPv6 DNS mapping entries of the specified host.
- **vrouter** *vr-name* – Specifies the VRouter the host belongs to.

This command is used to clear the specified or all the dynamic IPv6 DNS mapping entries. To clear static IPv6 DNS mapping entries that are configured manually, in the global configuration mode, use the command **no ipv6 host** *host-name* [**vrouter** *vr-name*].

Viewing IPv6 DNS Mapping Entries

To view IPv6 DNS mapping entries, in any mode, use the following command:

show ipv6 host [*host-name*] [**vrouter** *vr-name*]

- *host-name* – Shows IPv6 DNS mapping entries of the specified host.
- **vrouter** *vr-name* – Specifies the VRouter the host belongs to.

Viewing IPv6 DNS Configuration

To view IPv6 DNS configuration, in any mode, use the following command:

show ipv6 dns

Configuring PMTU

When an IPv6 node sends large amount of data to another node, the data is transferred in form of a series of IPv6 packets. If possible, the size of these packets should not exceed the size limit for packets that requires fragmentation in the path from the source node to the destination node. This size is known as path MTU (PMTU) which equals to the smallest MTU of each hop in the path. IPv6 defines a standard mechanism that is used to discover PMTU in any path. StoneOS supports this PMTU discovery mechanism.

By default the PMTU discovery mechanism in StoneOS is disabled. To enable or disable the PMTU discovery mechanism, in the flow configuration mode, use the following commands:

- Enable: **ipv6 pmtu enable**
- Disable: **no ipv6 pmtu enable**



Tip: To enter the flow configuration mode, in the global configuration mode, use the command **flow**.

With PMTU enabled, the system will generate a PMTU entry to record the destination address, interface, PMTU value and aging out time after receiving an ICMPv6 Packet Too Big error. If any session to the destination address specified by the PMTU entry is established within the aging out time, the system will refresh the aging out time, i.e., restart counting; if no session matches to the PMTU entry within the aging out time, the entry will be aged out and deleted. You can specify an appropriate aging out time for the PMTU entry as needed.

To specify an aging out time, in the flow configuration mode, use the following command:

ipv6 pmtu ageout-time *time*

- *time* – Specifies the aging out time. The value range is 10 to 600 seconds. The default value is 300.

To restore to the default aging out time, in the flow configuration mode, use the following command:

no ipv6 pmtu ageout-time

You can also clear a PMTU entry immediately as needed. To clear a PMTU entry, in any mode, use the following command (if no optional parameter is specified, the command will clear all the existing PMTU entries):

clear ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – Specifies the IPv6 address of the PMTU entry that will be deleted.
- *interface-name* – Specifies the interface of the PMTU entry that will be deleted.

To view PMTU entry information, in any mode, use the following command (if no optional parameter is specified, the command will show the information of all the existing PMTU entries):

show ipv6 pmtu [**dst-ip** *ipv6-address* **interface** *interface-name*]

- *ipv6-address* – Shows the PMTU entry of the specified IPv6 address.
- *interface-name* – Shows the PMTU entry of the specified interface.

To view the status of PMTU, e.g., if the function is enabled, or the aging out time, in any mode, use the following command:

show ipv6 pmtu status

Configuring User-defined Application

Besides the predefined applications, you can also create your own user-defined applications based on IPv6 address. By configuring the customized application signature rules, StoneOS can identify and manage the IPv6 traffic that crosses into the device, thus identifying the type of the IPv6 traffic.

The configurations of IPv6 User-defined Application includes:

- Configuring IPv6 source address
- Configuring IPv6 destination address



Tip: This section only describes IPv6-related configurations. For more information about User-defined Application and its configurations, see "Service and Application" of "Firewall".

Creating/Deleting the User-defined Applications

To create a user-defined application and add this newly-created one to the application book, use the following command in the global configuration mode:

application *application-name*

- *application-name* – Specifies the name of the user-defined application. You can specify up to 31 characters. This name must be unique in the entire system.

After executing this command, the system enters the application configuration mode.

To delete the user-defined application, use the following command:

no application *application-name*

Enabling the User-defined Application Signature Configuration Mode

To enable the user-defined application signature configuration mode, use the following command in the global configuration mode:

app-signature

Enabling the Application Signature Rule Configuration Mode

In the user-defined application signature configuration mode, use the following command to create a user-defined application signature rule and enter the application signature rule configuration mode. If the specified ID already exists, the system will enter the application signature rule configuration mode.

signature [**id** *id*]

- *id* – Specify the ID of user-defined application signature rule. If the ID is not specified, system will create a user-defined application signature rule and specify the ID automatically.

To delete this user-defined application signature rule, use the following command in the application signature rule configuration mode:

no signature id*id*

Configuring IPv6 Source Address

To specify the IPv6 source address for the user-defined application signature, use the following command in the application signature rule configuration mode:

src-ipv6 *ipv6-address*

- *ipv6-address* – Specifies the IPv6 source address for the user-defined application signature.

Configuring IPv6 Destination Address

To specify the IPv6 destination address for the user-defined application signature, use the following command in the application signature rule configuration mode:

dst-ipv6 *ipv6-address*

- *ipv6-address* – Specifies the IPv6 destination address for the user-defined application signature.

Configuring a User-defined ICMPv6 Application Rule

To add an ICMPv6 application rule, in the application signature rule configuration mode, use the following command:

protocol icmpv6 type*type-value* [**code** *min-code* [*max-code*]]

- *type-value* – Specifies the ICMPv6 type value. For more information about the value range, see Appendix 1: ICMPv6 Type and Code. The default value is Any, which indicates all the

ICMPv6 type values.

- **code** *min-code* [*max-code*] – Specifies the minimum code value (*min-code*) and maximum code value (*max-code*) for ICMPv6. The value range is 0 to 255. If the code value is not specified, by default the system will use the code value that corresponds to the Type value (defined in RFC); if the maximum code value is not specified, by default the system will use the minimum code value as the maximum code value.

To delete the specified ICMPv6 application rule, in the application signature rule configuration mode, use the following command:

no protocol

Configuring an IPv6 Policy Rule

Policy is a basic function of network security devices. Network traffic is controlled by policy rules. StoneOS supports both IPv4 and IPv6 policy rules. The basic components of a policy rule include addresses (source and destination address), service and action. This section describes IPv6 configuration of the above components.

Configuring an IPv6 Address Entry

StoneOS address book supports both IPv4 and IPv6 address entries. IPv4 address entries only contain members of IPv4 addresses, IPv4 segments, IPv4 hosts and other IPv4 address entries; IPv6 address entries only contain members of IPv6 addresses, IPv6 segments and other IPv6 address entries. The address book contains a default address entry named ipv6-any that contains all the IPv6 addresses; the address entry named Any contains all the IPv4 addresses.



Tip: This section only describes the configuration of IPv6-related policy rules. For more information about policy rule configurations, see "Policy".

To create an address entry and enter the address entry configuration mode, in the global configuration mode, use the following command:

address *address-entry* **ipv6**

If the specified address entry already exists, the system will directly enter the address entry configuration mode. To add an IPv6 address to the address entry or delete an IPv6 address from the address entry, in the address entry configuration mode, use the following commands:

ip *ipv6-address/M*

no ip *ipv6-address/M*

To add an IPv6 address range to the address entry or delete an IPv6 address range from the address entry, in the address entry configuration mode, use the following commands:

range *min-ipv6-address max-ipv6-address*

no range *min-ipv6-address max-ipv6-address*

When creating an IPv6 address entry, keep in mind that:

- An IPv6 address entry cannot nest an IPv4 address entry, and vice versa;
- The first 64 bits of an IPv6 address range must be identical. For example, the address range from 2005::1 to 2006::1 is not permitted, while the address range from 2005::1 to 2005::1000 is permitted;
- The current version does not support hosts with IPv6 addresses.

Configuring an IPv6 Service

StoneOS includes some new predefined services in the service book to support IPv6 service; besides it also supports IPv6 ports for some network applications. To view all the supported predefined services and service groups, use the command **show service predefined** and **show servgroup predefined** respectively. A service group can contain both IPv4 and IPv6 services. You can also create a user-defined IPv6 service (ICMPv6) as needed.



Tip: For more information about the configuration of IPv4 service book, see "Application and Service" of "Firewall".

For more information about how to create a user-defined ICMPv6 service, see the section below:

To create a user-defined service and enter the user-defined service configuration mode, in the global configuration mode, use the following command:

service *service-name*

If the specified service already exists, the system will directly enter the user-defined service configuration mode.

To add an ICMPv6 service, in the user-defined configuration mode, use the following command:

icmpv6 type *type-value* [**code** *min-code* [*max-code*]]

- *type-value* – Specifies the ICMPv6 type value. For more information about the value range, see Appendix 1: ICMPv6 Type and Code. The default value is Any, which indicates all the ICMPv6 type values.
- **code** *min-code* [*max-code*] – Specifies the minimum code value (*min-code*) and maximum code value (*max-code*) for ICMPv6. The value range is 0 to 6 and Any (any ICMPv6 code value). If the code value is not specified, by default the system will use the code value that corresponds to the Type value (defined in RFC); if the maximum code value is not specified, by default the system will use the minimum code value as the maximum code value.

To delete the specified ICMPv6 service, in the user-defined configuration mode, use the following command:

no icmpv6 type *type-value* [**code** *min-code* [*max-code*]][**timeout** *timeout-value*]

Configuring an Action for IPv6 Policy Rule

IPv4 policy rules support the following five actions: deny, permit, fromtunnel, tunnel and webauth; in the current version IPv6 policy rules only support two basic actions: deny and permit.

Configuring an IPv6 Policy Rule

When configuring a policy rule, you must specify the same type of source address and destination address, i.e., if the source address is an IPv6 address, the destination address must be an IPv6 address.

To configure an IPv6 policy rule, in the policy configuration mode (to enter the policy configuration mode, in the global configuration mode, use the command policy-global), use the following command:

rule [**id** *id*] [**top** | **before** *id* | **after** *id*] **from** {*src-addr* | *ipv6-address*} **to** {*dst-addr* | *ipv6-address*} **service** *service-name* [**application** *app-name*]{**permit** | **deny**}

- **id** *id* – Specifies the ID of the policy rule. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system.
- **top** | **before** *id* | **after** *id* – Specifies the location of the policy rule. The location can be **top** | **before** *id* | **after** *id*. By default, the newly-created policy rule is located at the end of all the rules.
- **from** *src-addr* – Specifies the source address of the policy rule. src-addr can be an IPv6 address, an IPv6 address entry defined in the address book, or ipv6-any.
- **to** *dst-addr* – Specifies the destination address of the policy rule. dst-addr can be an IPv6 address, an IPv6 address entry defined in the address book, or ipv6-any.
- **service** *service-name* – Specifies the service name of the policy rule. service-name is the service defined in the service book.
- **permit** | **deny** – Specifies the action of the policy rule. **permit**means system will permit the traffic to pass through. **deny** means system will deny the traffic.

Besides you can also use the following command in the policy configuration mode to create a policy rule ID and enter the policy rule configuration mode for further configurations:

rule {**id** *id* | {**top** | **before** *id* | **after** *id*}}

- **id** *id* – Specifies the ID of the policy rule. If the policy exists, the system will directly enter the policy configuration mode. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system. The policy rule ID is not related to the matching sequence of the policy rule.

- **top** | **before** *id* | **after** *id* – Specifies the location of the policy rule. The location can be **top** | **before** *id* | **after** *id*. By default, the newly-created policy rule is located at the end of all the rules.

Editing an IPv6 Policy Rule

You can edit improper parameters for the policy rule in the policy rule configuration mode. To enter the policy rule configuration mode via CLI, in the global configuration mode, use the following commands:

- **rule** {**id** *id* | {**top** | **before** *id* | **after** *id*}}
- **rule id** *id*(The command applies to the case that ID is existing. To delete the rule, use the command **no rule id** *id*.)

After entering the policy rule configuration mode, to edit the policy rule, use the following commands:

- To add the source address of the IP member type: **src-ip** *ipv6-address/M*
- To delete the source address of the IP member type: **no src-ip** *ip-address/M*
- To add the source address of the IP range type: **src-range** *min-ipv6-address* [*max-ipv6-address*]
- To delete the source address of the IP range type: **no src-range** *min-ipv6-address* [*max-ipv6-address*]
- To add the destination address of the IP member type: **dst-ip** *ipv6-address/M*
- To delete the destination address of the IP member type: **no dst-ip** *ipv6-address/M*
- To add the destination address of the IP range type: **dst-range** *min-ipv6-address* [*max-ipv6-address*]
- To delete the destination address of the IP range type: **no dst-range** *min-ipv6-address* [*max-ipv6-address*]

Configuring Access Control for an IPv6 Policy

The combination of the ACL Profile and policy rule allows the Hillstone devices to access control over the IPv6 message based on an IPv6 policy, such as IPv6 extended header, source / destination MAC address etc.

To configure the access control function, take the following three steps:

1. Configure a ACL profile, which contains access control rules.
2. Configure an access control rule, which is used to specify the IPv6 extended message, rule type, and control action required to be controlled.
3. Binding the ACL profile to a policy rule. Only after the configured ACL profile is bound to a policy rule can access control function on the device.

Configuring an ACL Profile

The ACL profile needs to be configured in the ACL profile configuration mode. To enter the ACL profile configuration mode, in the global configuration mode, use the following command:

acl-profile *acl-profile-name*

- *acl-profile-name* – Specifies the name of the ACL profile. After executing the command, the system will create a ACL profile with the specified name, and enter the ACL profile configuration mode; if the specified name exists, the system will directly enter the ACL profile configuration mode. You can specify up to 64 ACL profiles.

To delete the specified ACL Profile, in the global configuration mode, use the command **no acl-profile** *acl-profile-name*.

Configuring an Access Control Rule

To configure an access control rule, in the ACL Profile configuration mode, use the following command:

sequence *id* {**drop** |**pass**} [**both** |**forward** |**backward**] [**src-mac** *src-mac-address*] [**dst-mac** *dst-mac-address*][**dscp** *dscp-value*] [**flow-label** *flow-label-value* [*end-flow-label-value*]] [**ext-header** [**ah**] [**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* |**home-address**]]][**mobility** [*mobility-value1 [mobility-value2*]|**bind-refresh** | **bind-ack** |**bink-err** | **bind-update** | **cot** | **coti**| **hot** |**hoti**]][**routing** [*routing-value1* [*routing-value2*]] [**no-recommended-order** | **recommended-order**]] [**single-ext-header** { **ah** | **dest** | **esp** |**fragment** | **hop** | **mobility** | **routing**} **number**{**equal** | **greater-than** | **less-than**} *number*] [**log**]

- *id* – Specifies the ID of the access control rule. .The range is 1 to 32.
- **drop** | **pass** – Specifies the action for the access control rule, drop or pass.
- **both** |**forward** |**backward** – Specifies the traffic direction of the access control rule.
- **src-mac** *src-mac-address* – Specifies the source MAC address of the access control rule.
- **dst-mac** *dst-mac-address* – Specifies the destination MAC address of the access control rule.
- **dscp** *dscp-value* – Specifies the DSCP value, the range is 0 to 63.
- **flow-label** *flow-label-value* [*end-flow-label-value*] – Specifies the IPv6 flow label or flow label range, the range is 0 to 1048575.
- [**ext-header** [**ah**][**fragment**][**esp**][**hop**][**none**][**dest** [*dest-value1* [*dest-value2* |**home-address**]]] [**mobility** [*mobility-value1 [mobility-value2*]|**bind-refresh** | **bind-ack** |**bink-err** | **bind-update** | **cot** | **coti**| **hot** |**hoti**]][**routing** [*routing-value1* [*routing-value2*]][**no-recommended-order** | **recommended-order**]] – Specifies the IPv6 extended header and parameter values.
- [**no-recommended-order** | **recommended-order**] - Specify whether the access control rule restricts the IPv6 message extension header to be arranged in recommended order-."recommend-order" means that the extension headers should be arranged in order. "**no-recommended-order**" means that the extension headers are arranged in non order, that is, out of order. If the restriction requirements are met, the system will process according to the action of the rule.

- [**single-ext-header** {**ah** | **dest** | **esp** |**fragment** | **hop** | **mobility** | **routing**} **number**{**equal** | **greater-than** | **less-than**} *number*] - Specify the number limit of single headers contained in IPv6 messages for the access control rule.
- **log** - System will log when the messages matching the access control rules.

To delete the specified access control rule, in the ACL Profile configuration mode, use the command **no sequence** *id*.

Configuring the Default Action

When there is no access control rule is hit, the system will take the specified default access control action. To configure the default action, in the ACL Profile configuration mode, use the following command:

default-action {**drop** |**pass**}

- **drop** | **pass** – Specifies the default action for the access control rule, drop or pass.

To delete the default action, in the ACL Profile configuration mode, use the command **no default-action**.

Binding the ACL Profile to a Policy Rule

The configured ACL profiles will not take effect until being bound to a policy rule. To bind an ACL Profile to a policy rule, in the policy configuration mode, use the following command:

acl *acl-profile-name*

- *acl-profile-name* – Specifies the name of the ACL profile that will be bound.

To cancel the binding,, in the ACL Profile configuration mode, use the command **no acl**.

Viewing ACL Profile Information

To view the ACL profile configuration, in any mode, use the following command:

show acl-profile [*acl-profile-name*]

- *acl-profile-name* – Shows the configuration of the specified ACL profile. If this parameter is not specifies, the command will show the configurations of all the ACL profiles.

Configuring IPv6 ALG

Compared with IPv4 ALG, the system supports IPv6 ALG for the following protocols: FTP, TFTP, HTTP, RSH, SIP, MSRPC, RTSP, SQLNetV2 and SUNRPC. Besides, you can also specify IPv6 addresses for the IPs that are not restricted by the URL filter. When configuring an ALG-related policy rule, make sure the rule references IPv6 addresses, for example, **rule from ipv6-any service to ipv6-any ftp permit**.



Notes: The ALG function of FTP, TFTP, HTTP, RSH, SIP, MSRPC, RTSP, SQLNetV2 and SUNRPC is enabled by default, while the ALG function of FTPS is disabled by default.

NDP Protection

NDP is a key IPv6 protocol, but it is not designed with any authentication mechanism, resulting in untrusted network nodes and attacks against the protocol. The main attacks include:

- Address spoofing: Attackers modify the MAC address of victim host by RS (Router Solicitation)/NS(Neighbor Solicitation)/NA(Neighbor Advertisement)/RA(Router Advertisement)/Redirect packets, or modify the MAC address of gateway by RS/NS/NA/RA packets, resulting in communication errors between the victim host and network.
- DAD attack: When the victim host performs DAD query, attackers interfere with the process by NS or NA packets, resulting in DAD failure and inability to obtain the IP address on the victim host.
- RA spoofing: Attackers launch spoofing attacks by forging RA packets, resulting in network configuration error on the victim host.

- Flooding: Attackers send huge amount of NS/RS/NA/RA packets to flood the ND table entries on the gateway.
- Redirection: Attackers use link layer address as the source address and send redirection packets to the victim host; when the victim host receives the erroneous redirection message, its routing table will be modified.

StoneOS provides a series of NDP protection measures for the above attacks to assure the security of IPv6 network, including:

- IP-MAC binding
- NDP learning
- NDP inspection
- NDP spoofing defense (NDP reverse query, IP number per MAC check, unsolicited NA packets rate)
- NDP spoofing statistics

You can adopt different protection measures for different network applications. For example, to implement Layer 2 NDP protection, you can enable NDP inspection (configuring an NDP packet rate limit, configuring a trusted interface, denying RA packets); to implement Layer 3 protection, you can disable NDP learning or dynamic entry learning, enable ND reverse query, or enable one-click binding to convert dynamic IP-MAC entries to static entries.

The following section describes the configuration and usage of the above protection measures.

IP-MAC Binding

To reinforce network security control, the device supports IP-MAC binding. The binding information can be obtained statically or dynamically: the information learned via NDP is known as dynamic binding information, and the information manually configured is known as static binding information. To simplify the configuration of static IP-MAC binding, you can convert the dynamic binding information to static binding information by one-click binding. Both the static and dynamic binding information is stored in the IPv6 ND cache table.

Adding a Static IP-MAC Binding Entry

To add a static IP-MAC binding entry to the cache table, in the global configuration mode, use the following command:

ipv6 neighbor *ipv6-address interface-name mac-address*

- *ipv6-address* – Specifies the IPv6 address of the static binding entry.
- *interface-name* – Specifies the interface of the static binding entry.
- *mac-address* – Specifies the MAC address of the static binding entry.

To delete the specified static IP-MAC binding entry, in the global configuration mode, use the following command:

no ipv6 neighbor {**all** | *ipv6-address interface-name*}

One-click Binding

One-click binding allows you to convert dynamic IP-MAC binding entries that are obtained via NDP learning to static binding entries when all the hosts in the Intranet can visit Internet. To configure one-click binding, in the execution mode, use the following command:

exec ipv6 nd-dynamic-to-static [**vrouter** *vr-name*]

- *vr-name* – Specifies the VRouter on which the function is implemented. The default value is the default VR **trust-vr**.

The above command will convert all the dynamic IP-MAC binding entries in the system to static binding entries.

Permitting Static IP-MAC Binding Hosts Only

By default the system allows hosts that are dynamically learned via NDP to visit Internet. To only allow hosts in the static IP-MAC binding entries to visit Internet, in the interface configuration mode, use the following command:

ipv6 nd-disable-dynamic-entry

To disable the function, in the interface configuration mode, use the following command:

no ipv6 nd-disable-dynamic-entry

Viewing IP-MAC Binding Information

To view IP-MAC binding information, in any mode, use the following command (if no parameter is specified, the command will show all the static and dynamic IP-MAC binding entries in the system):

show ipv6 neighbor [**generic** | **interface** *interface-name* | **slot** *slot-num* | **static** | **vrouter** *vr-name* | *ipv6-address*]

- **generic** – Shows IP-MAC binding entry statistics.
- **interface** *interface-name* – Shows IP-MAC binding entries of the specified interface.
- **slot** *slot-num* – Shows IP-MAC binding entries of the specified slot. Only for some devices (X series, K9180 and K6580 devices).
- **vrouter** *vr-name* – Shows IP-MAC binding entries of the specified VRouter.
- **static** – Shows IP-MAC binding entries.
- *ipv6-address* – Shows IP-MAC binding information of the specified IPv6 address.

Clearing Dynamic IP-MAC Binding Information

To clear dynamic IP-MAC binding information, in any mode, use the following command (if not parameter is specified, the command will clear all the dynamic IP-MAC binding information in the system):

clear ipv6 neighbor [*ipv6-address*]

- *ipv6-address* – Clears IP-MAC binding information of the specified IP address.

NDP Learning

Hillstone devices obtain IP-MAC binding information in the Intranet via ND learning, and add the binding information to the ND table. By default NDP learning is enabled, i.e., the device will keep on NDP learning and add all the learned IP-MAC binding information to the ND table. If any IP or MAC address changes during NDP learning, the device will update the IP-MAC binding information and add it to the ND table. With NDP learning disabled, the system will only allow hosts whose IP addresses are in the ND table to forward packets.

To configure NDP learning, in the interface configuration mode, use the following command:

- Enable: **ipv6 nd-learning**
- Disable: **no ipv6 nd-learning**

NDP Learning Limit

After the NDP learning function is enabled, when a user host that connects to the interface initiates NDP attacks, ND entry resources may be exhausted, making other interfaces unable to perform NDP learning. To avoid this issue, the system allows you to enable NDP learning limit and specify the maximum number of ND entries that can be learned on the interface. After a limit is specified, the interface can no longer perform NDP learning when the maximum number of ND entries is reached.

To enable the NDP learning limit function and specify the limit, in interface configuration mode, use the following command:

ipv6 nd-learning-limit *number*

- *number* - Specifies the maximum number of IP-MAC bindings that can be learned on the interface. Valid values: 1 to capacity. The capacity varies based on device platforms.

In interface configuration mode, use the **no ipv6 nd-learning-limit** command to disable the NDP learning limit function.

NDP Inspection

Hillstone devices support NDP inspection on interfaces. With this function enabled, the system will check all the NDP packets passing through the specified interface, and compare the IP addresses of the NDP packets with the static binding entries in the ND cache table:

- If the IP address is in the ND cache table, and the MAC address and interface of the packet are also consistent with the binding entry, then the system will forward the NDP packet;
- If the IP address is in the ND cache table, but the MAC address or interface of the packet is not consistent with the binding entry, then the system will drop the NDP packet;
- If the IP address is not in the ND cache table, then the system will drop or forward the packet according to the configuration (**ipv6 nd-inspection** {**drop** | **forward**}).

Enabling/Disabling NDP Inspection

The BGroup and VSwitch interfaces of StoneOS support NDP inspection. This function is disabled by default. To enable NDP inspection on a BGroup or VSwitch interface, in the BGroup or VSwitch interface configuration mode, use the following command:

ipv6 nd-inspection {**drop** | **forward**}

- **drop** – Drops NDP packets whose IP addresses are not in the ND cache table.
- **forward** – Forwards NDP packets whose IP addresses are not in the ND cache table.

To disable NDP inspection, in the BGroup or VSwitch interface configuration mode, use the following command:

no ipv6 nd-inspection

Configuring a Trusted Interface

You can configure a physical interface in BGroup or VSwitch as the trusted interface. Packets passing through the trusted interface are exempt from NDP inspection. By default all the inter-

faces on the device are untrusted. To configure a trusted interface, in the interface configuration mode, use the following command:

ipv6 nd-inspection trust

To cancel the specified trusted interface, in the interface configuration mode, use the following command:

no ipv6 nd-inspection trust

Denying RA Packets

To prevent interfaces from sending RA packets arbitrarily, you can specify to deny RA packets on some specific interfaces (physical interfaces only). Such a measure can prevent against RA attacks and improve LAN security effectively. To deny RA packets on an interface, in the interface configuration mode, use the following command:

ipv6 nd-inspection deny-ra

To cancel the above restriction, in the interface configuration mode, use the following command:

no ipv6 nd-inspection deny-ra

Configuring an NDP Packet Rate Limit

To configure an NDP packet rate limit, in the interface (physical interface only) configuration mode, use the following command:

ipv6 nd-inspection rate-limit *number*

- *number* – Specifies the number of NDP packets that are allowed per second. If the number of NDP packets received per second exceeds the value, the system will drop excessive NDP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

To cancel the specified rate limit, in the interface configuration mode, use the following command:

no ipv6 nd-inspection rate-limit

Viewing NDP Inspection Configuration

To view the NDP inspection configuration, in any mode, use the following command:

show ipv6 nd-inspection configuration

Configuring NDP Spoofing Defense

NDP spoofing defense is designed to protect Intranet from NDP spoofing attacks. To configure NDP spoofing defense, in the security zone configuration mode, use the following command:

ad ipv6 nd-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **unsolicited-na-send-rate** *number*}

- **reverse-query** – Enables reverse query. When the system receives an NDP request, it will log the IP address and reply with another NDP request; and then the system will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the NDP request packet. To disable the function, use the command **no ad ipv6 nd-spoofing reverse-query**.
- **ip-number-per-mac** *number* – Specifies whether to check the IP number per MAC in NDP table. If the parameter is set to 0 (the default value), the system will not check the IP number; if set to a value other than 0, the system will check the IP number, and if the IP number per MAC is larger than the parameter value, the system will take the action specified by action [**drop** | **alarm**]. The available actions include **drop** (give an alarm and drop the ARP packets) and **alarm** (give an alarm but still allow the packets to pass through). The value range is 0 to 1024. To restore to the default value, use the command **no ad ipv6 nd-spoofing ip-number-per-mac**.
- **unsolicited-na-send-rate** *number* – Specifies whether to send gratuitous NA packet(s). If the parameter is set to 0 (the default value), the system will not send any gratuitous NA packet; if set to a value other than 0, the system will send gratuitous NA packet(s), and the number sent

per second is the specified parameter value. The value range is 0 to 10. To restore to the default value, use the command **no ad ipv6 nd-spoofing unsolicited-na-send-rate**.

Viewing NDP Spoofing Statistics

After configuring NDP spoofing defense, to view attack statistics, use the following command:

show ipv6 nd-spoofing-statistics

NDP Spoofing Prevention

With NDP learning, NDP inspection and NDP spoofing defense configured, StoneOS is able to prevent against NDP attacks efficiently. Besides, the system also supports statistics on NDP spoofing attacks. To view NDP spoofing attack statistics, in any mode, use the following command:

show ipv6 nd-spoofing-statistics [*number*]

- *number* – Shows statistics of the top number records.

To clear NDP spoofing attack statistics, in any mode, use the following command:

clear ipv6 nd-spoofing-statistics

Configuring the Aging Time of ND Table Entries

ND table entries that are not used within a specified time will enter a "stale" state (neighbor reachability unknown status). In this state, ND table entries that exceed the aging time can be either deleted directly or subjected to validity detection. For detailed configuration, please refer to the Enabling/Disabling Validity Detection for Aged ND Table Entries. Configuring the valid time of ND table entries can automatically delete existing invalid ND table entry information to accelerate the aging process. The default aging time is 24 hours, which means that the reachability of neighbors will be re-detected or the "stale" ND table entries will be directly deleted every 24 hours.

To configure the aging time of ND table entries, in the Flow configuration mode, use the following command:

ipv6 nd stale-timeout *num*

- *num* - Specifies the aging time of the ND table entries. The value range is 60 to 86,400 seconds. The default value is 86,400 seconds.

To restore to the default value, in the Flow configuration mode, use the command **no ipv6 nd stale-timeout**.

Enabling/Disabling Validity Detection for Aged ND Table Entries

When an ND table entry is in the "stale" state and reaches the aging time, it is supported to configure whether to resend messages for validity detection. When validity detection is performed and the neighbor is reachable, the status of the ND table entry changes to "reach" (neighbor reachable status). Otherwise, the ND table entry is deleted. When validity detection is not performed, the ND table entry is directly deleted. By default, the system does not perform validity detection, that is, ND table entries that are in the "stale" state and have reached the aging time are directly deleted by default.

To enable validity detection for aged ND table entries, in the Flow configuration mode, use the following command:

ipv6 nd stale-timeout-probe

To disable validity detection for aged ND table entries, in the Flow configuration mode, use the following command: **no ipv6 nd stale-timeout-probe**.

Attack Defense

The system supports IPv6 attack defense functions listed in Table below. For more details and configuration, see "Attack Defense" of "Threat Prevention".

Attack defense	Configuration (in the security zone configuration mode)
Huge ICMP packet defense	**ad huge-icmp-pak** [**threshold** *number* | **action** {**alarm** | **drop**}]
IP sweeping defense	**ad ip-sweep** [**threshold** *value*| **action** {**alarm** | **drop**}]
L3 IP spoofing	**ad ip-spoofing**

Attack defense	Configuration (in the security zone configuration mode)
defense	
ICMP Flood defense	**ad icmp-flood** [**threshold** *number* | **action** {**alarm** | **drop**}]
UDP Flood defense	**ad udp-flood** [**threshold** *number* | **action** {**alarm** | **drop**}]
SYN Flood defense	**ad syn-flood** [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**} | **destination** [**ip-based** | **port-based** [**address-book** *address-book-name* | *ip-address/netmask*]]]
SYN-Proxy SYN-Cookie	**ad syn-proxy** [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** *number* | **cookie**]
Teardrop defense	**ad tear-drop**
IP fragment defense	**ad ip-fragment** [**action** {**alarm** | **drop**}]
Ping of Death defense	**ad ping-of-death**
Port scan defense	**ad port-scan** [**threshold** *value* | **action** {**alarm** | **drop**}]
TCP anomaly defense	**ad tcp-anomaly** [**action** {**alarm** | **drop**}]
TCP Split Hand-shake defense	**ad tcp-split-handshake** [**action** {**alarm** | **drop**}]
IP Option defense	**ad ip-option** [**action** {**alarm** | **drop**}]

Attack defense	Configuration (in the security zone configuration mode)
DNS Query Flood defense	**ad dns-query-flood** [**recursion**] [**source-threshold***number*] [**destination-threshold***number* | **action** {**alarm** | **drop**}]
DNS Reply Flood defense	**ad dns-reply-flood** [**source-threshold** *number*] [**destination-threshold** *number* | **action** { **alarm** | **drop** }]
Land attack defense	**ad land-attack** [**action** {**alarm** | **drop**}]

IPv6 over IPv4 Tunnel

At the time of writing IPv4 networks are still mainstream networks, while IPv6 networks are comparatively isolated. IPv6 over IPv4 tunnel allows IPv6 packets to be transmitted via IPv4 networks, enabling communication between isolated IPv6 networks via IPv4 networks. The system supports to configure the following IPv6 over IPv4 tunnels:

- Configuring an Automatic 6to4 Tunnel
- Configuring a Manual 6to4 Tunnel
- Configuring an ISATAP Tunnel
- Configuring a 6RD Tunnel

Configuring an Automatic 6to4 Tunnel

Automatic 6to4 tunnel is an automatic one-to-many tunnel that is used to connect multiple isolated IPv6 networks via IPv4 networks. Hillstone devices can either be used as 6to4 routes or 6to4 relay routers, specifically relying on network environment.

The configuration of automatic 6to4 tunnel includes:

- Creating a tunnel
- Specifying IPv6 6to4 Subtunnel Limit

- Specifying an egress interface
- Binding a tunnel to the tunnel interface

Creating a Tunnel

To create an IPv6 automatic 6to4 tunnel, in the global configuration mode, use the following command, after executing which, the system will create an IPv6 automatic 6to4 tunnel with the specified name and enter tunnel configuration mode. If the specified name already exists, the system will directly enter tunnel configuration mode.

tunnel ipv6-over-ipv4 *tunnel-name* **6to4**

- *tunnel-name* – Specifies the name of the IPv6 automatic 6to4 tunnel.
- **6to4** – Specifies the tunnel type to be automatic 6to4 tunnel.

In the global mode, use the no form of the above command to delete the specified IPv6 automatic 6to4 tunnel:

no tunnel ipv6-over-ipv4*tunnel-name***6to4**

Specifying IPv6 6to4 Subtunnel Limit

Each automatic 6to4 tunnel can have a maximum of 1200 sub-tunnels. To specify the subtunnel number of a 6to4 tunnel, in the tunnel configuration mode, use the following command:

subtunnel-limit*maximum*

- *maximum* - Specifies the subtunnel number of a automatic 6to4 tunnel. The value rang is 1 to 1,200, and the default value is 200.

In the tunnel configuration mode, use the following command to resume the default value:

no subtunnel-limit

Specifying an Egress Interface

To specify an egress interface for the tunnel, in the tunnel configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface).

To cancel the specified egress interface, in the tunnel configuration mode, use the following command:

no interface

Binding an IPv6 Automatic 6to4 tunnel to the Tunnel Interface

The configured IPv6 automatic 6to4 tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one IPv6 automatic 6to4 tunnel at most. To bind an IPv6 automatic 6to4 tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command under global configuration mode and use the following command:

tunnel ipv6-over-ipv4*ipv6-tunnel-name*

- *ipv6-tunnel-name* – Specifies the name of IPv6 automatic 6to4 tunnel.

To cancel the binding between the IPv6 automatic 6to4 tunnel and tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv6-over-ipv4*ipv6-tunnel-name*

Showing Configuration Information About IPv6 Automatic 6to4 Tunnel

To show the configuration information about the IPv6 automatic 6to4 tunnel, in any mode, use the following command:

show ipv6-over-ipv46to4-tunnel

Configuring a Manual 6to4 Tunnel

Manual 6to4 tunnel provides point-to-point connection. The end point of the tunnel is manually configured.

The configuration of manual 6to4 tunnel includes:

- Creating a tunnel
- Specifying an egress interface
- Specifying a destination address for the manual tunnel
- Binding a tunnel to the tunnel interface

Creating a tunnel

To create an IPv6 manual 6to4 tunnel, in the global configuration mode, use the following command, after executing which, the system will create an IPv6 manual 6to4 tunnel with the specified name and enter tunnel configuration mode. If the specified name already exists, the system will directly enter tunnel configuration mode.

tunnel ipv6-over-ipv4 *tunnel-name* **manual**

- *tunnel-name* – Specifies the name of the IPv6 manual 6to4 tunnel.
- **manual** – Specifies the tunnel type to be manual 6to4 tunnel.

In the global mode, use the no form of the above command to delete the specified IPv6 manual 6to4 tunnel:

no tunnel ipv6-over-ipv4*tunnel-name***manual**

Specifying an Egress Interface

To specify an egress interface for the tunnel, in the tunnel configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface).

To cancel the specified egress interface, in the tunnel configuration mode, use the following command:

no interface

Specifying a Destination Address for the Manual Tunnel

The destination address of automatic 6to4 tunnel can be obtained automatically by the IPv4 address embedded in the compatible IPv6 address. Therefore, you need not to specify the destination for the automatic 6to4 tunnel. To specify a destination address for the IPv6 manual 6to4 tunnel, in the tunnel configuration mode, use the following command:

destination*ipv4-address*

- *ipv4-address* – Specifies a destination address (must be an IPv4 address) for the manual tunnel.

To cancel the specified destination address, in the tunnel configuration mode, use the following command:

no destination

Binding an IPv6 Manual 6to4 tunnel to the Tunnel Interface

The configured IPv6 manual 6to4 tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one IPv6 manual 6to4 tunnel at most. To bind an IPv6 manual 6to4 tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command in the global configuration mode and use the following command:

tunnel ipv6-over-ipv4*ipv6-tunnel-name*

- *ipv6-tunnel-name* – Specifies the name of IPv6 manual 6to4 tunnel.

To cancel the binding between the IPv6 manual 6to4 tunnel and tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv6-over-ipv4*ipv6-tunnel-name*

Showing Configuration Information About IPv6 Manual 6to4 Tunnel

To show the configuration information about the IPv6 manual 6to4 tunnel, in any mode, use the following command:

show ipv6-over-ipv4manual-tunnel

IPv4 over IPv6 Tunnel

At the time of writing, IPv4 networks are still mainstream networks, while the application of IPv6 networks keeps growing. To solve the problems caused by wide deployment of IPv6 networks, StoneOS supports IPv4 over IPv6 tunnel technique to enable communication between isolated IPv4 networks via IPv6 networks.

The system only supports to configure the following IPv4 over IPv6 tunnels.

- Configuring a Manual 4to6 Tunnel
- Configuring a DS-lite Tunnel

Configuring a Manual 4to6 Tunnel

Manual 4to6 tunnel provides point-to-point connection. The end point of the tunnel is manually configured.

The configuration of manual 4to6 tunnel includes:

- Creating a tunnel
- Specifying a source address/interface for the tunnel
- Specifying a destination address for the tunnel
- Binding a tunnel to the tunnel interface

Creating a tunnel

To create an IPv6 manual 4to6 tunnel, in the global configuration mode, use the following command, after executing which, the system will create an IPv6 manual 4to6 tunnel with the specified name and enter tunnel configuration mode. If the specified name already exists, the system will directly enter tunnel configuration mode.

tunnel ipv4-over-ipv6 *tunnel-name* **manual**

- *tunnel-name* – Specifies the name of IPv6 manual 4to6 tunnel.

To delete the specified IPv6 manual 4to6 tunnel, in the global configuration mode, use the following command:

no tunnel ipv4-over-ipv6 *tunnel-name* **manual**

Specifying the Source Address/Egress Interface

To specify the egress interface and source address of IPv6 manual 4to6 tunnels, under tunnel configuration mode, use the following command:

interface *interface-name* **source** *ipv6-address*

- *interface-name* – Specifies the egress interface for the tunnel.
- *ipv6-address* – Specfies the source address of IPv6 4to6 tunnel. This address should be an IPv6 address.

Under tunnel configuration mode, use the command to delete egress interface and source address:

no interface

Specifying a Destination Address for the Tunnel

To specify a destination address for the IPv6 manual 4to6 tunnel, in the tunnel configuration mode, use the following command:

destination *ipv6-address*

- *ipv6-address* – Specifies a destination address (must be an IPv6 address) for the IPv6 manual 4to6 tunnel.

To cancel the specified destination address, in the tunnel configuration mode, use the following command:

no destination

Binding an IPv6 manual 4to6 Tunnel to the Tunnel Interface

The configured IPv6 manual 4to6 tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one IPv6 manual 4to6 tunnel at most. To bind an IPv6 manual 4to6 tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command in the global configuration mode and use the following command:

tunnel ipv4-over-ipv6 *tunnel-name*

- *tunnel-name* – Specifies the name of IPv6 4to6 tunnel.

To cancel the binding between the IPv6 4to6 tunnel and tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv4-over-ipv6 *tunnel-name*

Showing the Configuration Information About the IPv6 Manual 4to6 Tunnel

To show the configuration information about the IPv6 manual 4to6 tunnel, in any mode, use the following command:

show ipv4-over-ipv6 manual-tunnel

Configuring a 6RD Tunnel

6RD (IPv6 Rapid Deployment on IPv4 Infrastructures) is a stateless tunneling mechanism, allowing a service provider to quickly and securely deploy IPv6 without upgrading existing IPv4 access network infrastructures.

6RD builds on the 6to4 tunneling mechanism. It uses a service provider's own IPv6 prefix rather than the fixed prefix (2002::/16) of the automatic 6to4 tunnel. This not only resolves the IPv4 address exhaustion problem, but also conquers the disadvantage that automatic 6to4 tunnels use the fixed well-known IPv6 prefix on all 6to4 sites. From the perspective of customer sites and the IPv6 Internet at large, the IPv6 service provided is equivalent to native IPv6.

The IPv6 address of 6RD is composed of the delegated prefix and the subnet ID. The delegated prefix is calculated by combining the 6RD prefix and a consecutive set of bits from the IPv4 address. The 6RD prefix is obtained from a service provider, and the IPv4 bits are obtained from all or part of the IPv4 address. The number of IPv4 bits needed depends on the IPv4 prefix length configured for the 6RD tunnel.

The format of 6RD IPv6 address is as follows.



6RD application scenarios include:

- 6RD tunnel: 6RD can be used for interconnection between 6RD domains. A 6RD domain consists of 6RD CE (Customer Edge) routers and one or more 6RD BRs (Border Relays). Each 6RD domain uses a specific 6RD prefix. Devices on the two sides of a 6RD tunnel are both 6RD CEs or both 6RD BRs.
- 6RD relay: 6RD can be used for interconnection between a 6RD domain and an IPv6 native network. The device on one side of the 6RD tunnel is a 6RD CE, and on the other side is a 6RD BR.

The configuration of 6RD tunnel includes:

- Creating a 6RD tunnel
- Specifying an egress interface of the 6RD tunnel
- Specifying a 6RD prefix
- Specifying the IPv4 prefix length

- Binding the 6RD tunnel to a tunnel interface
- Configuring the IPv4 address of the BR (for the 6RD relay application scenario)

Creating a 6RD Tunnel

To create a 6RD tunnel, in the global configuration mode, use the following command, after executing which, the system will create a 6RD tunnel with the specified name and enter tunnel configuration mode. If the specified name already exists, the system will directly enter tunnel configuration mode.

tunnel ipv6-over-ipv4*tunnel-name***6rd**

- *tunnel-name*- Specifies the name of a 6RD tunnel.

To delete the specified 6RD tunnel, in the global configuration mode, use the following command:

no tunnel ipv6-over-ipv4*tunnel-name***6rd**

Specifying an Egress Interface of the 6RD Tunnel

To specify an egress interface of the 6RD tunnel, in the 6RD tunnel configuration mode, use the following command:

interface*interface-name*

- *interface-name* - Specifies the egress interface name of the 6RD tunnel.

To delete the egress interface of the 6RD tunnel, in the 6RD tunnel configuration mode, use the following command:

no interface

Specifying a 6RD Prefix

To specify a 6RD prefix, in the 6RD tunnel configuration mode, use the following command:

ipv6-prefix*ipv6-prefix / prefix-length*

- *ipv6-prefix / prefix-length* - Specifies a 6RD prefix and the prefix length, which are used for matching 6RD packets, in the format of "X:X:X:X:X:X:X:X/M". A 6RD prefix is assigned by a service provider. The value of prefix length ranges from 1 to 63.

To delete the configuration of the 6RD prefix, in the 6RD tunnel configuration mode, use the following command:

no ipv6-prefix

Specifying the IPv4 Prefix Length

To specify the IPv4 prefix length, in the 6RD tunnel configuration mode, use the following command:

ipv4-mask-len*prefix-length*

- *prefix-length* - Specifies the IPv4 prefix length. The value ranges from 0 to 31.

To delete the configuration of IPv4 prefix length, in the 6RD tunnel configuration mode, use the following command:

no ipv4-mask-len

Configuring the BR's IPv4 Address

In the 6RD relay application scenario, when the destination IP address of 6RD packets fails to match the 6RD prefix, the BR's IPv4 address will be used as the destination IPv4 address of the outer-layer IPv4 packets.

To configure the IPv4 address of the BR, in the 6RD tunnel configuration mode, use the following command:

border-relay-address*ipv4-address*

- *ipv4-address* - Specifies the BR's IPv4 address, in the format of "x.x.x.x".

To delete the configuration of the BR's IPv4 address, in the 6RD tunnel configuration mode, use the following command:

no border-relay-address

Specifying 6RD Subtunnel Limit

To specify the maximum number of 6RD subtunnels, in the 6RD tunnel configuration mode, use the following command:

subtunnel-limit *maximum*

- *maximum* - Specifies the maximum number of 6RD subtunnels. The value ranges from 1 to 1,200. The default value is 200.

In the 6RD tunnel configuration mode, use the following command to restore to the default maximum number of 6RD subtunnels:

no subtunnel-limit

Binding the 6RD Tunnel to a Tunnel Interface

The configured 6RD tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one 6RD tunnel at most. To bind a 6RD tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command under global configuration mode and use the following command:

tunnel ipv6-over-ipv4 *tunnel-name*

- *tunnel-name* - Specifies the 6RD tunnel name.

To cancel the binding between the 6RD tunnel and the tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv6-over-ipv4 *tunnel-name*

Showing the Configuration Information About the 6RD Tunnel

To show the configuration information about the 6RD tunnel, in any mode, use the following command:

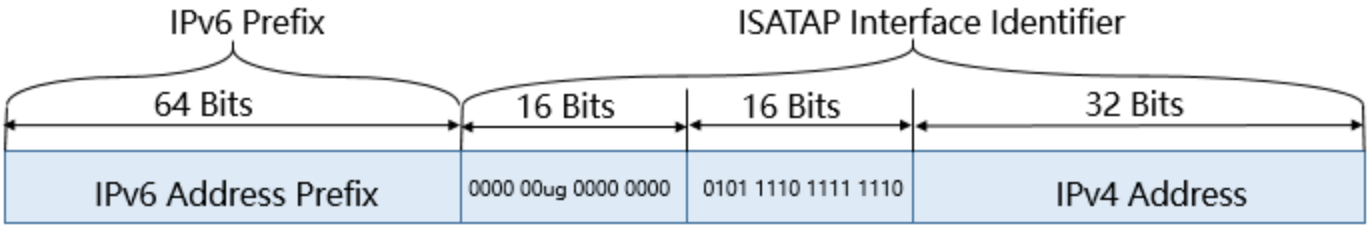
show ipv6-over-ipv4 6rd-tunnel [*tunnel-name*]

- *tunnel-name* - Displays the detailed configurations of the 6RD tunnel with the specified name. If the tunnel name is not specified, this command will display all 6RD tunnels that have been configured.

Configuring an ISATAP Tunnel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is a auto tunnel technology of IPv6 point-to-multipoint. It's mainly used for the dual-stack host in the IPv4 networks to visit IPv6 networks. With the technology, the dual-stack host can obtain the terminal of tunnel automatically via the embedded IPv4 address in the destination address of IPv6 packets.

When ISATAP tunnel is built, both the destination address of IPv6 packets and IPv6 address of the tunnel interface need the special ISATAP address. The ISATAP address contains the IPv6 prefix and ISATAP interface identifier. The formats of ISATAP address are as follows:



- If the IPv4 address is globally unique, the **u** bit is 1, otherwise, it is 0.
- The **g** bit means an IEEE (Institute of Electrical and Electronic Engineers) group or individual ID, which is 0 all the time.

For example, the prefix of IPv6 is 2001:DB8:1234:5678::/64 and the IPv4 address needs to be embedded is 10.173.129.8, which can be identified as 0AAD:8108 (hexadecimal), the ISATAP address is 2001:DB8:1234:5678:0000:5EFE: 0AAD:8108.

The configuration of ISATAP tunnel includes:

- Creating an ISATAP Tunnel
- Specifying ISATAP Subtunnel Limit
- Specifying an Egress Interface of ISATAP Tunnel
- Binding an ISATAP Tunnel to the Tunnel Interface

Creating an ISATAP Tunnel

To create an ISATAP tunnel, in the global configuration mode, use the following command. After the command is executed, the system will create an ISATAP tunnel with the specified name and enter the ISATAP tunnel configuration mode; if the specified name already exists, the system will directly enter the ISATAP tunnel configuration mode.

tunnel ipv6-over-ipv4 *tunnel-name* **isatap**

- *tunnel-name* – Specifies the name of ISATAP tunnel.
- **isatap** – Specifies the tunnel type to be ISATAP tunnel.

To delete the specified ISATAP tunnel, in the global configuration mode, use the following command:

no tunnel ipv6-over-ipv4*tunnel-name***isatap**

Specifying ISATAP Subtunnel Limit

To specify the subtunnel number of a ISATAP tunnel, in the ISATAP tunnel configuration mode, use the following command:

subtunnel-limit*maximum*

- *maximum* – Specifies the number of subtunnels for an ISATAP tunnel. The value range is 1 to 1,200, and the default value is 200.

In the ISATAP tunnel configuration mode, use the following command to resume the default value:

no subtunnel-limit

Specifying an Egress Interface of ISATAP Tunnel

To specify an egress interface for the ISATAP tunnel, in the ISATAP tunnel configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of egress interface, which can be a physical interface or logical interface (except tunnel interface).

To cancel the specified egress interface, in the ISATAP tunnel configuration mode, use the following command:

no interface

Binding an ISATAP tunnel to the Tunnel Interface

The configured ISATAP tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one ISATAP tunnel at most. To bind an ISATAP tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command under global configuration mode and use the following command:

tunnel ipv6-over-ipv4 *ipv6-tunnel-name*

- *ipv6-tunnel-name* – Specifies the name of ISATAP tunnel.

To cancel the binding between the ISATAP tunnel and tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv6-over-ipv4 *ipv6-tunnel-name*

Showing Configuration Information About the ISATAP Tunnel

To show the configuration information about the ISATAP tunnel, in any mode, use the following command:

show ipv6-over-ipv4isatap-tunnel

Configuring a DS-lite Tunnel

StoneOS supports DS-lite technology. DS-lite integrates with IPv4-in-IPv6 tunnel with NAT. The IPv4 client uses the B4 (Base Bridge Broadband) device and the AFTP (Address Family Transition Router) device to create a tunnel in the IPv6 network. And then it uses this tunnel to communicate with the resource in the IPv4 network. In the end point of this tunnel, the AFTR device uses NAT to translate the private IPv4 address.

Hillstone device can act as the AFTR device to support DS-lite and NAT. Configuring DS-lite includes the following sections:

- Creating a DS-lite tunnel
- Specifying an interface and IP address for the DS-lite tunnel
- Specifying DS-lite Subtunnel Limit
- Binding a DS-lite Tunnel to the Tunnel Interface

When using DS-lite, you must also configure the corresponding NAT settings.

Creating a DS-lite Tunnel

Each device supports to create up to 10 DS-lite tunnels. To create a DS-lite tunnel, in the global configuration mode, use the following command, after executing which, the system will create a DS-lite tunnel with the specified name and enter DS-lite tunnel configuration mode. If the specified name already exists, the system will directly enter DS-lite tunnel configuration mode.

tunnel ipv4-over-ipv6 *tunne-name* **ds-lite**

- *tunnel-name* – Specifies the name of the DS-lite tunnel.

To delete a tunnel, use the following command in the global configuration mode:

no tunnel ipv4-over-ipv6 *tunnel-name* **ds-lite**

Specifying an Interface and IP Address for the DS-lite Tunnel

To specify an interface and IP address for the DS-lite tunnel, use the following command in the DS-lite tunnel configuration mode:

interface *interface-name* **src-ip** *X:X:X:X::X*

- *interface-name* - Specifies the egress interface for the DS-lite.
- *X:X:X:X::X* – Specifies the IPv6 address owned by this egress interface.

To cancel the above settings, use the **no interface** command in the DS-lite tunnel configuration mode.

Specifying DS-lite Subtunnel Limit

When a B4 device accesses the DS-lite tunnel, AFTR will dynamically create a sub tunnel. To specify the maximum number of sub tunnels, use the following command in the DS-lite tunnel configuration mode:

subtunnel-limit*value*

- *value* – Specifies the maximum number of sub tunnels that AFTR can create. The default value is 200. The value ranges from 1 to 1,200.

Use the **no** form to restore the value to the default one.

Binding a DS-lite Tunnel to the Tunnel Interface

The configured DS-lite tunnel will only take effect after being bound to the tunnel interface. Each tunnel interface can bind only one DS-lite tunnel at most. To bind a DS-lite tunnel to a tunnel interface, enter the tunnel interface configuration mode using the **interface tunnel***X* command in the global configuration mode and use the following command:

tunnel ipv4-over-ipv6*tunnel-name*

- *tunnel-name* – Specifies the name of the DS-lite tunnel.

To cancel the binding between the DS-lite tunnel and tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel ipv4-over-ipv6*tunnel-name*

Showing Configuration Information About the DS-lite Tunnel

To show the configuration information of the DS-lite tunnel, in any mode, use the following command:

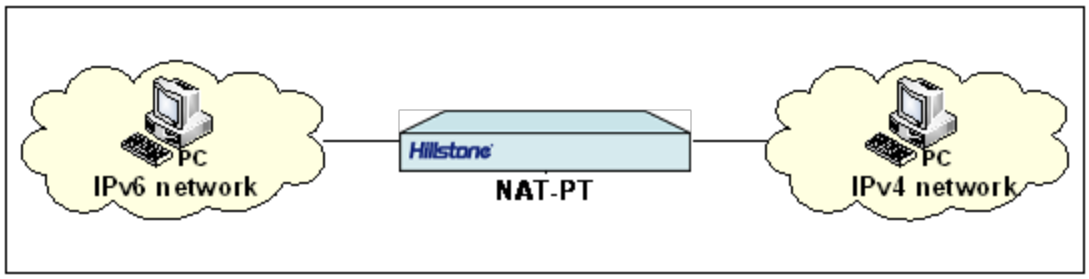
show ipv4-over-ipv6 ds-lite-tunnel

Configuring NAT-PT

IPv6 can solve the problem of increasingly exhausted IP addresses, and will replace IPv4 to become the core of next generation Internet. However, it’s not possible to upgrade the existing

IPv4 networks to IPv6 networks overnight; for quite a long time, IPv6 and IPv4 networks will co-exist and communicate with each other.

NAT-PT (Network Address Translation - Protocol Translation) is a transitional mechanism that is designed for the inter-communication between pure IPv6 and IPv4 networks. NAT-PT adopts NAT for the translation between IPv4 and IPv6 addresses, and adopts PT for the translation of protocols (including network layer protocols, transport layer protocols and application layer protocols) on the basis of semantically equivalent rules. Powered by NAT-PT, you can implement the inter-communication between IPv6 and IPv4 networks without any change to the existing IPv4 networks. Figure below shows an illustration of intercommunication between a pure IPv6 and IPv4 network via a Hillstone device with NAT-PT enabled.



Notes: NAT-PT on the current firmware version supports translation of IP, TCP, UDP and ICMP protocols, and supports FTP-ALG, TFTP-ALG and HTTP-ALG controls.

Configuring a NAT-PT Rule

NAT-PT rules are created based on VRouters. You can create, move and delete SNAT/DNAT rules in the VRouter configuration mode.

To enter the VRouter configuration mode, in the global configuration mode, use the following command:

ip vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of VRouter.

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT-PT on the source IPv6/IPv4 address of the matched traffic. If NAT-PT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule for NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id***id*] [**before** *id* | **after** *id* | **top**] **from** *src-address***to***dst-address* [**eif***egress-interface* | **evr***vrouter-name*] **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip**| **eif-ipv6**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**] [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*] } [**log**] [**group** *group-id*][**description** *description*]

- **id** *id* – Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **before** *id*, **after** *id*, **top**. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions include:
  - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.
- **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip**| **eif-ipv6**} – Specifies the translated IP address. It can be an IPv4 or IPv6 address, an address entry in the address book,

the IP address of the egress interface (**eif-ip**), or the IPv6 address of the egress interface (**eif-ipv6**). When you configure the NAT46, system does not support to specifies the **eif-ip**. When you configure the NAT64, system does not support to specifies the **eif-ipv6**..

- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**] [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*] } – Specifies the translation mode. StoneOS supports three modes for the translation between IPv4 and IPv6 addresses: static, dynamicip and dynamicport. For more details, see the table below:
  - **static** - Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same number of IP addresses as that of the source address entry (*src-address*).
  - **dynamicip** - Dynamic IP mode means many-to-many translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
  - **dynamicport** - Namely NAPT-PT (Network Address Port Translation - Protocol Translation). Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is not enabled, the system will select an IP address in the address entry, when port resources of the first address are exhausted, the second address will be used. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. When configuring the SNAT rule of NAT64, you can specify the static port block mapping mode by configuring [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*. The static port block mapping mode means each source IP address corresponds to a fixed port block of the mapped IP. **start** *start-port* **end** *end-port* specifies the start port and end port of the available port range. The value range is 1024 to 65535. **size** *port-block-size* specifies the size of the port block. The value range is 64 to 64512, and the value must be the integer multiple of 64.

- **log** – Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule).
- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config-vrouter)# snatrule from ipv6-any to ipv6-any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

Moving an SNAT Rule

Each SNAT rule is labeled with a unique ID. When traffic flows into the Hillstone device, the device will query for SNAT rules in the list by turns, and then implement NAT-PT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show snat is the query sequence for the matching. You can move an SNAT rule to modify the matching sequence. To move an SNAT rule, in the VRouter configuration mode, use the following command:

snatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the SNAT rule that will be moved.
- **before** *id* – Moves the SNAT rule before the specified ID.
- **after** *id* – Moves the SNAT rule after the specified ID.
- **top** – Moves the SNAT rule to the top of the SNAT rule list.
- **bottom** – Moves the SNAT rule to the bottom of the SNAT rule list.

Deleting an SNAT Rule

To delete the SNAT rule with the specified ID, in the VRouter configuration mode, use the following command:

no snatrule id *id*

Viewing SNAT Configuration Information

To view the SNAT configuration information, in any mode, use the following command:

show snat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – Shows the SNAT rule information of the specified ID.
- **vrouter** *vrouter-name* – Shows the SNAT configuration information of the specified VRouter.

When the SNAT translation mode is set to dynamicport, to view the usage of port resources in the source address pool, in any mode, use the following command:

show snat resource [**vrouter** *vrouter-name*]

- **vrouter** *vrouter-name* – Shows the port usage of SNAT source address pool of the specified VRouter.

Creating a DNAT Rule

DNAT rules are used to specify whether to implement NAT-PT on the destination IPv6/IPv4 address of the matched traffic. To configure a DNAT rule for NAT-PT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- id id – Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the

original rule will be overwritten.

- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules. When traffic flows into the Hillstone device, the device will query for DNAT rules in the list by turns, and then implement NAT on the destination IP of the traffic according to the first matched rule.
- **from** *src-address* **to** *dst-address* [**service** *service-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* – Specifies the source IP address of the traffic. *src-address* should be an IPv4 or IPv6 address, or an address entry in the address book.
  - **to** *dst-address* – Specifies the destination IP address of the traffic. *dst-address* should be an IPv4 or IPv6 address, or an address entry in the address book.
  - **service** *service-name* – Specifies the service type of the traffic. If the port number needs to be translated together (specified by **port** *port*), the specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.
- **trans-to** *trans-to-address* – Specifies the translated IP address. *trans-to-address* should be an IPv4 or IPv6 address, or an address entry in the address book. The number of this translated IP address must be the same as that of the destination IP address of the traffic (specified by **to** *dst-address*).
- **port** *port* – Specifies port number of the internal network server.
- **load-balance** – Enables load balancing for this DNAT rule, i.e., balances the traffic to different servers in the internal network.

- **track-tcp** *port* – If this parameter is configured and the port number of the internal network server is specified, the system will send TCP packets to the internal network server to monitor if the specified TCP port is reachable.
- **track-ping** – If this parameter is configured, the system will send ping packets to the internal network server to monitor if the server is reachable.
- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this DNAT rule).
- **group** *group-id* - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.

For example, the following command will translate the IP address of the request from addr1 to the IP address of addr2, but will not translate the port number:

```
hostname(config-vrouter)# dnatrule from ipv6-any to addr1 service any trans-to addr2
rule id=1
```

To configure a DNAT rule that disables NAT-PT, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **no-trans** [**group** *group-id*]

Moving a DNAT Rule

Each DNAT rule is labeled with a unique ID. When traffic flowing into the Hillstone device, the device will query for DNAT rules by turns, and then implement NAT on the source IP of the traffic according to the first matched rule. However, the rule ID is not related to the matching sequence during the query. The sequence displayed by the command show dnat is the query sequence for the matching. You can move a DNAT rule to modify the matching sequence. To move a DNAT rule, in the VRouter configuration mode, use the following command:

dnatrule move *id* {**before** *id* | **after** *id*| **top** | **bottom**}

- *id* – Specifies the ID of the DNAT rule that will be moved.
- **before** *id* – Moves the DNAT rule before the specified ID.
- **after** *id* – Moves the DNAT rule after the specified ID.
- **top** – Moves the DNAT rule to the top of the DNAT rule list.
- **bottom** – Moves the DNAT rule to the bottom of the DNAT rule list.

Deleting a DNAT Rule

To delete the DNAT rule with the specified ID, in the VRouter configuration mode, use the following command:

no dnatrule id *id*

Viewing DNAT Configuration Information

To view the DNAT configuration information, in any mode, use the following command:

show dnat [**id** *id*] [**vrouter** *vrouter-name*]

- **id** *id* – Shows the DNAT rule information of the specified ID.
- **vrouter** *vrouter-name* – Shows the DNAT configuration information of the specified VRouter.

To show the information of the DNAT rule with load balancing configured, in any mode, use the following command:

show dnat server [*ip-address*] [**vrouter** *vrouter-name*] [**tcp-port** *port*] [**ping**]

- *ip-address* – Shows status of the internal network server of the specified IP address.
- **vrouter** *vrouter-name* – Shows status of the internal network server of the specified VRouter.
- **tcp-port** *port* – Shows status of the internal network server of the specified port number.
- **ping** – Shows ping monitor status of the internal network server.

Configuring DNS64 and NAT64

DNS64 and NAT64 are transitional mechanisms for the intercommunication between IPv6-only and IPv4-only networks. These mechanisms are designed to support IPv6 clients' request for network resources on IPv4 servers, and addresses most of the deficiencies of NAT-PT in the intercommunication between IPv6 and IPv4 networks.

If the IPv6 client host receives the DNS query request, it will use DNS64 to resolve the AAAA record (IPv6 address) in the DNS query information. If the resolution is successful, the IPv6 address is directly returned to the client. If the resolution fails, it will use DNS64 to resolve the A record (IPv4 address) in the DNS query information, and return the A record (IPv4 address) to the AAAA record (IPv6 address) to the client.

NAT64 works with DNS64, NAT64 is mainly used for the address translation from IPv6 to IPv4 addresses. During source address translation, NAT64 translates source IPv6 addresses to source IPv4 addresses via the IPv4 address pool; during destination address translation, NAT64 directly extracts destination IPv4 addresses from the IPv6 addresses returned by DNS64.

DNS64 and NAT64 on Hillstone devices are implemented by combining IPv6 DNS proxy rules and configuring DNS64 functionality and NAT64 rules. NAT64 rules include SNAT and DNAT rules. The configuration of SNAT rules is the same as that of SNAT rules in NAT-PT. For more information, see "Creating an SNAT Rule" of "Firewall".

Enabling/Disabling DNS64

After configuring the IPv6 DNS proxy rules, you can enable or disable the DNS64. By default, the DNS64 function is disabled. In DNS proxy rule configuration mode, use the following command:

- Enable: **dns64 enable** (After executing this command, system will enter the DNS64 configuration mode.)
- Disable: **no dns64 enable**



Notes: The DNS64 function is only supported in IPv6 DNS proxy rules and is not supported in IPv4 DNS proxy rules.

Configuring DNS64 Server

The DNS64 server is used to resolve the A record (IPv4 address) in the DNS query information. Each IPv6 DNS proxy rule can specify up to 6 DNS64 servers. To configure the DNS64 server, in the DNS64 configuration mode, use the following command:

server *server-ip* [**vrouter***vrouter-name*]

- *server-ip* – Specifies the IP address of DNS64 server, this IP address can only be an IPv4 address.
- *vrouter-name* – Specifies a VRouter for the DNS64 server.

To delete the DNS64 server, in the DNS64 configuration mode, use the command**no server***server-ip* [**vrouter***vrouter-name*].

Configuring DNS64 Prefix

You need to specify the DNS64 prefix to synthesize the A record (IPv4 address) into an AAAA record (IPv6 address). The synthesized IPv6 address is in the form of "DNS64 prefix + IPv4 address". By default, the DNS64 prefix is "64:ff9b::/96". To specify the DNS64 prefix and prefix length, in the DNS64 configuration mode, use the following command:

prefix *ipv6-address/Mask*

- *ipv6-address* – Specifies the DNS64 prefix address.
- *Mask* – Specifies the prefix length, the range is 1 to 96.

To delete the DNS64 prefix configuration, in the DNS64 configuration mode, use the command**no prefix***ipv6-address/Mask*.

Creating a DNS64 Rule

Only be available on some firmwares. To create a DNS64 rule, in the global configuration mode, use the following command:

ipv6 dns64-proxy id *id* **prefix** *ipv6-address/Mask* [**source** {*ipv6-address/Mask* | *address-entry-v6*} | **trans-mapped-ip** {*ipv4-address/Mask* | *address-entry-v4*}]

- **id** *id* – Specifies the ID of the DNS64 rule. The value range is 1 to 16. Each DNS64 rule has a unique ID. If the specified DNS64 ID exists, the original rule will be overwritten.
- **prefix** *ipv6-address/Mask* – Specifies the IPv6 prefix and length of the prefix. DNS64 uses the prefix to translate IPv4 addresses to IPv6 addresses. The value range of prefix length is 0 to 96.
- **source** {*ipv6-address/Mask* | *address-entry-v6*} – Specifies the source IP address of traffic which can be an IPv6 address or an IPv6 address entry in the address book.
- **trans-mapped-ip** {*ipv4-address/Mask* | *address-entry-v4*} – Specifies the response address of IPv4 DNS server which can be an IPv4 address or an IPv4 address entry in the address book.

To delete the specified DNS64 rule, in the global configuration mode, use the following command:

no ipv6 dns64-proxy id *id*

Creating a DNAT Rule

To create a DNAT rule, in the VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **v4-mapped** [**log**] [**group** *group-id*]

- **id** *id* – Specifies the ID of the DNAT rule. Each DNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified DNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **top**, **before** *id* or **after** *id*. If the position is not specified, the rule would be located at the end of all the DNAT rules. By default, the newly-created DNAT rule is located at the end of all the rules. When traffic flows into the Hillstone device, the device will query for DNAT rules in the list

by turns, and then implement NAT on the destination IP of the traffic according to the first matched rule.

- **from** *src-address* **to** *dst-address* [**service** *service-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions are:
  - **from** *src-address* – Specifies the source IP address of the traffic. src-address should be an IPv6 address, or an IPv6 address entry in the address book.
  - **to** *dst-address* – Specifies the destination IP address of the traffic. src-address should be an IPv6 address, or an IPv6 address entry in the address book.
  - *service-name* – Specifies the service type of the traffic. The specified service can only be configured with one protocol and one port. For example, the TCP port number can be 80, but cannot be 80 to 100.
- **v4-mapped** – Extracts the destination IPv4 address from the destination IPv6 address of the packet directly.
- **log** – Enables the log function for this DNAT rule (Generating a log when the traffic is matched to this DNAT rule).
- **group** *group-id* - Specifies the HA group that the DNAT rule belongs to. If the parameter is not specified, the DNAT rule being created will belong to HA group0.

To delete the specified DNAT rule, in the VRouter configuration mode, use the following command:

no dnatrule id *id*

Configuring a IPv6 Track Object

To configure a track object, in the global configuration mode, use the following command:

track *track-object-name* [**local**]

- **track-object-name** – Specifies a name for the track object. The length of it can be 1 to 31 characters.
- **local** – If you enter this parameter, the system will not synchronize configuration of this track with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

This command creates the track object and leads you into the track object configuration mode; if the object exists, you will enter its configuration mode directly.

To delete the specified track object, use the following command:

no track *track-object-name*

You are allowed to track your object by using five protocols of ICMP, HTTP, DNS, NDP and TCP. Besides, the object also can be tracked by counting the traffic information of specified interface.

Track by IPv6 ICMP Packets

To track an object using Ping packets, in the object configuration mode, use the following command:

icmp6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name* [**prior-used-srcip**]] [**weight***value*]

- *ipv6-address* | **host** *host-name* – Specifies the IPv6 address or host name of the tracked object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* – Specifies the egress interface sending Ping packets.
- **interval***value* – Specifies the interval of sending Ping packets . The value range is 1 to 255 seconds. The default value is 3.
- **threshold***value* – Specifies the number which determines the tracking fails. If the system does not receive response packets of the number specified here, it determines that the track-

ing has failed, namely, the destination is unreachable. The value range is 1 to 255. The default value is 3.

- **src-interface***interface-name* – Specifies the source interface of Ping packets.
- **prior-used-srcip** *ipv6-address* – If the secondary IP is specified for the source interface and specifies the IP to be prior-used-srcip, system will use the IP to send track packets priorly. If the parameter is not specified, system will use default IP of the source interface to send track packets.
- **weight** *value* – pecifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more Ping tracking entries.

To delete the specified tracking entry, use the following command:

no icmp6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**delay**]

Track by IPv6 HTTP Packets

To track an object using HTTP packets, in the track object configuration mode, use the following command:

http ipv6 {*ipv6-address* | **host***host-name*} **interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name*] [**weight***value*]

- *ipv6-address* | **host** *host-name* – Specifies the IPv6 address or host name of the track object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* – Specifies the egress interface of sending HTTP test packets.
- **interval** *value* – Specifies the interval of sending HTTP packets. The value range is 1 to 255 seconds. The default value is 3.

- **threshold** *value* – Specifies the number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 1.
- **src-interface** *interface-name* – Specifies the source interface of the HTTP packets.
- **weight** *value* – Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more HTTP tracking entries.

To delete the specified tracking entry, use the following command:

no http ipv6 { *ipv6-address* | **host***host-name*} **interface***interface-name*

Track by IPv6 DNS Packets

To track an object using DNS packets, in the track object configuration mode, use the following command:

dns ipv6 *ipv6-address***interface***interface-name* [**interval***value*] [**threshold***value*] [**weight***value*] [**src-interface***interface-name*]

ipv6-address – Specifies the IPv6 address of track object.

- **interface***interface-name* – Specifies the egress interface of sending DNS test packets.
- **interval***value* – Specifies the interval of sending DNS packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold***value* – Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight***value* – Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **src-interface***interface-name* – Specifies the source interface of DNS test packets.

Repeat the command to configure more DNS tracking entries.

To delete the specified tracking entry, use the following command:

no dns ipv6*ipv6-address***interface***interface-name*

Track by NDP Packets

To track an object using NDP packets, in the track object configuration mode, use the following command:

ndp *ipv6-address***interface***interface-name* [**interval***value*] [**threshold***value*] [**weight***value*]

- *ipv6-address* – Specifies the IPv6 address of track object.
- **interface** *interface-name* – Specifies the egress interface of sending NDP test packets.
- **interval***value* – Specifies the interval of sending NDP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold***value* – Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight***value* – Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

To delete the specified tracking entry, use the following command:

no ndp *ipv6-address* **interface** *interface-name*

Track by IPv6 TCP Packets

To track an object using TCP packets, in the track object configuration mode, use the following command:

tcp ipv6 {{ipv6-addres | **host***host-name*} **port***port-number***interface***interface-name* [**interval***value*] [**threshold***value*] [**src-interface***interface-name*] [**weight***value*]

- *ipv6-address* | **host***host-name* – Specifies the IPv6 address or host name of track object. The length of the host name can be 1 to 63 characters.
- **port***port-number* – Specifies the destination port of the track object. The value range is 0 to 65535.
- **interface***interface-name* – Specifies the egress interface for sending TCP test packets.
- **interval***value* – Specifies the interval of sending TCP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold***value* – Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **src-interface***interface-name* – Specifies the source interface of TCP test packets.
- **weight***value* – Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more TCP tracking entries. For one single track object, you cannot configure both the HTTP track on the host and TCP track on port 80 simultaneously.

To delete the specified tracking entry, use the following command:

no tcp ipv6 {*ipv6-address* | **host***host-name*} **port***port-number***interface***interface-name*

IPv6 Configuration Examples

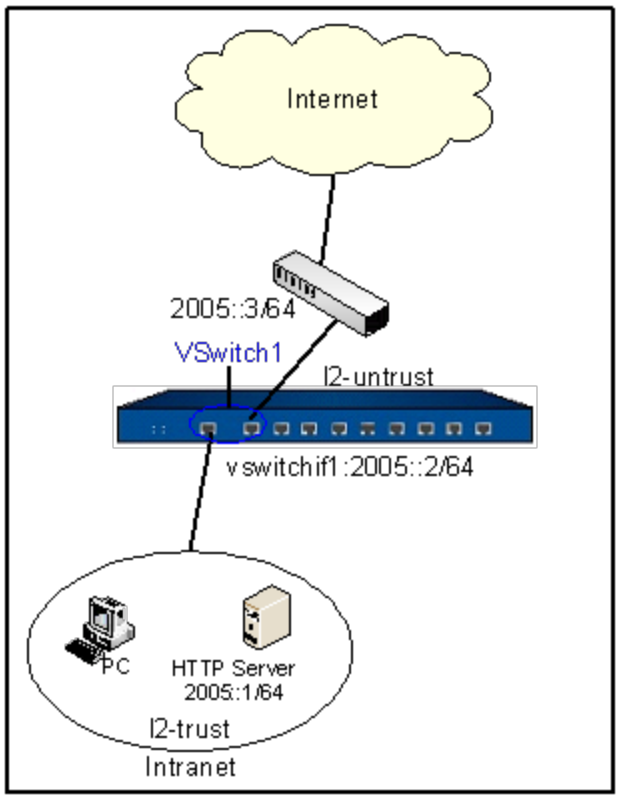
This section describes several configuration examples of IPv6, including:

- Example 1: IPv6 transparent mode configuration
- Example 2: IPv6 routing mode configuration
- Example 3: IPv6 Manual 6to4 tunnel configuration
- Example 4: IPv6 Automatic 6to4 tunnel configuration

- Example 5: IPv6 SNMP configuration example
- Example 6: IPv6 NAT-PT configuration example

Example 1: IPv6 Transparent Mode Configuration

Hillstone device is deployed in the transparent mode. Ethernet0/0 belongs to the l2-trust zone, and is connected to the Intranet; ethernet0/1 belongs to the l2-untrust zone; both l2-trust and l2-untrust belong to VSwitch1. The goal is to allow the hosts in the Intranet to visit Internet, and allow hosts in the Internet to visit the HTTP server in the Intranet. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-trust
hostname(config-if-eth0/0)# exit
```

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-untrust
hostname(config-i f-eth0/1)# exit
hostname(config)# interface vswitchif1
hostname(config-if-vsw1)# zone trust
hostname(config-if-vsw1)# ipv6 enable
hostname(config-if-vsw1)# ipv6 address 2005::2/64
hostname(config-if-vsw1)# exit
hostname(config)#
```

Step 2: Configure an address entry:

```
hostname(config)# address http-server ipv6
hostname(config-addr)# ip 2005::1/64
hostname(config-addr)# exit
hostname(config)#
```

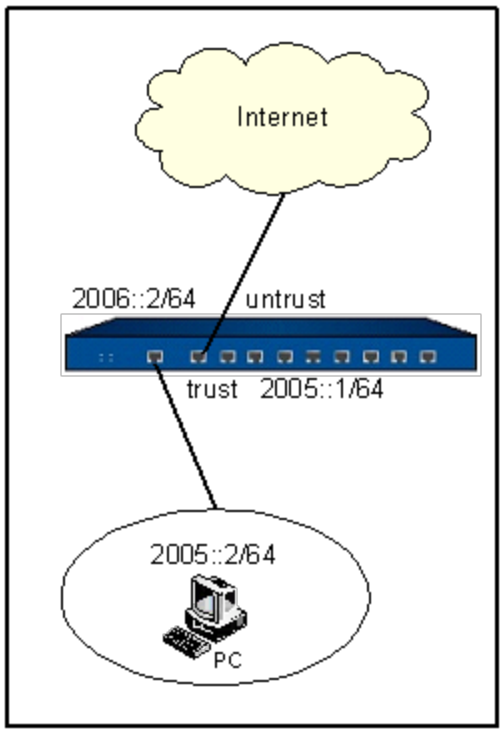
Step 3: Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone l2-trust
hostname(config-policy-rule)# dst-zone l2-untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
```

```
hostname(config-policy-rule)# src-zone l2-untrust
hostname(config-policy-rule)# dst-zone l2-trust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr http-server
hostname(config-policy-rule)# service http
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Example 2: IPv6 Routing Mode Configuration

Hillstone device is deployed in the routing mode. Ethernet0/0 belongs to the trust zone, and is connected to the Intranet; ethernet0/1 belongs to the untrust zone, and is connected to the Internet. The public address provided by the ISP is 2006::1/64. The goal is to allow the PC in the Intranet to visit Internet. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2005::1/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2006::2/64
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure a default router:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route ::/0 2006::1
hostname(config-vrouter)# exit
hostname(config)#
```

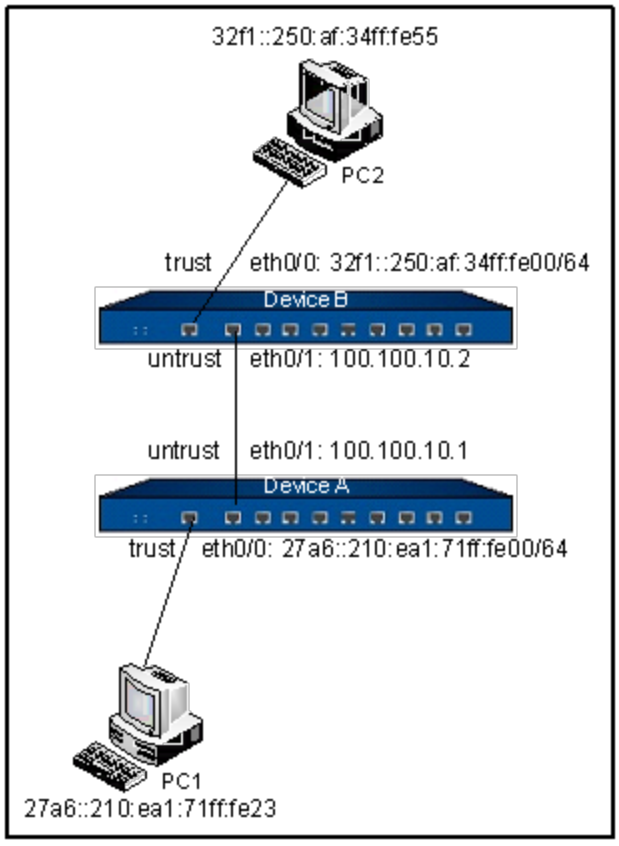
Step 3: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr 2005::2/64
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Example 3: IPv6 Manual 6to4 Tunnel Configuration

PC1 and PC2 use IPv6 addresses and belong to different subnets. The goal is to allow the inter-communication between PC1 and PC2 via an IPv6 manual 6to4 tunnel. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address
27a6::210:ea1:71ff:fe00/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 100.100.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

```
Device B
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address
32f1::250:af:34ff:fe00/64
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 100.100.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure tunnels:

```
Device A
```

```
hostname(config)# tunnel ipv6-over-ipv4 test-tunnelA
manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 100.100.10.2

hostname(config-ip6in4-manual)# exit
hostname(config)#
```

```
Device B
hostname(config)# tunnel ipv6-over-ipv4 test-tunnelB
manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 100.100.10.1

hostname(config-ip6in4-manual)# exit
hostname(config)#
```

Step 3: Bind the IPv6 manual 6to4 tunnel to tunnel interfaces:

```
Device A
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ipv6-over-ipv4 test-tun-
nelA
hostname(config-if-tun1)# exit
hostname(config)#
```

```
Device B
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
```

```
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ipv6-over-ipv4 test-tun-
nelB
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure policy rules:

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

```
Device B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
hostname(config)#
```

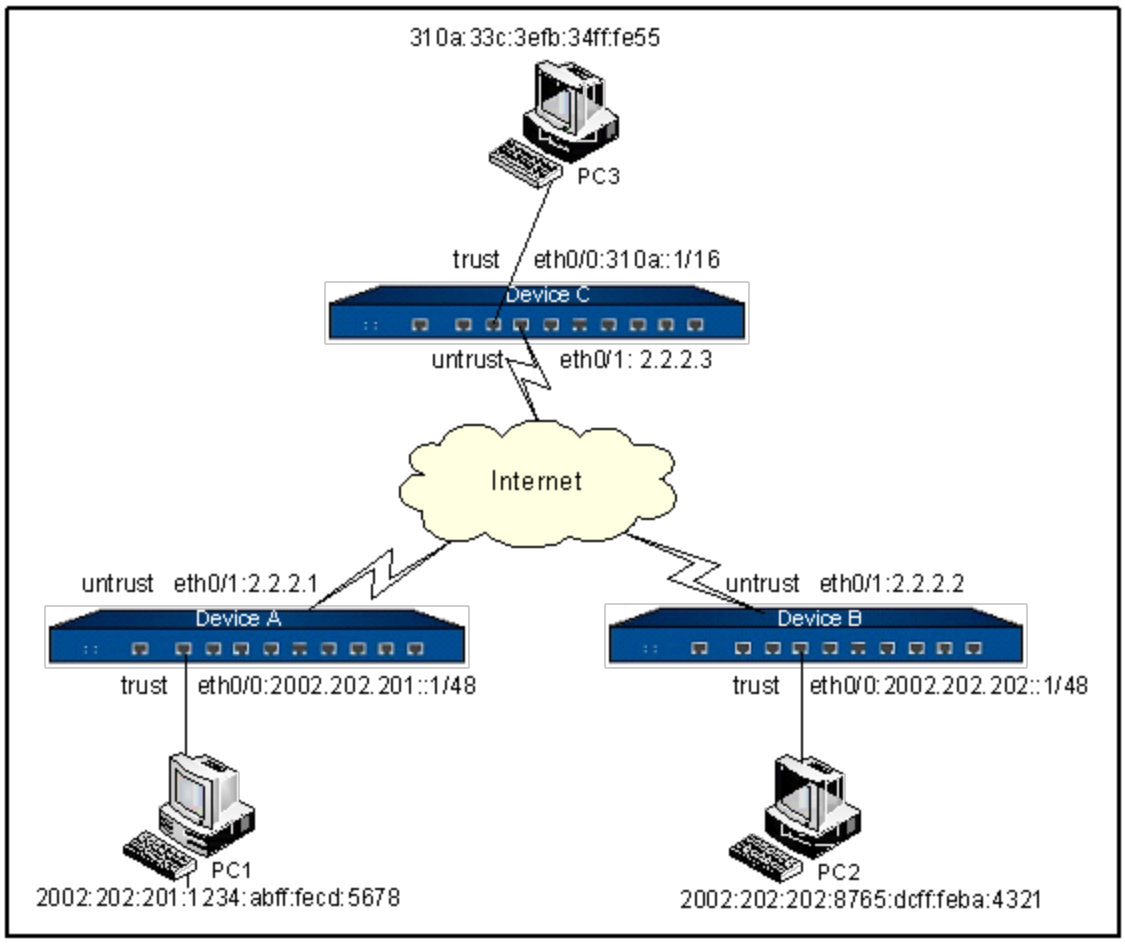
Step 5: Configure routes:

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 32f1::/64 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

```
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 27a6::/64 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

Example 4: IPv6 Automatic 6to4 Tunnel Configuration

PC1, PC2 and PC3 are IPv6 hosts, among which PC1 and PC2 use 6to4 addresses, while PC3 uses a general IPv6 address. The goal is to configure automatic 6to4 tunnels on Device A, Device B and Device C for the intercommunication among PC1, PC2 and PC3. The network topology is shown below.



Take the following steps:

Step 1: Configure interfaces:

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address
2002:202:201::1/48
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.1/24
```

```
hostname(config-if-eth0/1)# exit
hostname(config)#
Device B
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address
2002:202:202::1/48
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
Device C
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 310a::1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.2.2.3/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure tunnels:

```
Device A
hostname(config)# tunnel ipv6-over-ipv4 test-tunnelA
6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
Device B
hostname(config)# tunnel ipv6-over-ipv4 test-tunnelB
6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
Device C
hostname(config)# tunnel ipv6-over-ipv4 test-tunnelC
6to4
hostname(config-ip6in4-6to4)# interface ethernet0/1
hostname(config-ip6in4-6to4)# exit
hostname(config)#
```

Step 3: Bind the automatic 6to4 tunnels to tunnel interfaces:

```
Device A
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ipv6-over-ipv4 test-tunnelA
hostname(config-if-tun1)# exit
hostname(config)#
Device B
```

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ipv6-over-ipv4 test-tunnelB
hostname(config-if-tun1)# exit
hostname(config)#
Device C
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ipv6-over-ipv4 test-tunnelC
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure a policy rule (on all the three devices):

```
Device A、Device B、Device C
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr ipv6-any
hostname(config-policy-rule)# dst-addr ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Configure routes:

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 2002:202:202::/48
tunnel1
hostname(config-vrouter)# ipv6 route 310a::/16 tunnel1
2002:202:203::1
hostname(config-vrouter)# exit
hostname(config)#
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 2002:202:201::/48
tunnel1
hostname(config-vrouter)# ipv6 route 310a::/16 tunnel1
2002:202:203::1
hostname(config-vrouter)# exit
hostname(config)#
Device C
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 2002::/16 tunnel1
hostname(config-vrouter)# exit
hostname(config)#
```

Example 5: IPv6 SNMP Configuration

This section describes the following two IPv6 SNMP configuration examples:

- Viewing IPv6 MIB information via an IPv4 network
- Viewing IPv6 MIB information via an Ipv6 network

Viewing IPv6 MIB Information via an IPv4 Network

The host address is 1.1.12/24; the host is connected to etherenet0/0 that belongs to the untrust zone with address of 1.1.1.1/24. Take the following steps:

Step 1: Configure an interface:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# manage snmp
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure SNMP (only required configuration is listed):

```
hostname(config)# snmp-server manager
hostname(config)# snmp-server host 1.1.1.2 community pub-
lic ro
```

Finishing the above configuration, you can view IPv6-related MIB information via a MIB browser on the management host.

Viewing IPv6 MIB Information via an Ipv6 Network

The host address is 2008::2/64; the host is connected to etherenet0/0 that belongs to the untrust zone with address of 2008::1/24. Take the following steps:

Step 1: Configure an interface:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ipv6 enable
hostname(config-if-eth0/0)# ipv6 address 2008::1/64
hostname(config-if-eth0/0)# manage snmp
```

```
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure SNMP (only required configuration is listed):

```
hostname(config)# snmp-server manager
hostname(config)# snmp-server ipv6-host 2008::2 com-
munity public ro
```

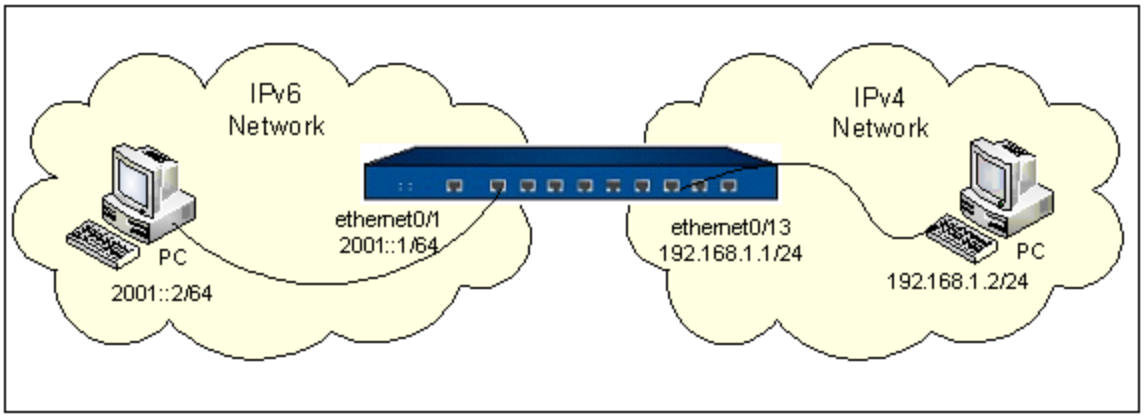
Finishing the above configuration, you can view IPv6-related MIB information via a MIB brower on the management host.

Example 6: IPv6 NAT-PT Configuration

IPv6 and IPv4 networks are connected via a Hillstone device. The goal for NAT-PT configuration is:

- Requirement 1: The host in the IPv6 network can initiate access to the host in the IPv4 network, while the host in the IPv4 network cannot initiate access the host in the IPv6 network;
- Requirement 2: The host in the IPv4 network can initiate access to the host in the IPv6 network, while the host in the IPv6 network cannot initiate access the host in the IPv4 network.

The network topology is shown below:



Requirement 1

The host in the IPv6 network can initiate access to the host in the IPv4 network, while the host in the IPv4 network cannot initiate access the host in the IPv6 network. Assume the situation below: for the host in the IPv6 network, the mapping IPv6 address of the host in the IPv4 network is 2003::2.

Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

Step 2: Configure NAT-PT rules:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from ipv6-any to 2003::2 service any trans-to eif-ip mode dynamicport
rule ID=1
hostname(config-vrouter)# dnatrule from ipv6-any to 2003::2 service any trans-to 192.168.1.2
rule ID=1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
Rule id 2 is created
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-ip 2001::2/64
hostname(config-policy-rule)# dst-ip 2003::2/128
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Requirement 2

The host in the IPv4 network can initiate access to the host in the IPv6 network, while the host in the IPv6 network cannot initiate access the host in the IPv4 network. Assume the situation below: for the host in the IPv4 network, the mapping IPv4 address of the host in the IPv6 network is 192.168.2.2.

Take the following steps:

Step 1: Configure interfaces:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 2001::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/13
hostname(config-if-eth0/13)# zone trust
```

```
hostname(config-if-eth0/13)# ip address 192.168.1.1/24
hostname(config-if-eth0/13)# exit
hostname(config)#
```

Step 2: Configure NAT-PT rules:

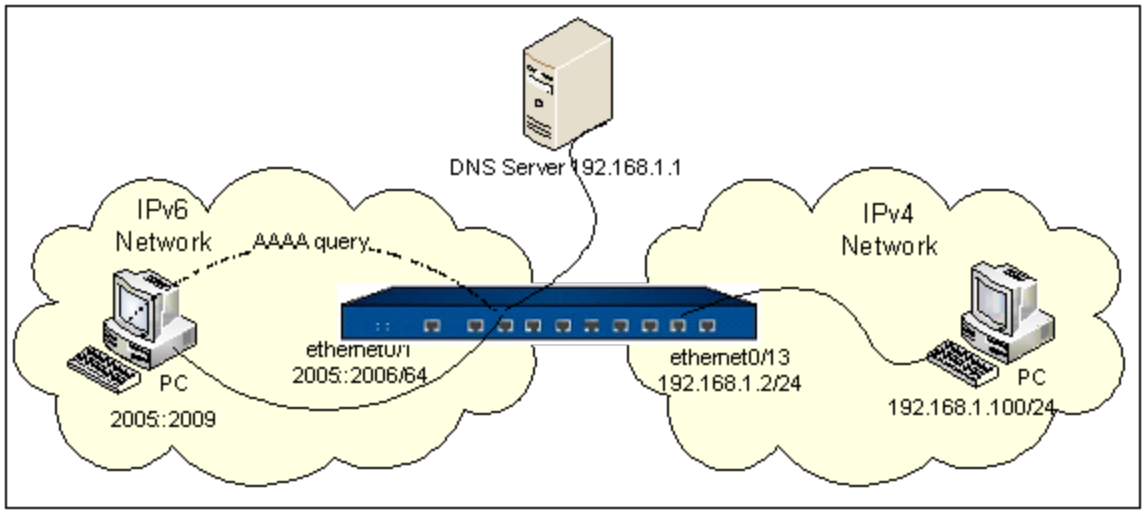
```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to 192.168.2.2 service any trans-to 2001::2 mode dynamicport
rule ID=2
hostname(config-vrouter)# dnatrule from any to 192.168.2.2 service any trans-to 2001::3
rule ID=2
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
Rule id 3 is created
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-ip 192.168.1.2/24
hostname(config-policy-rule)# dst-ip 192.168.2.2/32
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Example 7： IPv6 DNS64 and NAT64 Configuration

IPv6 and IPv4 networks are connected via a Hillstone device. The goal is to allow the host in the IPv6 network to initiate access to the host in the IPv4 network by configuring DNS64 and NAT64 on the device. The network topology is shown below:



Take the following steps:

Step 1: Configure DNS rule and enable the DNS64 function:

```
hostname(config)# dns-proxy rule
Rule id 1 is created
hostname(config-dns-proxy-rule)# ingress-interface ethernet0/1
hostname(config-dns-proxy-rule)# src-ip 2005::2006/64
hostname(config-dns-proxy-rule)# dst-addr IPv6-any
hostname(config-dns-proxy-rule)# domain any
hostname(config-dns-proxy-rule)# action proxy
hostname(config-dns-proxy-rule)# name-server 192.168.1.1
hostname(config-dns-proxy-rule)# dns64 enable
hostname(config-dns-proxy-dns64)# prefix 64:ff9b::/96
hostname(config-dns-proxy-dns64)# server 192.168.1.1
hostname(config-dns-proxy-dns64)# exit
```

```
hostname(config-dns-proxy-rule)# exit
hostname(config)#
```

Step 2: Configure the NAT64.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from 2005::2009 to 64:ff9b::/96 service any trans-to eif-ip mode dynamicport
rule ID=1
hostname(config-vrouter)# dnatrule from 2005::2009 to 64:ff9b::/96 service any v4-mapped
rule ID=1
hostname(config-vrouter)# exit
hostname(config)#
```

Appendix 1: ICMPv6 Type and Code

ICMPv6 Type	ICMPv6 Code	Reference
1 Destination Unreachable	0 - no route to destination	[RFC4443]
	1 - communication with destination administratively prohibited	[RFC4443]
	2 - beyond scope of source address	[RFC4443]
	3 - address unreachable	[RFC4443]
	4 - port unreachable	[RFC4443]
	5 - source address failed ingress/egress policy	[RFC4443]
	6 - reject route to destination	[RFC4443]
2 Packet Too Big	0	[RFC4443]
3 Time Exceeded	0 - hop limit exceeded in transit	[RFC4443]
	1 - fragment reassembly time exceeded	[RFC4443]
4 Parameter Problem	0 - erroneous header field encountered	[RFC4443]
	1 - unrecognized Next Header type encountered	[RFC4443]
	2 - unrecognized IPv6 option encountered	[RFC4443]
5-99 Unallocated Error message	0	[RFC4443]
100 Private experimentation	-	[RFC4443]
101 Private experimentation	-	[RFC4443]
102-126 Unallocated	0	[RFC4443]

ICMPv6 Type	ICMPv6 Code	Reference
Error message		
127 Reserved for expansion of ICMPv6 error messages	-	[RFC4443]
128 Echo Request	0	[RFC4443]
129 Echo Reply	0	[RFC4443]
130 Multicast Listener Query	0	[RFC2710]
131 Multicast Listener Report	0	[RFC2710]
132 Multicast Listener Done	0	[RFC2710]
133 Router Solicitation	0	[RFC4861]
134 Router Advertisement	0	[RFC4861]
135 Neighbor Solicitation	0	[RFC4861]
136 Neighbor Advertisement	0	[RFC4861]
137 Redirect Message	0	[RFC4861]
138 Router Renumbering	0 - Router Renumbering Command	[Crawford] [RFC2894]
	1 - Router Renumbering Result	[Crawford] [RFC2894]
	255 - Sequence Number Reset	[Crawford]

ICMPv6 Type	ICMPv6 Code	Reference
		[RFC2894]
139 ICMP Node Information Query	0 - The Data field contains an IPv6 address which is the Subject of this Query	[RFC4620]
	1 - The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP.	[RFC4620]
	2 - The Data field contains an IPv4 address which is the Subject of this Query.	[RFC4620]
140 ICMP Node Information Response	0 - A successful reply. The Reply Data field may or may not be empty.	[RFC4620]
	1 - The Responder refuses to supply the answer. The Reply Data field will be empty.	[RFC4620]
	2 - The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.	[RFC4620]
141 Inverse Neighbor Discovery Solicitation Message	0	[RFC3122]
142 Inverse Neighbor Discovery Advertisement Message	0	[RFC3122]
143 Version 2 Multicast Listener Report	-	[RFC3810]
144 Home Agent Address Discovery Request Message	0	[RFC3775]

ICMPv6 Type	ICMPv6 Code	Reference
145 Home Agent Address Discovery Reply Message	0	[RFC3775]
146 Mobile Prefix Solicitation	0	[RFC3775]
147 Mobile Prefix Advertisement	0	[RFC3775]
148 Certification Path Solicitation Message	-	[RFC3971]
149 Certification Path Advertisement Message	-	[RFC3971]
150 ICMP messages utilized by experimental mobility protocols such as Seamoby	-	[RFC4065]
151 Multicast Router Advertisement	-	[RFC4286]
152 Multicast Router Solicitation	-	[RFC4286]
153 Multicast Router Termination	-	[RFC4286]
154 FMIPv6 Messages	-	[RFC5268]
200 Private experimentation	-	[RFC4443]
201 Private exper-	-	[RFC4443]

ICMPv6 Type	ICMPv6 Code	Reference
imentation		
255 Reserved for expansion of ICMPv6 informational messages	-	[RFC4443]

Chapter 8 User Authentication

The chapter introduces the following topics:

- Authentication, Authorization and Accounting describes the AAA function: Authentication, Authorization and Accounting.
- User Identification describesdescribes various methods of user identification, which is used to authenticate users who access the Internet via the device.
- 802.1X Authentication describes the function of 802.1X authentication. 802.1X is a standard defined by IEEE for Port-based Network Access Control.
- PKI describes the function of Public Key Infrastructure, which provides public key encryption and digital signature service.

Authentication, Authorization and Accounting

Overview

AAA is the abbreviation for Authentication, Authorization and Accounting. Details are as follows:

- Authentication: Authenticates users' identities.
- Authorization: Grants certain privileges according to the configuration.
- Accounting: Records the fees users should pay for their network resource usage.

Hillstone devices support the following authentication methods:

- Local authentication: Configures user information (including username, password and properties) on Hillstone devices. Local authentication is fast, and can reduce operation cost, but the amount of information that will be stored is limited by the hardware of the device. By default, Hillstone devices use local authentication.
- External authentication: Hillstone devices also support external authentication over RADIUS, AD, LDAP and TACACS+ protocol. User information is stored in an external RADIUS, AD, LDAP or TACACS+ server, and Hillstone devices authenticate users by the external server.

Hillstone devices support the following authorization methods:

- Local authorization: Authorizes user privileges according to the configurations of Hillstone devices.
- Authorization after external authentication: RADIUS/LDAP/AD/TACACS+ authentication is mapped to an authorization.

Hillstone devices support the following accounting methods:

- None accounting: No accounting required.
- External accounting: Performs Accounting for authenticated users via a RADIUS server.

External Authentication Procedure

When a user has established a connection from a terminal to a Hillstone device and gained access or management privilege, the Hillstone device can authenticate the user via the configured RADIUS or LDAP server. The figure below shows the external authentication procedure:



As shown above, the procedure is:

1. The user sends username and password to the Hillstone device.
2. The Hillstone device receives the username and password, and sends an authentication request to the RADIUS/LDAP/AD/TACACS+server.
3. If the request is legal, the RADIUS/LDAP/AD/TACACS+ server performs authentication. If passed, the RADIUS/LDAP/AD/TACACS+server returns the user information to the Hillstone device, otherwise returns denial information. The security between the Hillstone device and RADIUSTACACS+ server is guaranteed by the shared secret (secret key or cipher text).

Configuring an AAA Server

The configurations of an AAA server include:

- Creating an AAA server
- Configuring a local authentication server
- Configuring a RADIUS authentication server

- Configuring an Active-Directory authentication server
- Configuring a TACACS+ authentication server
- Configuring an LDAP authentication server
- Configuring OAuth2 authorization server
- Configuring a RADIUS accounting server
- Configuring Authentication and Authorization for the Server
- Viewing and Debugging AAA
- Configuring the Brute-force Cracking Defense

Creating an AAA Server

AAA configurations need to be done in the AAA service configuration mode. To create an AAA server, in the global configuration mode, use the following command:

aaa-server*aaa-server-name* [**type**] {**local** | **radius** | **active-directory** | **ldap** | **tacacs+** | **oauth**}

- *aaa-server-name* – Specifies the name of the AAA server. The length is 1 to 31 characters and is case sensitive.
- **type** {**local** | **radius** | **active-directory** | **ldap** | **tacacs+** | **oauth**} – Specifies the type of the AAA server to be created. It can be a local server (`local`), RADIUS server (`radius`), Active-Directory server (`active-directory`), LDAP server (`ldap`), TACACS+ server (`tacacs+`), or OAuth2 server (oauth).

After executing this command, the system will create an AAA server with the specified name, and enter the AAA server configuration mode. If the specified name exists, the system will directly enter the AAA server configuration mode.

To delete the specified AAA server, in the global configuration mode, use the following command:

no aaa-server *aaa-server-name*

Configuring a Local Authentication Server

To enter the local server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**. The local authentication server configuration includes:

- Configuring the account control
- Configuring the password control
- Specifying user name format
- Configuring a role mapping rule
- Configuring a user blacklist
- Configuring a backup authentication server

Configuring the Account Control

To improve the account security, the system provides the account control function, allowing you to enable and configure account expiration notification. Account expiration notification is disabled by default. With this function enabled, the system checks the status of the user account on the local server, that is, checks whether the account expires. If the account is about to expire, the system sends an notification on how many days are remained before the expiration date.

To enable and configure account expiration notification, in the local server configuration mode, use the following command:

alert-before-account-expire *alert-day*

- *alert-day* – Specifies the warning period before account expiry. The value range is from 1 to 30 days. For example, if the value is 10, it indicates that you will get a warning about the approaching account expiry 10 days before the expiration date. The default value is 7. For more information about how to configure user account expiration date, refer to Specifying a User Expiration Date.

To disable account expiration notification, use the **no alert-before-account-expire** command.

Notes:

1. In the scenario where Account Expiry Warning is enabled and configured, Web Authentication is enabled and the authentication server is a local server, when a user whose account is about to expire attempts to login through Web authentication, the system will display a message on the Web authentication login page, warning how many days are remained before the account expiration date.
2. If the system uses a local authentication server for user authentication of the SSL VPN/ZTNA client, when users whose accounts are about to expire log in to the system through SSL VPN/ZTNA client, a window will pop up on the client to show the remaining number of days their account is valid. The client versions that support the pop-up window reminder of the remaining valid days of the account include Windows client v5.0.1.10328 and later, Android client v5.0.1.10331 and later, iOS client v5.0.1 and later, macOS client v5.0.1.10331 and later, Linux client v5.0.1.10331 and later. Other client versions do not have a pop-up reminder.

Configuring the Password Control

To prevent account security problem, you can configure the password control function. The configuration of the password control function must be performed in the password control configuration mode. To enter the password control configuration mode, in the local server configuration mode, use the following command:

password-control

The password control function include:

- Allowing Password Change by Local Users
- Configuring the Password Validity and Password Expiry Warning
- Configuring the History Password Check
- Configuring the Password Complexity
- Enabling/disabling Forced Password Change for First Login

Allowing Password Change by Local Users

Local users can change their password on the login page after successful authentication. For configuration, prefer to "User Authentication > User Identification > Web Authentication > Allowing Password Change by Local Users".

By default, the local user is not allowed to change its password, but you can configure the device to enable password changing right for local users if they pass SSL VPN authentication. For configuration, prefer to "VPN > SSL VPN> Configuring SSL VPN Server > Allowing Password Change by Local Users".

Configuring Change Password after First Login

By default , the function is disabled. Configure Change Password after First Login function, in the password control mode, use the following command:

first-login-check [**mode** { **compatibility** | **enforcement** }]

- **compatibility** – Specifies the compatible mode for the Change Password after First Login function: ①If this function does not apply to the SSL VPN client, users can log in to the SSL VPN client for the first time without changing the password.②If this function applies to the SSL VPN client, users need to change the login password immediately after logging in to the SSL VPN client for the first time.
- **enforcement** – Specifies the enforce mode for the Change Password after First Login function. Users need to change the login password immediately after logging in to the SSL VPN client for the first time.



Notes:

- In case the Enforce Mode is configured, the SSL VPN client cannot be used if this function does not apply to the SSL VPN client. You are advised to

upgrade the SSL VPN client or switch to the compatible mode.

- The SSL VPN client versions that allow you to change the password upon the first login are as follows: SSL VPN Windows client 1.4.9.1274 or later version, Linux 1.4.0 or later version, Android 4.5 or later version, and iOS 2.0.6 or later version.
- Change Password after First Login function does not apply to SSL VPN Windows client(non-administrator) version 1.5.x.

Configuring the Password Validity and Password Expiry Warning

You can configure the password validity and the days how long users will be reminded of password expiry before it expires.

To configure the password validity and password expiry warning, in the password control mode, use the following command:

aging*aging-day* [**alert-before-expire***alert-day*]

- *aging-day* – Specifies the valid period of password. The value range is 1 to 365 days. The default value is 90.
- *alert-day* – Specifies the days to remind the user to change the password before the password expires. The value range is 1 to 30 days. The default value is 7.

To cancel the settings of password validity and password expiry warning, use the **no aging** command.

Configuring the History Password Check

When the history password check function is enabled, system will verify the newly changed password with verifying the historical passwords, ensuring the new password is different from the history passwords.

To configure the history password check function, in the password control mode, use the following command:

history-check*count*

- *count* – Configure the newly changed passwords is different from the passwords set in the recent specified times. The value range is 1 to 5. The default value is 3.

To cancel the history password check configuration, use the **no history-check** command.

Configuring the Password Complexity

The lower the complexity of the password, the more likely it is to be cracked, such as including the username and short password length. For security reasons, you can enable the password complexity configuration and configure the password complexity requirements to ensure that the user's password has high complexity.

To enable password complexity configuration, in the password control mode, use the following command:

complexity enable

To disable this function, use the**no complexity enable**command.

To configure the password complexity, in the password control mode, use the following command:

complexity {**capital - letters***letters* | **small-letters***length* | **min - length***length* | **no-include -username** | **non-alphanumeric-letters***length* |**numeric-characters***length*}

- **capital - letters***letters* - Specifies the minimum length of uppercase letters contained in the password. The range is 0-16. The default value is 0.
- **small-letters***length* - Specifies the minimum length of lowercase letters contained in the password. The range is 0-16. The default value is 0.
- **min - length***length* - Specify the minimum password length, the range is 1-16, the default value is 1.

- **no-include -username** - Specifies the password cannot contain a username.
- **non-alphanumeric-letters***length*- Specifies the minimum length of the password containing special characters (that is, non-numeric characters), the range is 0-16, and the default value is 0.
- **numeric-characters***length* - Specifies the minimum length of the number contained in the password. The range is 0-16. The default value is 0.

To restore the default value, use the **no complexity** {**capital - letters** | **small-letters** | **min - length** | **no-include -username** | **non-alphanumeric-letters** |**numeric-characters** }command.

Specifying User Name Format

During user authentication, the system will extract the user name based on the configured authentication user name format. If the desired format is not available, the system will directly use the original user name for authentication.

To specify the authentication user name format, in the local server configuration mode, use the following command:

extract-username-format authenticate { [**domain\username**] [**username@domain**] }

To delete configuration of the authentication user name format, in the local server configuration mode, use the following command:

no extract-username-format authenticate { [**domain\username**] [**username@domain**] }

While implementing policy control based on user name or user group, the system will search the group to which a user name belongs from the organization units locally stored.

To specify the user name format supported when searching for the user group, in the local server configuration mode, use the following command:

extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

To delete configuration of the user name format for searching groups, in the local server configuration mode, use the following command:

no extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

Configuring a Role Mapping Rule

After specifying a role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure a role mapping rule for the server, in the local server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing role mapping rule.

To cancel the specified role mapping rule configuration, in the local server configuration mode, use the following command:

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the local server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the local server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the local server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring a Backup Authentication Server

After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the local server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the local server configuration mode, use the following command:

no backup-aaa-server



Notes:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.

Configuring the Brute-force Cracking Defense

To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP, i.e., within the specified period, if the failed attempts reached the specified times, the user or IP will be locked for a while. The Brute-force Cracking Defense configuration includes:

- Enabling/Disabling the Brute-force Cracking Defense
- Configuring the number of attempts
- Configuring the lock time

Enabling/Disabling the Brute-force Cracking Defense

By default, the Brute-force Cracking Defense function is disabled. To enable this function, in the local server configuration mode, use the following command:

- Enable: **lockout {ip | user} enable**
- Disable: **lockout {ip | user} disable**

Configuring the Number of Attempts

The number of attempts, that is, the allowed times of login failure within the specified time. To configure the number of attempts, in the local server configuration mode, use the following command:

lockout {**ip** | **user**} **failed-attempts***number* **interval***interval*

- **failed-attempts***number* – Specifies the allowed times of login failure. For lockout user, the range is 1 to 32, the default value is 5. For lockout IP, the range is 1 to 2048, the default value is 64.
- **interval** *interval* – Specifies the allowed time of login. The range is 1 to 180 and the default value is 60 seconds.

Configuring the Lockout Time

If the failed attempts reached the specified times in the specified time, the user or IP will be locked out for a while. To configure the lockout time, in the local server configuration mode, use the following command:

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time***time* – Specifies the lockout time. The range is 30 to 180. The default value is 600 seconds for lockout user, and 60 seconds for lockout IP.

Viewing the Lockout Information

To view the information of locked user or IP, in any mode, use the following command:

show aaa-server*aaa-server-name***lockout** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specifies the name of AAA server.
- **user** [*username*] - View the information of the locked user of the specified name.
- **ip** [*ip-address***vr_id***number*] - View the information of the locked IP of the specified IP address and VRouter ID.

Unlocking the User / IP

To unlock and delete the user or IP, in any mode, use the following command:

exec aaa aaa-server*aaa-server-name***lockout delete** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specify the name of the AAA server.
- **user** [*username*] - Unlock the user of the specified name.
- **ip** [*ip-address***vr_id***number*] - Unlock the IP of the specified IP address and VRouter ID.

Configuring a RADIUS Authentication Server

To enter the RADIUS server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type radius**.

The RADIUS authentication server configuration includes:

- Configuring LOCAL NAS IP for RADIUS Authentication
- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the secret
- Configuring the retry times
- Configuring the timeout
- Specifying user name format
- Specifying a role mapping rule
- Configuring a user blacklist

- Configuring the Brute-force Cracking Defense
- Configuring a backup authentication server
- Enabling / Disabling the authentication policy
- Adding authentication policy to aggregate policy

Configuring LOCAL NAS IP for RADIUS Authentication

When the Radius server is used to authenticate users, you can specify the LOCAL NAS (Network Access Server) IP address as needed. To specify the LOCAL NAS IP address, in the Radius server configuration mode, use the following command:

local-nas-ip *ip-address*

- *ip-address* – Specifies the LOCAL NAS IP address (At present, the system only supports IPv4 addresses). This way, the source IP address of Radius authentication packets and accounting packets, as well as the *nas-ip-address* of the authentication packets are all changed to this specified IP address, ensuring that packets returned by the Radius server are received by the current device in the complex network environment. The LOCAL NAS IP should be the same as the interface IP of the device. Otherwise, Radius authentication packets or accounting packets may not be properly sent.

To delete the LOCAL NAS IP address, in the Radius server configuration mode, use the following command:

no local-nas-ip *ip-address*



Notes:

- In the HA environment, the configuration of the LOCAL NAS IP address is not synchronized to the backup device. Therefore, you need to configure it in both primary and backup devices.
- It should be ensured that there are reachable routes between the current device and the Radius server.

Configuring the IP Address, Domain Name, or VRouter of the Primary Server

To configure the IP address, domain name, or VRouter of the primary authentication server, in the RADIUS server configuration mode, use the following command:

host {*ip-address* | *host-name* } [**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the primary authentication server.
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default Vrouter is trust-vr.

To delete the above configurations of the primary authentication server, in the RADIUS server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server' s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address, domain name, or VRouter of the backup authentication server 1, in the RADIUS server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* } [**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the back server 1 belongs to. The default Vrouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 1, in the RADIUS server configuration mode, use the command:

no backup1

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 2

This configuration is optional. Backup server must be of the same type of main server. When the authentication does not pass main server' s check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 2, in the RADIUS server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the back server 2 belongs to. The default Vrouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 2, in the RADIUS server configuration mode, use the command:

no backup2

Configuring the Port Number

To configure the port number of the RADIUS server, in the RADIUS server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the RADIUS server. The value ranges from 1024 to 65535. The default value is 1812.

To restore the default value of the port number, in the RADIUS server configuration mode, use the command:

no port

Configuring the Secret

To configure the secret of the RADIUS server, in the RADIUS server configuration mode, use the following command:

secret *secret*

- *secret* – Specifies the secret string of the RADIUS server. The length is 1 to 31 characters.

To cancel the secret configuration of the RADIUS server, in the RADIUS server configuration mode, use the command

no secret

Configuring the Retry Times

If the security device does not receive the response packets from the AAA server, it will resend the authentication packets. Retry times refers to the times for the authentication packets resent to the AAA server. To configure the retry times, in the RADIUS server configuration mode, use the following command:

retries *times*

- *times* – Specifies a number of retry times for the authentication packets sent to the AAA server. The value range is 1 to 10. The default value is 3.

To restore to the default value, in the RADIUS server configuration mode, use the command:

no retries

Configuring the Timeout

If the security device does not receive response packets from the AAA server when the server response time ends, the device will resend the authentication packets. To configure the timeout, in the RADIUS server configuration mode, use the following command:

timeout *time-value*

- *time-value* – Specifies the response timeout for the server. The value range is 1 to 30 seconds. The default value is 3.

To restore to the default timeout, in the RADIUS server configuration mode, use the command:

no timeout

Specifying User Name Format

During user authentication, the system will extract the user name based on the configured authentication user name format. If the desired format is not available, the system will directly use the original user name for authentication.

To specify the authentication user name format, in the RADIUS server configuration mode, use the following command:

extract-username-format authenticate { [**domain\username**] [**username@domain**] }

To delete configuration of the authentication user name format, in the RADIUS server configuration mode, use the following command:

no extract-username-format authenticate { [**domain\username**] [**username@domain**] }

While implementing policy control based on user name or user group, the system will search the group to which a user name belongs from the organization units locally stored.

To specify the user name format supported when searching for the user group, in the RADIUS server configuration mode, use the following command:

extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

To delete configuration of the user name format for searching groups, in the RADIUS server configuration mode, use the following command:

no extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure a role mapping rule, in the RADIUS server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing role mapping rule.

To cancel the role mapping rule configuration, in the RADIUS server configuration mode, use the command:

no role-mapping-rule

Configuring the Brute-force Cracking Defense

To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP, i.e., within the specified period, if the failed attempts reached the specified times, the user or IP will be locked for a while. The Brute-force Cracking Defense configuration includes:

- Enabling/Disabling the Brute-force Cracking Defense
- Configuring the number of attempts
- Configuring the lock time

Enabling/Disabling the Brute-force Cracking Defense

By default, the Brute-force Cracking Defense function is disabled. To enable this function, in the RADIUS server configuration mode, use the following command:

- Enable: **lockout** {**ip** | **user**} **enable**
- Disable: **lockout** {**ip** | **user**} **disable**

Configuring the Number of Attempts

The number of attempts, that is, the allowed times of login failure within the specified time. To configure the number of attempts, in the RADIUS server configuration mode, use the following command:

lockout {**ip** | **user**} **failed-attempts***number* **interval***interval*

- **failed-attempts***number* – Specifies the allowed times of login failure. For lockout user, the range is 1 to 32, the default value is 5. For lockout IP, the range is 1 to 2048, the default value is 64.
- **interval** *interval* – Specifies the allowed time of login. The range is 1 to 180 and the default value is 60 seconds.

Configuring the Lockout Time

If the failed attempts reached the specified times in the specified time, the user or IP will be locked out for a while. To configure the lockout time, in the RADIUS server configuration mode, use the following command:

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time***time* – Specifies the lockout time. The range is 30 to 180. The default value is 600 seconds for lockout user, and 60 seconds for lockout IP.

Viewing the Lockout Information

To view the information of locked user or IP, in any mode, use the following command:

show aaa-server*aaa-server-name***lockout** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specifies the name of AAA server.
- **user** [*username*] - View the information of the locked user of the specified name.
- **ip** [*ip-address***vr_id***number*] - View the information of the locked IP of the specified IP address and VRouter ID.

Unlocking the User / IP

To unlock and delete the user or IP, in any mode, use the following command:

exec aaa aaa-server*aaa-server-name***lockout delete** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specify the name of the AAA server.
- **user** [*username*] - Unlock the user of the specified name.
- **ip** [*ip-address***vr_id***number*] - Unlock the IP of the specified IP address and VRouter ID.

Configuring a User Blacklist

After configuring a user blacklist for the RADIUS server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the RADIUS server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the RADIUS server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring a Backup Authentication Server

After configuring a backup authentication server for the RADIUS server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be different from main server. It can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the RADIUS server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the RADIUS server configuration mode, use the following command:

no backup-aaa-server



Notes:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.



- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If a RADIUS server is configured with backup server 1 (backup1), backup server 2 (backup2) and backup authentication server (backup-aaa-server), when user's authentication request is not responded on the primary server, the system will re-authenticate the user on backup server 1 or backup server 2, and if user's authentication request is not responded on backup server 1 or backup server 2, the system will re-authenticate the user on the backup authentication server; when user's authentication failed on the primary server, backup server 1 or backup server 2, the system will re-authenticate the user on the backup authentication server.

Enabling / Disabling the Authentication Policy

When a user is authenticated by the Radius server, when the user is authenticated successfully, the Radius server will create a security policy for the authenticated user that includes the destination network segment, destination port, protocol, and behavior. This policy is called an authorization policy. System supports two authorization policies: "Authorization Policy During Authentication" and "Dynamic Authorization Policy". You can enable the authorization policy function to enable to obtain the authorization policy from the Radius server and add it to the system's policy list to make it effective. When the authenticated user is disconnected, the authorization policy will be deleted automatically.

By default, the authentication policy is disabled. To enable or disable the authentication policy, in the RADIUS server configuration mode, use the following command:

- Enable: **authorization-policy enable**
- Disable: **authorization-policy disable**



Notes: If you need to obtain the dynamic authorization policy, please configure the radius dynamic authorization function first. For the configuration of radius dynamic authorization function, refer to "Radius Dynamic Authorization" on Page 1256.

Adding Authentication Policy to Aggregate Policy

After the authorization policy of the Radius server is enabled, you add the obtained authorization policy to the aggregation policy that has been created, and arrange it as the member of aggregation policy at the end of aggregation policy, which is more convenient for the user to manage the authorization policy uniformly. If it is not added to the aggregation policy, the authorization policy will be added to the end of the system policy list by default.

To add the authentication Policy to an aggregate policy, in the RADIUS server configuration mode, use the following command:

authorization-policy associated-aggregate-rule*rule-name*

- *rule-name*- Specifies the aggregate policy name.

To cancel the configuration, in the RADIUS server configuration mode, use the following command:

no authorization-policy associated-aggregate-rule

Importing Dictionary

When a third party wants to customize some attributes, they can use a dictionary file to include its self-defined fields. The dictionary file of Hillstone Networks is “dictionary.hillstone”. The RADIUS server administrator adds dictionary.hillstone file into its server by editing the master RADIUS dictionary.

dictionary.hillstone contains the following attributes:

Attribute	Description
Hillstone-user-type	User Type. admin type=16 PnPVPN=4

Attribute	Description
	all=31 Users other than types listed here do not need this checking.
Hillstone-user-vsys-id	vSYS ID value. For admin type user, this attribute is mandatory. Currently, ID can only equals to 0.
Hillstone-user-login-type	Admin login type. telnet=2 SSH=4 CONSOLE=1 HTTP=8 HTTPS=16 all=31 For cominations of two or more protocols, the value is the sum of each value (e.g. telnet+SSH=6).
Hillstone-user-role-name	Admin role type. admin= Administrator operator= Operator auditor= Auditor admin-read-only= Administrator-read-only *role-name*= Custom administrator role
Hillstone-user-policy-dst-ip-begin	The start IP address of the access scope. Only IPv4 address is supported.
Hillstone-user-policy-dst-ip-end	The end IP address of the access scope. Only IPv4 address is supported.
Hillstone-User-Data-Filter	Radius server sends policy rules to authenticated users through this attribute.

Attribute	Description
	The attribute format is: **rule***number* {**permit**|**deny**} [**dst***ip-address*] [*protocol* [**dst-port***port*]] • *number*: Number of the policy in the Radius server • **permit**|**deny**: Policy rule action.**permit**means access is allowed, **deny** means access denied . • **dst***ip-address*: Destination address. Can be configured multiple, please use spaces to separate • *protocol*: Protocol type, which can be specified as TCP or UDP. • **dst-port***port*]: Destination port number. Can be configured multiple, please use spaces to separate them.

Configuring an Active-Directory Authentication Server

To enter the Active-Directory server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type active-directory**.

The Active-Directory authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the authentication or synchronization method
- Refreshing the connection with the server

- Specifying the Base-DN
- Specifying the Synchronization Base-DN
- Specifying the Synchronization Object
- Specifying the Authentication Base-DN
- Specifying the login DN
- Specifying sAMAccountName
- Specifying the login password
- Specifying the mobile number attribute name
- Specifying the email attribute name
- Enabling/Disabling the SSL Encrypted Connection
- Specifying user name format
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring a LDAP User
- Configuring User Expiration
- Configuring the Brute-force Cracking Defense
- Configuring an AD User
- Configuring User Expiration
- Configuring automatic user information synchronization
- Specifying Naming Attribute

- Specifying Group Class
- Specifying User Class
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server
- Configuring the User-Groups under Base-DN Synchronization
- Enabling/Disabling Authentication Simplification

Configuring the IP Address, Domain Name, and VRouter of the Primary Server

To configure the IP address, domain name, or VRouter of the primary authentication server, in the Active-Directory server configuration mode, use the following command:

host {*ip-address* | *host-name* } [**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6)or domain name of the primary authentication server.
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the primary authentication server, in the Active-Directory server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address or domain name of the backup authentication server 1, in the Active-Directory server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* } [**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup authentication server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server 1 belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 1, in the Active-Directory server configuration mode, use the command:

no backup1

Configuring the IP Address or Domain Name of the Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server' s check, the backup server 1 and 2 will start checking its credentials consecuritvely. To configure the IP address or domain name of the backup authentication server 2, in the Active-Directory server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server 2 belongs to. The default VRouter is trust-vr.

To delete the IP address or domain name configuration of the backup authentication server 2, in the Active-Directory server configuration mode, use the command:

no backup2

Configuring the Port Number

To configure the port number of the Active-Directory server, in the Active-Directory server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the Active-Directory server. The value range is 1 to 65535. The default value is 389.

To restore to the default port number, in the Active-Directory server configuration mode, use the command:

no port

Configuring the Authentication or Synchronization Method

Plain text and MD5 method can be configured to authenticate or synchronize user between the Active-Directory server and the system. To configure the authentication or synchronization method, in the Active-Directory server configuration mode, use the following command:

auth-method {**plain** | **digest-md5**}

- **plain** – Specifies the authentication or synchronization method to be plain text.
- **digest-md5** – Specifies the authentication or synchronization method to be MD5. The default method is MD5.

To restore to the default authentication or synchronization method, in the Active-Directory server configuration mode, use the command:

no auth-method



Notes: If the sAMAccountName is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.

Specifying the Base-DN

Base-DN is the starting point at which your search will begin when the AD server receives an authentication request. To specify the Base-DN, in the Active-Directory server configuration mode, use the following command:

base-dn *string*

- *string* – Specifies the Base-DN for the Active-Directory server, such as dc = hillstonenet.

To cancel the Base-DN configuration, in the Active-Directory server configuration mode, use the command:

no base-dn

Specifying the Synchronization Base-DN

Synchronization Base-DN is the starting point at which the system synchronizes users and user groups from the Active-Directory server. All users and user groups in the Base-DN will be synchronized to the local when you specify the Synchronization Base-DN. To specify the Synchronization Base-DN, in the Active-Directory server configuration mode, use the following command:

sync-base-dn*string*

- *string* - Specifies the starting point at which the system synchronizes users and user groups from the Active-Directory server, such as OU=test, dc = com.

You can repeatedly execute the command to configure multiple paths to be synchronized.

To delete a specified Synchronization Base-DN configuration, in the Active-Directory server configuration mode, use the following command:

no sync-base-dn *string*

Specifying the Synchronization Object

When the Synchronization Base-DN is specified, all users and groups in the Synchronization Base-DN will be synchronized to the local. If no Synchronization Base-DN is specified, all users and groups in the Base-DN will be synchronized to the local. After you specify that the Synchronization Object is users or groups, the system filters the information synchronized to the local and retains the information of the specified object. To specify the Synchronization Object, in the Active-Directory server configuration mode, use the following command:

sync-object {**user** | **group**}

- **user** – Specifies the Synchronization Object as users. System will retain user information only.

- **group** – Specifies the Synchronization Object as groups. System will retain group information only.

To cancel the Synchronization Object configuration, in the Active-Directory server configuration mode, use the command **no sync-object** {**user** | **group**}.

Specifying the Authentication Base-DN

Base-DN is the starting point at which your search will begin when the AD server receives an authentication request. All users in the Base-DN (including those directly under the user group) will be allowed to pass the authentication when you specify the Authentication Base-DN. To specify the Authentication Base-DN, in the Active-Directory server configuration mode, use the following command:

auth-base-dn*string*

- *string* - Specifies the Authentication Base-DN for the Active-Directory server, such as OU=A, dc = hillstonenet.

To cancel the Authentication Base-DN configuration, in the Active-Directory server configuration mode, use the command **no auth-base-dn**.

Specifying the Login DN

If plain text method is configured to authenticate or synchronize user, the system will send the login DN and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. The login DN is typically a user account with query privilege predefined by the Active-Directory server. To specify the login DN, in the Active-Directory server configuration mode, use the following command:

login-dn *string*

- *string* – Specify the login DN for the Active-Directory server, which is a string of 1 to 255 characters and is not case sensitive.

To cancel the login DN configuration, in the Active-Directory server configuration mode, use the command:

no login-dn

Specifying sAMAccountName

If MD5 method is configured to authenticate or synchronize user, the system will send the sAMAccountName and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. To specify the sAMAccountName, in the Active-Directory server configuration mode, use the following command:

login-dn sAMAccountName *string*

- *string* – Specifies the sAMAccountName, which is a string of 1 to 63 characters and is case sensitive.

To cancel the sAMAccountName configuration, in the Active-Directory server configuration mode, use the command:

no login-dn sAMAccountName

Specifying the Login Password

The login password here should correspond to the password for Login DN. To configure the login password, in the Active-Directory server configuration mode, use the following command:

login-password *string*

- *string* – Specifies the login password for the Active-Directory server.

To cancel the password configuration, in the Active-Directory server configuration mode, use the command:

no login-password

Specifying the Mobile Number Attribute Name

When the mobile number attribute name of the user is specified, the system can obtain the mobile number of the user by using this attribute. The mobile number is used in the SMS-based authentication scenario. For example, in the SSL VPN SMS-based authentication scenario, the system can obtain the mobile number of the user by using this attribute. When the user logs in to SSL VPN, the system will send the SMS verification code to the mobile number. To do this, in Active-Directory server configuration mode, use the following command:

mobile-attribute*string*

- *string* - Specifies the name of the mobile number attribute, which is mobile by default. Valid values: 1 to 63 characters in length, which is not case-insensitive.

To restore the mobile number attribute name to the default value, use the **no mobile-attribute** command.

Specifying the Email Attribute Name

When the email attribute name of the user is specified, the system can obtain the email address of the user by using this attribute. The email address is used in the email-based authentication scenario. For example, in the SSL VPN email-based authentication scenario, the system can obtain the email address of the user by using this attribute. When the user logs in to SSL VPN, the system will send the verification code to the email address. To do this, in Active-Directory server configuration mode, use the following command:

email-attribute*string*

- *string* - Specifies the name of the email attribute, which is mail by default. Valid values: 1 to 63 characters in length, which is not case-insensitive.

To restore the email attribute name to the default value, use the **no email-attribute** command.

Enabling/Disabling the SSL Encrypted Connection

With the SSL encrypted connection function enabled, the system connects to the Active Directory authentication server through SSL, thus ensuring the security of data transmission between the system and the Active Directory authentication server. To enable/disable the SSL encrypted connection, in the Active-Directory server configuration mode, use the following command:

connect-through-SSL {**enable** | **disable**}

- **enable** | **disable** - Enable (**enable**) or (**disable**) the SSL encrypted connection function.

Specifying User Name Format

During user authentication, the system will extract the user name based on the configured authentication user name format. If the desired format is not available, the system will directly use the original user name for authentication.

To specify the authentication user name format, in the Active-Directory server configuration mode, use the following command:

extract-username-format authenticate { [**domain\username**] [**username@domain**] }

To delete configuration of the authentication user name format, in the Active-Directory server configuration mode, use the following command:

no extract-username-format authenticate { [**domain\username**] [**username@domain**] }

While implementing policy control based on user name or user group, the system will search the group to which a user name belongs from the organization units locally stored.

To specify the user name format supported when searching for the user group, in the Active-Directory server configuration mode, use the following command:

extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

To delete configuration of the user name format for searching groups, in the Active-Directory server configuration mode, use the following command:

no extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure role mapping rules, in the Active-Directory server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing mapping rule.

To cancel the role mapping rule configuration, in the Active-Directory server configuration mode, use the command:

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the Active-Directory server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the Active-Directory server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the Active-Directory server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring an LDAP User

You can configure users for different LDAP servers. To create a LDAP user, in the LDAP server configuration mode, use the following command:

user*user-name*

• *user-name* – Specifies the user name. The value range is 1 to 63 characters.

After executing this command, the system will create a user with the specified name and enter the user configuration mode. If the specified user name already exists, the system will directly enter the user configuration mode. In the LDAP server configuration mode, use the following command to delete the specified user:

no user *user-name*

Configuring User Expiration

Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire. To specify user expiration, in the user configuration mode, use the following command:

expire*Month/day/year HH:MM*

• *Month/day/year HH:MM* – Specifies the date and time for user expiration. The date is in the format of DD/MM/YYYY HH:SS. For example, command**expire***02/12/2022 12:00* indicates that user expires on February 12, 2022 at 12:00.

To cancel user expiration, in the user configuration mode, use the following command:

no expire

Configuring the Brute-force Cracking Defense

To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP, i.e., within the specified

period, if the failed attempts reached the specified times, the user or IP will be locked for a while. The Brute-force Cracking Defense configuration includes:

- Enabling/Disabling the Brute-force Cracking Defense
- Configuring the number of attempts
- Configuring the lock time
- Viewing the Lockout Information
- Unlocking the User / IP

Enabling/Disabling the Brute-force Cracking Defense

By default, the Brute-force Cracking Defense function is disabled. To enable this function, in the Active-Directory server configuration mode, use the following command:

- Enable: **lockout** {**ip** | **user**} **enable**
- Disable: **lockout** {**ip** | **user**} **disable**

Configuring the Number of Attempts

The number of attempts, that is, the allowed times of login failure within the specified time. To configure the number of attempts, in the Active-Directory server configuration mode, use the following command:

lockout {**ip** | **user**} **failed-attempts***number* **interval***interval*

- **failed-attempts***number* – Specifies the allowed times of login failure. For lockout user, the range is 1 to 32, the default value is 5. For lockout IP, the range is 1 to 2048, the default value is 64.
- **interval** *interval* – Specifies the allowed time of login. The range is 1 to 180 and the default value is 60 seconds.

Configuring the Lockout Time

If the failed attempts reached the specified times in the specified time, the user or IP will be locked out for a while. To configure the lockout time, in the Active-Directory server configuration mode, use the following command:

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time***time* – Specifies the lockout time. The range is 30 to 180. The default value is 600 seconds for lockout user, and 60 seconds for lockout IP.

Viewing the Lockout Information

To view the information of locked user or IP, in any mode, use the following command:

show aaa-server*aaa-server-name***lockout** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specifies the name of AAA server.
- **user** [*username*] - View the information of the locked user of the specified name.
- **ip** [*ip-address***vr_id***number*] - View the information of the locked IP of the specified IP address and VRouter ID.

Unlocking the User / IP

To unlock and delete the user or IP, in any mode, use the following command:

exec aaa aaa-server*aaa-server-name***lockout delete** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specify the name of the AAA server.
- **user** [*username*] - Unlock the user of the specified name.
- **ip** [*ip-address***vr_id***number*] - Unlock the IP of the specified IP address and VRouter ID.

Configuring an AD User

You can configure users for different AD servers. To create an AD user, in the Active-Directory server configuration mode, use the following command:

user*user-name*

• *user-name* – Specifies the user name. The value range is 1 to 63 characters.

After executing this command, the system will create a user with the specified name and enter the user configuration mode. If the specified user name already exists, the system will directly enter the user configuration mode. In the Active-Directory server configuration mode, use the following command to delete the specified user:

no user *user-name*

Configuring User Expiration

Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire. To specify user expiration, in the user configuration mode, use the following command:

expire*Month/day/year HH:MM*

• *Month/day/year HH:MM* – Specifies the date and time for user expiration. The date is in the format of DD/MM/YYYY HH:SS. For example, command**expire***02/12/2022 12:00* indicates that user expires on February 12, 2022 at 12:00.

To cancel user expiration, in the user configuration mode, use the following command:

no expire

User Synchronization

User synchronization specifies that the system will synchronize user information on the configured Active-Directory server to the local. By default, the system will synchronize user information every 30 minutes.

Enable or Disable User Synchronization

Before synchronizing user information, you need to enable synchronization function. By default, it is enabled. To enable or disable user synchronization function, in the Active-Directory

configuration mode, use the following command:

- Enable user synchronization: **sync enable**
- Disable user synchronization: **sync disable**

Configuring User Synchronization

System supports two synchronization modes: manual synchronization and automatic synchronization.

Manul Synchronization

In the Active-Directory configuration mode, use the following command to update the connections with Active-Directory server and manually synchronize user information:

manual-sync

After executing the command, system will synchronize information immediately. If reconfigure the command during synchronization process, the system will clear the existed user information and resynchronize.

Automatic Synchronization

To configure the automatic synchronization, in the Active-Directory server configuration mode, use the following command:

auto-sync {**periodically** *interval* | **daily** *HH:MM* | **once**}

- *interval* – Specifies the time interval of automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.
- *HH:MM* – Specifies the time when the user information is synchronized everyday. HH and MM indicates hour and minute respectively.
- *once* – If this parameter is specified, the system will synchronize automatically when the configuration of Active-Directory server is modified. After executing this command , the system will synchronize user information immediately.

By default, the system will synchronize the user information on the authentication server to the local every 30 minutes. To restore the automatic synchronization mode to default, in Active-Directory server configuration mode, use the following command:

no auto-sync

Specifying Naming Attribute

After you specify the value of the username attribute, when the system synchronizes user information to the local server, the system can obtain the username by using this attribute; When the system performs user authentication, the system can identify the user by using this attribute. To do this, in Active-Directory server configuration mode, use the following command:

naming-attribute*string*

- *string* − Specifies the value of the username attribute, which needs to be a string whose length is 1 to 63 characters. The string is usually cn (Common Name), name, or sAMAccountName. The default value is sAMAccountName.

To restore the username attribute to the default value, in Active-Directory server configuration mode, use the following command:

no naming-attribute

Specifying Group Class

Specify the value of objectClass of the user group. When the system synchronizes Active Directory user information to the local server, the system will filter user information based on group class. To do this, in Active-Directory server configuration mode, use the following command:

group-class*string*

- *string* − Specifies the value of objectClass of the user group, which needs to be string whose length is 1 to 63 characters in length. The default value is group.

You can repeatedly use the command above to configure multiple group classes. The system allows you to configure at most 8 group classes and the logical operator among them is OR. In other words, user information that meets at least one group class can be synchronized to the system.

To delete the specified group class, in Active-Directory server configuration mode, use the **no group-class***string* command. After all group classes are deleted, the default group class is restored.

Specifying User Class

Specify the value of objectClass of the user. When the system synchronizes Active Directory user information to the local server, the system will filter user information based on user class. To do this, in Active-Directory server configuration mode, use the following command:

user-class*string*

- *string* – Specifies the value of objectClass of the user, which needs to be string whose length is 1 to 63 characters in length. The default value is person.

You can repeatedly use the command above to configure multiple user classes. The system allows you to configure at most 8 user classes and the logical operator among them is OR. In other words, user information that meets at least one user class can be synchronized to the system.

To delete the specified user class, in Active-Directory server configuration mode, use the **no user-class***string* command. After all user classes are deleted, the default user class is restored.

Configuring User Filter

After configuring user filters, the system can only synchronize and authenticate users that are match the filters on the authentication server. You must enter AAA server configuration mode before configuring user filter.

To enter the Active-Directory server configuration mode, in the global configuration mode, use the command:

aaa-server *aaa-server-name* **type active-directory**

To configure user-filter, in the Active-Directory server configuration mode, use the following command:

user-filter *filter-string*

- *filter-string* – Specifies the user filters. The length is 0 to 120 characters. For example, when you configure an Active-Directory server, if the *filter-string* is configured to "memberOf=CN=Admin, DC=test, DC=com", which indicates that the system only can

synchronize or authenticate user whose DN is “memberOf=CN=Admin,DC=test,DC=com”.

The commonly used operators are as follows:

Operator	Meaning
=	Equals a value.
&	and
|	or
!	not
*	Wildcard. It represents zero or more characters.
~=	fuzzy query
>=	Be equal or greater than a specified value in lexicographical order.
<=	Be equal or less than a specified value in lexicographical order.



Notes:

- The hillstone system supports all the operators that Active-Directory server supports.
- If the entered format does not comply with the rules of the Active-Directory server, the system may fail to synchronize or authenticate users from the server.

In the Active-Directory server configuration mode, use **no user-filter** to cancel the above configuration.

Configuring Synchronization Mode of User Information

Two synchronization modes can be selected to synchronize organization structure and user information to local from Active-Directory server: OU-based and Group-based, so that you can

configure above two types of user group in security policy rules. By default, user information will be synchronized to the local based on Group.

To configure the synchronization mode of user information, in the Active-Directory server configuration mode, use the following command:

sync-type {**ou** | **group**}

- **ou** – Synchronizes user information to the local based on OU.
- **group** – Synchronizes user information to the local based on Group.

If the OU mode is selected, you can configure the maximum depth of OU to be synchronized. In the Active-Directory server configuration mode, use the following command:

sync-ou-depth *depth-value*

- *depth-value* – Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized to the local.

Configuring a Backup Authentication Server

After configuring a backup authentication server for the Active-Directory server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the Active-Directory server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the Active-Directory server configuration mode, use the following command:

no backup-aaa-server



Notes:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If an Active-Directory server is configured with backup server 1 (backup1), backup server 2 (backup2) and backup authentication server (backup-aaa-server), when user's authentication request is not responded on the primary server, the system will re-authenticate the user on backup server 1 or backup server 2, and if user's authentication request is not responded on backup server 1 or backup server 2, the system will re-authenticate the user on the backup authentication server; when user's authentication failed on the primary server, backup server 1 or backup server 2, the system will re-authenticate the user on the backup authentication server.

Configuring the User-Groups under Base-DN Synchronization

When you sync the users and user-groups from Active-Directory server, you can enable or disable the user-groups under Base-DN Synchronization as need. In the Active-Directory server configuration mode, use the following command:

- Enable: **sync-group-under-basedn enable**
- Disable: **no sync-group-under-basedn enable**

Enabling/Disabling Authentication Simplification

Authentication is required before the system establishes connection with the Active-Directory server. During the connection authentication, the system first sends a request to query the encryption method of the server, and then connects to the server based on the queried encryption method. In some cases, the server forbids to response requests querying its encryption method, resulting in failed connection authentication between the system and the server. To solve this issue, the system supports the simplified authentication. With this feature enabled, the system connects to the Active-Directory server by using the authentication method configured in the system (with the command **auth-method** {**plain** | **digest-md5**}) and no longer queries the encryption method of the server.

By default, authentication simplification is disabled. To enable/disable authentication simplification, in the Active-Directory server configuration mode, use the following command:

simplified-authentication {**enable** | **disable**}

- **enable** - Enable authentication simplification.
- **disable** - Disable authentication simplification.



Notes: With authentication simplification enabled, if MD5 (configured with the command **auth-method digest-md5**) is used for authentication between the system and the Active-Directory server, to make authentication successful, you need to specify the domain name (the full name of the server system such as "WIN-S3VE2GEH3CK.addomain.com" instead of the IP address) of the authentication server and obtain the mapping relationship between the domain name and the IP address through DNS. (We recommend that you configure DNS static cache to map the domain name of the authentication server to the IP address)

Configuring an LDAP Authentication Server

To enter the LDAP server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type ldap**.

The LDAP authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the authentication or synchronization method
- Refreshing the connection with the Server
- Specifying the Base-DN
- Specifying the Synchronization Base-DN
- Specifying the Synchronization Object
- Specifying the login DN
- Specifying Authid
- Specifying the login password
- Enabling/Disabling the SSL Encrypted Connection
- Specifying the name attribute
- Specifying the group name attribute
- Specifying the Group-class
- Specifying user class
- Specifying the member attribute
- Specifying the mobile number attribute name
- Specifying the email attribute name

- Specifying user name format
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring the Brute-force Cracking Defense
- Configuring automatic user information synchronization
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server
- Enabling/Disabling Authentication Simplification

Configuring the IP Address, Domain Name, or VRouter of the Primary Server

To configure the IP address or domain name of the primary authentication server, in the LDAP server configuration mode, use the following command:

host {*ip-address* | *host-name* } [**vrouter** *vrouter-name*]

- *ip-address* | host-name – Specifies the IP address (IPv4 or IPv6)or domain name of the primary authentication server.
- **vrouter** *vrouter-name* – Specifies the VRouter that the primary server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the primary authentication server, in the LDAP server configuration mode, use the command:

no host

Configuring the IP Address, Domain Name, or VRouter of the Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start

checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 1, in the LDAP server configuration mode, use the following command:

backup1 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup authentication server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the LDAP server configuration mode, use the command:

no backup1

Configuring the IP Address, Domain Name, VRouter of the Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server’ s check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 2, in the LDAP server configuration mode, use the following command:

backup2 {*ip-address* | *host-name* }[**vrouter** *vrouter-name*]

- *ip-address* | *host-name* – Specifies the IP address (IPv4 or IPv6) or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 2, in the LDAP server configuration mode, use the command

no backup2

Configuring the Port Number

To configure the port number of the LDAP server, in the LDAP server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the LDAP server. The value range is 1 to 65535. The default value is 389.

To restore to the default value, in the LDAP server configuration mode, use the command:

no port

Configuring the Authentication or Synchronization Method

Plain text and MD5 method can be configured to authenticate or synchronize user between the LDAP server and the system. To configure the authentication or synchronization method, in the LDAP server configuration mode, use the following command:

auth-method {**plain** | **digest-md5**}

- **plain** – Specifies the authentication or synchronization method to be plain text.
- **digest-md5** – Specifies the authentication or synchronization method to be MD5. The default method is MD5.

To restore to the default authentication or synchronization method, in the LDAP server configuration mode, use the command:

no auth-method



Notes: If the Authid is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.

Specifying the Base-DN

Base-DN is the starting point at which your search will begin when the LDAP server receives an authentication request. To specify the Base-DN, in the LDAP server configuration mode, use the following command:

base-dn *string*

- *string* – Specifies the Base-DN for the LDAP server, such as dc = hillstonenet.

To cancel the Base-DN configuration, in the LDAP server configuration mode, use the command:

no base-dn

Specifying the Synchronization Base-DN

When the LDAP server receives an authentication request, it will begin search directories from the Base-DN. If Synchronization Base-DN is specified, all users and groups in the Base-DN will be synchronized to the local. To specify the Synchronization Base-DN, in the LDAP server configuration mode, use the following command:

sync-base-dn *string*

- *string* - Specifies the Synchronization Base-DN for the LDAP server, such as OU=A, dc = hillstonenet, dc=com.

To cancel the Synchronization Base-DN configuration, in the LDAP server configuration mode, use the command **no sync-base-dn**.

Specifying the Synchronization Object

If the Synchronization Base-DN is specified, only users and groups in the Synchronization Base-DN directory will be synchronized to the local. If no Synchronization Base-DN is specified, users and groups in the Base-DN will be synchronized to the local. After you specify that the Synchronization Object is users or groups, the system filters the information synchronized to the local and retains the information of the specified object. To specify the Synchronization Object., in the LDAP server configuration mode, use the following command:

sync-object {**user** | **group**}

- **user** – Specifies the Synchronization Object as users. System will retain user information only.
- **group** – Specifies the Synchronization Object as groups. System will retain group information only.

Specifying the Authentication Base-DN

When the LDAP server receives an authentication request, it will begin search directories from the Base-DN. All users in the Base-DN (including those directly under the user group) will be

allowed to pass the authentication when you specify the Authentication Base-DN. To specify the Authentication Base-DN, in the LDAP server configuration mode, use the following command:

auth-base-dn *string*

- *string* - Specifies the Authentication Base-DN for the LDAP server, such as OU=A, dc = hillstonenet, dc=com.

To delete the Authentication Base-DN configuration, in the LDAP server configuration mode, use the command **no auth-base-dn**.

Specifying the Login DN

If plain text method is configured to authenticate or synchronize user, the system will send the login DN and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. The login DN is typically a user account with query privilege predefined by the LDAP server. To specify the login DN, in the LDAP server configuration mode, use the following command:

login-dn *string*

- *string* – Specify the login DN for the LDAP server, which is a string of 1 to 255 characters and is not case sensitive.

To cancel the login DN configuration, in the LDAP server configuration mode, use the command:

no login-dn

Specifying Authid

If MD5 method is configured to authenticate or synchronize user, the system will send the Authid and the login password to the server to be authenticated, in order to connect to the server for user authentication or synchronization. To specify the Authid, in the LDAP server configuration mode, use the following command:

login-dn authid *string*

- *string* – Specifies the Authid, which is a string of 1 to 63 characters and is case sensitive.

To cancel the Authid configuration, in the LDAP server configuration mode, use the command:

no login-dn Authid

Configuring the Login Password

The login password here should correspond to the password for Login DN. To configure the login password, in the LDAP server configuration mode, use the following command:

login-password *string*

- *string* − Specifies the login password for the LDAP server.

To cancel the password configuration, in the LDAP server configuration mode, use the command:

no login-password

Enabling/Disabling the SSL Encrypted Connection

With the SSL encrypted connection function enabled, the system connects to the LDAP authentication server through SSL, thus ensuring the security of data transmission between the system and the LDAP authentication server. To enable/disable the SSL encrypted connection, in the LDAP server configuration mode, use the following command:

connect-through-SSL {**enable** | **disable**}

- **enable** | **disable** - Enable (**enable**) or (**disable**) the SSL encrypted connection function.

Specifying the Name Attribute

The name attribute is a string that uniquely identifies name in the LDAP server. To specify the name attribute, in the LDAP server configuration mode, use the following command:

naming-attribute *string*

- *string* − Specifies the name attribute. The length is 1 to 63 characters. The string is usually uid (User ID) or cn (Common Name). The default name attribute is uid.

To restore to the default value, in the LDAP server configuration mode, use the command:

no naming-attribute

Specifying the Group Name Attribute

The group name attribute is a string that uniquely identifies user group in the LDAP server. To specify the group name attribute, in the LDAP server configuration mode, use the following command:

group-naming-attribute *string*

- *string* − Specifies the group name attribute. The length is 1 to 63 characters. The string is usually uid (User ID) or cn (Common Name). The default name attribute is uid.

To restore to the default value, in the LDAP server configuration mode, use the command:

no group-naming-attribute

Specifying the Group-class

To specify the ObjectClass of the Group-class, in the LDAP server configuration mode, use the following command:

group-class *string*

- *string* − Specifies the Group-class. The length is 1 to 63 characters. The default value is groupOfUniqueNames.

You can repeatedly use the command above to configure multiple group classes. The system allows you to configure at most 8 group classes and the logical operator among them is OR. In other words, user information that meets at least one group class can be synchronized to the system.

To restore to the default value, in the LDAP server configuration mode, use the command:

no group-class *string*

Specifying User Class

Specify the value of objectClass of the user. When the system synchronizes LDAP user information to the local server, the system will filter user information based on user class. To do this, in LDAP server configuration mode, use the following command:

user-class*string*

- *string* – Specifies the value of objectClass of the user, which needs to be string whose length is 1 to 63 characters in length. The default value is inetOrgPerson, uidObject, or person.

You can repeatedly use the command above to configure multiple user classes. The system allows you to configure at most 8 user classes and the logical operator among them is OR. In other words, user information that meets at least one user class can be synchronized to the system.

To delete the specified user class, in LDAP server configuration mode, use the **no user-class***string* command. After all user classes are deleted, the default user class is restored.

Specifying the Member Attribute

To specify the member attribute of the Group-class, in the LDAP server configuration mode, use the following command:

member-attribute *string*

- *string* – Specifies the member attribute. The length is 1 to 63 characters. The default value is uniqueMember.

To restore the default value, in the LDAP server configuration mode, use the command:

no member-attribute

Specifying the Mobile Number Attribute Name

When the mobile number attribute name of the user is specified, the system can obtain the mobile number of the user by using this attribute. The mobile number is used in the SMS-based authentication scenario. For example, in the SSL VPN SMS-based authentication scenario, the system can obtain the mobile number of the user by using this attribute. When the user logs in to SSL VPN, the system will send the SMS verification code to the mobile number. To do this, in LDAP server configuration mode, use the following command:

mobile-attribute*string*

- *string* - Specifies the name of the mobile number attribute, which is mobile by default. Valid values: 1 to 63 characters in length, which is not case-insensitive.

To restore the mobile number attribute name to the default value, use the **no mobile-attribute** command.

Specifying the Email Attribute Name

When the email attribute name of the user is specified, the system can obtain the email address of the user by using this attribute. The email address is used in the email-based authentication scenario. For example, in the SSL VPN email-based authentication scenario, the system can obtain the email address of the user by using this attribute. When the user logs in to SSL VPN, the system will send the verification code to the email address. To do this, in LDAP server configuration mode, use the following command:

email-attribute*string*

- *string* - Specifies the name of the email attribute, which is mail by default. Valid values: 1 to 63 characters in length, which is not case-insensitive.

To restore the email attribute name to the default value, use the **no email-attribute** command.

Specifying User Name Format

During user authentication, the system will extract the user name based on the configured authentication user name format. If the desired format is not available, the system will directly use the original user name for authentication.

To specify the authentication user name format, in the LDAP server configuration mode, use the following command:

extract-username-format authenticate { [**domain\username**] [**username@domain**] }

To delete configuration of the authentication user name format, in the LDAP server configuration mode, use the following command:

no extract-username-format authenticate { [**domain\username**] [**username@domain**] }

While implementing policy control based on user name or user group, the system will search the group to which a user name belongs from the organization units locally stored.

To specify the user name format supported when searching for the user group, in the LDAP server configuration mode, use the following command:

extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

To delete configuration of the user name format for searching groups, in the LDAP server configuration mode, use the following command:

no extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

Specifying the Mobile Attribute field

When SSL VPN SMS authentication is authenticated by the LDAP server, user's mobile phone number can be obtained via the mobile attribute field. To specify the mobile attribute field, in the LDAP server configuration mode, use the following command:

mobile-attribute *string*

string - Specifies the name of the mobile attribute field. The default value is mobile. The value is case-insensitive and its range is from 1 to 63 characters.

Use the command **no mobile-attribute** to delete the configured mobile attribute field.

Specifying a Role Mapping Rule

After specifying the role mapping rule, the system will assign a role for users who have been authenticated by the server according to the specified role mapping rule. To configure role mapping rules, in the LDAP server configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* – Specifies the name of the existing mapping rule.

To cancel the role mapping rule configuration, in the LDAP server configuration mode, use the command

no role-mapping-rule

Configuring a User Blacklist

After configuring a user blacklist for the LDAP server, the system will not allow blacklist users who are authenticated by the server to access any network resource. To configure a user blacklist, in the LDAP server configuration mode, use the following command:

user-black-list username *user-name*

- *user-name* – Specifies the username of blacklist user. The value range is 1 to 63 characters.

To delete a user from the blacklist, in the LDAP server configuration mode, use the following command:

no user-black-list username *user-name*

Configuring the Brute-force Cracking Defense

To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP, i.e., within the specified period, if the failed attempts reached the specified times, the user or IP will be locked for a while. The Brute-force Cracking Defense configuration includes:

- Enabling/Disabling the Brute-force Cracking Defense
- Configuring the number of attempts
- Configuring the lock time

Enabling/Disabling the Brute-force Cracking Defense

By default, the Brute-force Cracking Defense function is disabled. To enable this function, in the LDAP server configuration mode, use the following command:

- Enable: **lockout** {**ip** | **user**} **enable**
- Disable: **lockout** {**ip** | **user**} **disable**

Configuring the Number of Attempts

The number of attempts, that is, the allowed times of login failure within the specified time. To configure the number of attempts, in the LDAP server configuration mode, use the following command:

lockout {**ip** | **user**} **failed-attempts***number* **interval***interval*

- **failed-attempts***number* – Specifies the allowed times of login failure. For lockout user, the range is 1 to 32, the default value is 5. For lockout IP, the range is 1 to 2048, the default

value is 64.

- **interval** *interval* – Specifies the allowed time of login. The range is 1 to 180 and the default value is 60 seconds.

Configuring the Lockout Time

If the failed attempts reached the specified times in the specified time, the user or IP will be locked out for a while. To configure the lockout time, in the LDAP server configuration mode, use the following command:

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time***time* – Specifies the lockout time. The range is 30 to 180. The default value is 600 seconds for lockout user, and 60 seconds for lockout IP.

Viewing the Lockout Information

To view the information of locked user or IP, in any mode, use the following command:

show aaa-server*aaa-server-name***lockout** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specifies the name of AAA server.
- **user** [*username*] - View the information of the locked user of the specified name.
- **ip** [*ip-address***vr_id***number*] - View the information of the locked IP of the specified IP address and VRouter ID.

Unlocking the User / IP

To unlock and delete the user or IP, in any mode, use the following command:

exec aaa aaa-server*aaa-server-name***lockout delete** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specify the name of the AAA server.
- **user** [*username*] - Unlock the user of the specified name.
- **ip** [*ip-address***vr_id***number*] - Unlock the IP of the specified IP address and VRouter ID.

User Synchronization

User synchronization specifies that the system will synchronize user information on the configured LDAP server to the local. By default, the system will synchronize user information every 30 minutes.

Enable or Disable User Synchronization

Before synchronizing user information, you need to enable synchronization function. By default, it is enabled. To enable or disable user synchronization function, in the LDAP configuration mode, use the following command:

- Enable user synchronization: **sync enable**
- Disable user synchronization: **sync disable**

Configuring User Synchronization

System supports two synchronization modes: manual synchronization and automatic synchronization.

Manul Synchronization

In the LDAP configuration mode, use the following command to update the connections with LDAP server and manually synchronize user information:

manual-sync

After executing the command, system will synchronize information immediately. If reconfigure the command during synchronization process, the system will clear the existed user information and resynchronize.

Automatic Synchronization

To configure the automatic synchronization, in the LDAP server configuration mode, use the following command:

auto-sync {**periodically** *interval* | **daily** *HH:MM* | **once**}

- *interval* – Specifies the time interval of automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.
- *HH:MM* – Specifies the time when the user information is synchronized everyday. HH and MM indicates hour and minute respectively.
- **once** – If this parameter is specified, the system will synchronize automatically when the configuration of LDAP server is modified. After executing this command , the system will synchronize user information immediately.

By default, the system will synchronize the user information on the authentication server to the local every 30 minutes. To restore the automatic synchronization mode to default, in the LDAP server configuration mode, use the following command:

no auto-sync

Configuring User Filter

After configuring user filters, the system can only synchronize and authenticate users that are match the filters on the authentication server. You must enter AAA server configuration mode before configuring user filter.

To enter the LDAP server configuration mode, in the global configuration mode, use the command:

aaa-server *aaa-server-name* **type ldap**

To configure user-filter, in the LDAP server configuration mode, use the following command:

user-filter *filter-string*

- filter-string – Specifies the user filters. The length is 0 to 120 characters. For example, when you configure a LDAP server, if the filter-string is configured to "(|(object-

class=inetOrgperson)(objectclass=person))”, which means that the system only can synchronize or authenticate users which are defined as inetOrgperson or person.

The commonly used operators are as follows:

Operator	Meaning
=	equals a value
&	and
|	or
!	not
*	Wildcard. It represents zero or more characters.
~=	fuzzy query
>=	Be equal or greater than a specified value in lexicographical order.
<=	Be equal or less than a specified value in lexicographical order.

Notes:

- The hillstone system supports all the operators that LDAP server supports.
- If the entered format does not comply with the rules of the LDAP server, the system may fail to synchronize or authenticate users from the server.

In the LDAP server configuration mode, use **no user-filter** to cancel the above configuration.

Configuring Synchronization Mode of User Information

Two synchronization modes can be selected to synchronize organization structure and user information to local from LDAP server: OU-based and Group-based, so that you can configure above two types of user group in security policy rules. By default, user information will be synchronized to the local based on Group.

To configure the synchronization mode of user information, in the LDAP server configuration mode, use the following command:

sync-type {**ou** | **group**}

- **ou** – Synchronizes user information to the local based on OU.
- **group** – Synchronizes user information to the local based on Group.

If the OU mode is selected, you can configure the maximum depth of OU to be synchronized. In the LDAP server configuration mode, use the following command:

sync-ou-depth *depth-value*

- *depth-value* – Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized to the local.

Configuring a Backup AAA Server

After configuring a backup authentication server for the LDAP server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in the system. To configure a backup authentication server, in the LDAP server configuration mode, use the following command:

backup-aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies an AAA server defined in the system.

To cancel the specified backup authentication server, in the LDAP server configuration mode, use the following command:

no backup-aaa-server

Notes:

- The backup authentication server and primary server should belong to the same VSYS. For more information about VSYS, see Virtual System.
- The backup authentication server should not nest another backup authentication server.
- Before deleting an AAA server, make sure the server is not specified as a backup authentication server.
- If an LDAP server is configured with backup server 1 (**backup1**), backup server 2 (**backup2**) and backup authentication server (**backup-aaa-server**), when user's authentication request is not responded on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server; when user's authentication failed on the primary server, the system will re-authenticate the user in the following order: backup server 1 -> backup server 2 -> backup authentication server.

Enabling/Disabling Authentication Simplification

Authentication is required before the system establishes connection with the LDAP server. During the connection authentication, the system first sends a request to query the encryption method of the server, and then connects to the server based on the queried encryption method. In some cases, the server forbids to response requests querying its encryption method, resulting in failed connection authentication between the system and the server. To solve this issue, the system supports the simplified authentication. With this feature enabled, the system connects to the LDAP server by using the authentication method configured in the system (with the command **auth-method** {**plain** | **digest-md5**}) and no longer queries the encryption method of the server.

By default, authentication simplification is disabled. To enable/disable authentication simplification, in the LDAP server configuration mode, use the following command:

simplified-authentication {**enable** | **disable**}

- **enable** - Enable authentication simplification.
- **disable** - Disable authentication simplification.

Configuring TACACS+ Authentication Server

Unser global mode, use the command aaa-server aaa-server-name type tacacs+ to enter TACACS+ server configuration mode.

Configuration of TACACS+ server includes:

- Configuring IP or Domain Name of Primary Authentication Server
- Configuring IP or Domain Name of Backup Server 1
- Configuring IP or Domain Name of Backup Server 2
- Configuring Port of TACACS+ Server
- Configuring Secret of TACACS+ Server
- Specifying User Name Format
- Configuring Role Mapping Rule
- Configuring the Brute-force Cracking Defense

Configuring IP or Domain Name of Primary Authentication Server

To configure the IP address or domain name of TACACS+ authentication server, under TACACS+ server configuration mode, use the command below:

host {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter***vrouter-name*]

- *ipv4-address* | *ipv6-address* | *host-name* – Specify the IPv4 address, IPv6 address, or domain name of the current primary TACACS+ server.

- **vrouter** *vrouter-name* – Specify the VRouter which the current TACACS+ server belongs to. The default VR is trust-vr.

Under TACACS+ server configuration mode, use the no command to delete its IP or domain name configuraiton :

no host

Configuring IP Address or Domain Name of Backup Server 1

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server's check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 1, in the TACACS+ server configuration mode, use the following command:

backup1 {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter***vrouter-name*]

- *ipv4-address* | *ipv6-address* | *host-name* – Specifies the IPv4 address, IPv6 address, or domain name of the backup authentication server 1.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the TACACS+ server configuration mode, use the command:

no backup1

Configuring IP Address or Domain Name of Backup Server 2

This configuration is optional. Backup server must be of the same type of primary server. When the authentication does not pass primary server's check, the backup server 1 and 2 will start checking its credentials consecuritvely.To configure the IP address or domain name of the backup authentication server 1, in the TACACS+ server configuration mode, use the following command:

backup2 {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter***vrouter-name*]

- *ipv4-address* | *ipv6-address* | *host-name* – Specifies the IPv4 address, IPv6 address, or domain name of the backup authentication server 2.
- **vrouter** *vrouter-name* – Specifies the VRouter that the backup server belongs to. The default VRouter is trust-vr.

To cancel the IP address or domain name configuration of the backup authentication server 1, in the TACACS+ server configuration mode, use the command:

no backup2

Configuring Port Number of TACACS+ Server

To configure the port number of the TACACS+ server, in its TACACS+ server configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the LDAP server. The default value is 49.

To restore to the default value, in the TACACS+ server configuration mode, use the command:

no port

Configuring Secret of TACACS+ Server

To configure the secret of TACACS+ server, under TACACS+ server configuration mode, use the command below:

secret *secret*

- *secret* – Specifies the secret string of TACACS+ server. The range is 1 to 31 characters.

To delete secret, under TACACS+ server configuration mode, use the no command:

no secret

Specifying User Name Format

During user authentication, the system will extract the user name based on the configured authentication user name format. If the desired format is not available, the system will directly use the

original user name for authentication.

To specify the authentication user name format, in the TACACS+ server configuration mode, use the following command:

extract-username-format authenticate { [**domain\username**] [**username@domain**] }

To delete configuration of the authentication user name format, in the TACACS+ server configuration mode, use the following command:

no extract-username-format authenticate { [**domain\username**] [**username@domain**] }

While implementing policy control based on user name or user group, the system will search the group to which a user name belongs from the organization units locally stored.

To specify the user name format supported when searching for the user group, in the TACACS+ server configuration mode, use the following command:

extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

To delete configuration of the user name format for searching groups, in the TACACS+ server configuration mode, use the following command:

no extract-username-format search-usergroup { [**domain\username**] [**username@domain**] }

Specifying Role Mapping Rule

The role mapping rule can allocate a role for the authenticated users in this server.

To assign a role mapping rule to users in TACACS+ server, under TACACS+ server configuration mode, use the command below:

role-mapping-rule *rule-name*

- *rule-name* – Enter an existing role mapping rule name.

To cancel this rule, under TACACS+ server configuration mode, use the command:

no role-mapping-rule

Configuring TACACS+ Server

TACACS+ server should also be configured if it wants to communicate with StoneOS system. The configuration is to add some user defined attributes.

You should make the following changes in TACACS+ server:

- For tac_plus in Linux: add hillstone attributes, seet the table below:
- For Cisco acs 4.2 and above:add new server with name “hillstone” and edit the service attributes to include hillstone characters, see table below:

Attribute	Description
user-type	User type. admin type=16 all=31 Other types of user do not need this value.
user-vsys-id	vSYS ID value. Admin user must have this attribute. Now, only ID=0 is supported.
user-admin-privilege	Read and Write privilege. Read and write=4294967295 Only read=0
user-admin-role	Administrator role privilege. admin＝Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information. operator＝Permission for reading, executing and writing. You have the authority over all features except modify the Administrator's configuration, view the current or historical configuration information , but no permission for check the log information. auditor＝You can only operate on the log information, including view, export and clear. admin-read-only＝ Permission for reading and executing. You can view the current or historical configuration inform-ation.

Attribute	Description
	Note: This attribute property is higher than **user-admin-privilege**. If the two attributes are configured at the same time, the **user-admin-role** will take effect. You are suggested to use **user-admin-role** directly.
user-login-type	Admin login type. telnet＝2 SSH＝4 CONSOLE＝1 HTTP＝8 HTTPS＝16 all＝31 If you want a combination, the value should the total of selected types (e.g. telnet+SSH＝6).
user-group	This attribute is optional. It defines the user group of the specified user. User group is for user group based policy control.

Configuring the Brute-force Cracking Defense

To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP, i.e., within the specified period, if the failed attempts reached the specified times, the user or IP will be locked for a while. The Brute-force Cracking Defense configuration includes:

- Enabling/Disabling the Brute-force Cracking Defense
- Configuring the number of attempts
- Configuring the lock time

Enabling/Disabling the Brute-force Cracking Defense

By default, the Brute-force Cracking Defense function is disabled. To enable this function, in the TACACS+ server configuration mode, use the following command:

- Enable: **lockout** {**ip** | **user**} **enable**
- Disable: **lockout** {**ip** | **user**} **disable**

Configuring the Number of Attempts

The number of attempts, that is, the allowed times of login failure within the specified time. To configure the number of attempts, in the TACACS+ server configuration mode, use the following command:

lockout {**ip** | **user**} **failed-attempts***number* **interval***interval*

- **failed-attempts***number* – Specifies the allowed times of login failure. For lockout user, the range is 1 to 32, the default value is 5. For lockout IP, the range is 1 to 2048, the default value is 64.
- **interval** *interval* – Specifies the allowed time of login. The range is 1 to 180 and the default value is 60 seconds.

Configuring the Lockout Time

If the failed attempts reached the specified times in the specified time, the user or IP will be locked out for a while. To configure the lockout time, in the TACACS+ server configuration mode, use the following command:

lockout {**ip** | **user**} **lockout-time** *time*

- **lockout-time***time* – Specifies the lockout time. The range is 30 to 180. The default value is 600 seconds for lockout user, and 60 seconds for lockout IP.

Viewing the Lockout Information

To view the information of locked user or IP, in any mode, use the following command:

show aaa-server*aaa-server-name***lockout** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specifies the name of AAA server.
- **user** [*username*] - View the information of the locked user of the specified name.
- **ip** [*ip-address***vr_id***number*] - View the information of the locked IP of the specified IP address and VRouter ID.

Unlocking the User / IP

To unlock and delete the user or IP, in any mode, use the following command:

exec aaa aaa-server*aaa-server-name***lockout delete** {**user** [*username*] | **ip** [*ip-address***vr_id***number*]}

- *aaa-server-name* - Specify the name of the AAA server.
- **user** [*username*] - Unlock the user of the specified name.
- **ip** [*ip-address***vr_id***number*] - Unlock the IP of the specified IP address and VRouter ID.

Configuring an OAuth2 Authorization Server

To enter the configuration mode of the OAuth2 server with a specified name, in global configuration mode, use the **aaa-server** *aaa-server-name* **type oauth** command. The OAuth2 server configuration includes:

1. Basic Configuration
2. Get Authorization Code Configuration
3. Get Access Token Configuration
4. Get User Information Configuration

Notes:

- Only one OAuth2 server can be configured within each VSYS.
- The OAuth2 server that can be connected to the system includes Hillstone User Center and AzureAD.

Basic Configuration

When an OAuth2 server is used for authentication, you need to specify the organization source server, virtual router, and prompt message for the OAuth2 authentication icon on the user authentication page.

Specifying the Organization Source Server

To specify the organization source server to which the authenticated user belongs, in OAuth server configuration mode, use the following command:

organization-source *aaa-server-name*

- *aaa-server-name* – Specifies the AAA server to which the authenticated user belongs. You can select a configured local, AD, or LDAP server. Then, the system can query the user group and role information corresponding to the username of the online user on the referenced AAA server. This can implement policy control based on user group and role.

To delete the organization source server, in OAuth server configuration mode, use the following command:

no organization-source

Specifying the Virtual Router to which the OAuth2 Server Belongs

To specify the virtual router to which the OAuth2 server belongs, in OAuth server configuration mode, use the following command:

vrouter *vrouter-name*

- *aaa-server-name* – Specifies the VRouter to which the OAuth2 server belongs.

To delete the virtual router, in OAuth server configuration mode, use the following command:

no vrouter

Specifying the Name of the OAuth2 Authentication Icon

To specify the name of the OAuth2 authentication icon, in OAuth server configuration mode, use the following command:

authentication-icon-name *name*

- *name* – Specifies the name of the OAuth2 authentication icon. On the user authentication page, when you hover your mouse over the icon, the prompt message about the OAuth2 server is displayed. Example: Use Hillstone User Center for authentication.

To delete the name of the OAuth2 authentication icon, in OAuth server configuration mode, use the following command:

no authentication-icon-name

Get Authorization Code Configuration

When an OAuth2 server is used for authentication, you need to configure the authorization code request, including the OAuth2 server URL, request parameter, and response parameter of the authorization code request.

Entering the Authorization Code Request Configuration Mode

Before you specify the OAuth2 server URL, request parameter, and response parameter of the authorization code request, you need to enter the authorization code request configuration mode. To do this, in OAuth server configuration mode, use the following command:

authorization-code-request

Configuring the OAuth2 Server URL of the Authorization Code Request

To configure the URL of the OAuth2 authorization server from which the system requests an authorization code, in authorization code request configuration mode, use the following command:

request-url *request-url*

- *request-url* – Specifies the URL of the OAuth2 authorization server from which the system requests an authorization code. Example: https://-passport.hillsonenet.com/OAuth/Authorize.

To delete the OAuth2 server URL, in authorization code request configuration mode, use the following command:

no request-url

Configuring client_id

To configure the request parameter client_id that is used for the system to apply for the authorization code, in authorization code request configuration mode, use the following command:

client-id-attribute *name value*

- *name value* – Specifies the client_id attribute. The attribute name *name* is fixed to **"client_id"** and the attribute value *value* is the client ID, which is obtained by the system from registration with the OAuth2 authorization server.

To delete the request parameter client_id, in authorization code request configuration mode, use the following command:

no client-id-attribute

Configuring redirect_uri

To configure the request parameter redirect_uri that is used for the system to apply for the authorization code, in authorization code request configuration mode, use the following command:

redirect-uri-attribute *name value*

- *name value* – Specifies the redirect_uri attribute. The attribute name *name* is fixed to **"redirect_uri"** and the attribute value *value* is the system address to which the server redirects after authorization, provided by the system during registration with the OAuth2 authorization server. This address is listened by the system. The redirect URL is in the following URL: https://host:17443/login/oauth (HTTPS listener) or http://host:17080/login/oauth (HTTP listener).

To delete the request parameter redirect_uri, in authorization code request configuration mode, use the following command:

no redirect-uri-attribute

Configuring the Response Type of the Authorization Code Request

To configure the response type of the authorization code request, in authorization code request configuration mode, use the following command:

response-type-attribute *name value*

- *name value* – Specifies the response type of the authorization code request. The *name* is fixed to **"response_type"**, and the *value* is set to **"code"**. In authorization code mode, the response type is fixed to "code".

To delete the response type of the authorization code request, in authorization code request configuration mode, use the following command:

no response-type-attribute

Configuring Custom Attribute of the Authorization Code Request

To configure the custom attribute in the authorization code request parameters, in authorization code request configuration mode, use the following command:

user-attribute *name value*

- *name value* – Specifies the custom attribute in the authorization code request parameters, including the attribute name *name* and attribute value *value*, which can be configured based on the actual OAuth2 server. You can configure at most 13 custom request parameters.

To delete the custom attribute of the authorization code request, in authorization code request configuration mode, use the following command:

no user-attribute *name*

Configuring the Response Parameter of the Authorization Code

To configure the response parameter of the authorization code, in authorization code request configuration mode, use the following command:

response-attribute-analyze *attribute_name* **mapping** *local_value*

- *attribute_name* **mapping** *local_value* – Specifies the parsed parameter and local variable in the response parameter of the authorization code. In authorization code mode, the parsed parameter *attribute_name* is fixed to "code", and the local variable *local_value* is fixed to **$code**. After the authorization code request succeeds, the system needs to parse the specified attribute field in the response and store it to the local variable for the next access token request.

To delete the response parameter of the authorization code, in authorization code request configuration mode, use the following command:

no response-attribute-analyze

Get Access Token Configuration

When an OAuth2 server is used for authentication, you need to configure the access token request, including the OAuth2 server URL, request parameter, and response parameter of the access token request.

Entering the Access Token Request Configuration Mode

Before you specify the OAuth2 server URL, request parameter, and response parameter of the access token request, you need to enter the access token request configuration mode. To do this,

in OAuth server configuration mode, use the following command:

access-token-request

Configuring the URL of the OAuth2 Server from which the System Requests an Access Token

To configure the URL of the OAuth2 server from which the system requests an access token, in access token request configuration mode, use the following command:

request-url *request-url*

- *request-url* – Specifies the URL of the OAuth2 server from which the system requests an access token. Example: https://passort.hillstonenet.com/OAuth/Token.

To delete the URL of the OAuth2 server, in access token request configuration mode, use the following command:

no request-url

Configuring grant_type

To configure the request parameter grant_type that is used for the system to apply for the access token, in access token request configuration mode, use the following command:

grant-type-attribute *name value*

- *name value* – Specifies the grant_type attribute. The attribute name *name* is fixed to **"grant_type"**, and the attribute value *value* is fixed to **"authorization_code"**, which indicates the authorization type of the authorization server. In authorization code mode, the authorization type is fixed to "authorization_code".

To delete the request parameter grant_type, in access token request configuration mode, use the following command:

no grant-type-attribute

Configuring code

To configure the request parameter code that is used for the system to apply for the access token, in access token request configuration mode, use the following command:

code-attribute *name value*

- *name value* – Specifies the code attribute. The attribute name *name* is fixed to **"code"**, and the attribute value references the local variable **$code**.

To delete the request parameter code, in access token request configuration mode, use the following command:

no code-attribute

Configuring redirect_uri

To configure the request parameter redirect_uri that is used for the system to apply for the access token, in access token request configuration mode, use the following command:

redirect-uri-attribute *name value*

- *name value* – Specifies the redirect_uri attribute. The attribute name *name* is fixed to **"redirect_uri"**. The attribute value *value* is the system address to which the server redirects after authorization, provided by the system during registration with the OAuth2 authorization server. The redirect URL is in the following format: https://*host*:17443/login/oauth (HTTPS listener) or http://*host*:17080/login/oauth (HTTP listener). This redirect URL needs to be consistent with that requested by the authorization code.

To delete the request parameter redirect_uri, in access token request configuration mode, use the following command:

no redirect-uri-attribute

Configuring Custom Attribute of the Access Token Request

To configure the custom attribute in the access token request parameters, in access token request configuration mode, use the following command:

user-attribute *name value* [**add-to-header**]

- *name value* – Specifies the custom attribute in the access token request parameters, including the attribute name *name* and attribute value *value*, which can be configured based on the actual OAuth2 server. You can configure at most 13 custom request parameters.
- **add-to-header** – Specifies to insert the custom attribute into the request header. If not specified, the custom attribute is inserted into the request content.

To delete the custom attribute of the access token request, in access token request configuration mode, use the following command:

no user-attribute *name*

Configuring the Response Parameter of the Access Token

To configure the response parameter of the access token, in access token request configuration mode, use the following command:

response-attribute-analyze *attribute_name* **mapping** *local_value*

- *attribute_name* **mapping** *local_value* – Specifies the parsed parameter and local variable in the response parameter of the access token. In authorization code mode, the parsed parameter *attribute_name* is fixed to **"access_token"**, and the local variable *local_value* is fixed to **$access_token**. After the access token request succeeds, the system needs to parse the specified attribute field in the response and store it to the local variable for the next user information request.

To delete the response parameter of the access token, in access token request configuration mode, use the following command:

no response-attribute-analyze

Get User Information Configuration

When an OAuth2 server is used for authentication, you need to configure the user information request, including the OAuth2 server URL, request parameter, and response parameter of the user information request.

Entering the User Information Request Configuration Mode

Before you specify the OAuth2 server URL, request parameter, and response parameter of the user information request, you need to enter the user information request configuration mode. To do this, in OAuth server configuration mode, use the following command:

user-info-request

Configuring the OAuth2 Server URL of the User Information Request

To configure the URL of the OAuth2 authorization server from which the system requests user information, in access token request configuration mode, use the following command:

request-url *request-url*

- *request-url* – Specifies the URL of the OAuth2 authorization server from which the system requests user information. Example: https://-passport.hillstonenet.com/API/Resource/UserInfo.

To delete the OAuth2 server URL, in user information request configuration mode, use the following command:

no request-url

Configuring Custom Attribute of the User Information Request

To configure the custom attribute in the user information request parameters, in user information request configuration mode, use the following command:

user-attribute *name value* [**add-to-header**]

- *name value* – Specifies the custom attribute in the user information request parameters, including the attribute name *name* and attribute value *value*, which can be configured based on the actual OAuth2 server. For example, the attribute name *name* is set to **"Authorization"**, and the attribute value *value* is set to **"Bearer $access_token"**, which is access_token obtained from the access token. You can configure at most 13 custom request parameters.
- **add-to-header** – Specifies to insert the custom attribute into the request header. If not specified, the custom attribute is inserted into the request content.

To delete the custom attribute of the user information request, in user information request configuration mode, use the following command:

no user-attribute *name*

Configuring the Response Parameter of User Information

To configure the response parameter of the user information, in user information request configuration mode, use the following command:

response-attribute-analyze *attribute_name* **mapping** *local_value*

- *attribute_name* **mapping** *local_value* – Specifies the parsed parameter and local variable in the response parameter of the user information. In authorization code mode, the parsed parameter can be username or mail, and the local variable is fixed to **$username**. After the use information request succeeds, the system needs to parse the specified attribute field in the response and store it to the local variable for displaying the username of the authenticated user.

To delete the response parameter of the user information, in user information request configuration mode, use the following command:

no response-attribute-analyze

Viewing Configuration Information about the Oauth2 Server

show aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the Oauth2 server. Only one Oauth2 server exists within each VSYS.

Example:

```
hostname(config)# show aaa-server oauth-server
==========================================================-
==
aaa-server: oauth-server (shows the Oauth2 server name)
type: oauth (shows that the type of the AAA server is
Oauth2)
vrouter: trust-vr (shows tha VRouter to which the Oauth2
server belongs)
organization source: local (shows the organization source
server to which the authenticated user belongs)
authentication icon name: test (shows the name of the OAuth2
authentication icon)
----------------------------------------------------------
--
authorization code: (shows the authorization code request
configuration information about the Oauth2 server)
request url: https://-
passport.hillsonenet.com/OAuth/Authorize
client_id: 832ee2e3089045b8...
redirect_uri: https://oau-
th2.hillstonenet.com:17443/login/oauth
response_type: code
display: page
scope: full_info
response attribute analyze code: code
```

```
response attribute analyze local value: $code
------------------------------------------------------------
--
access token: (shows the access token request configuration
information about the Oauth2 server)
request url: https://passort.hillstonenet.com/OAuth/Token
grant_type: authorization_code
redirect_uri: https://oau-
th2.hillstonenet.com:17443/login/oauth
code: $code
Authorization: Basic 0DMyZWUyZTMw0Dkw... http-header
response attribute analyze access token: access_token
response attribute analyze local value: $access_token
------------------------------------------------------------
--
user information: (shows the user information request con-
figuration information about the Oauth2 server)
request url: https://-
passport.hillstonenet.com/API/Resource/UserInfo
Authorization: Bearer $access_token http-header
response attribute analyze user infomation: username
response attribute analyze local value: $username
============================================================-
==
```

Configuring a RADIUS Accounting Server

Hillstone devices support accounting for authenticated users via a RADIUS server. To enter the RADIUS server configuration mode, in the global configuration mode, use the command **aaa-**

server *aaa-server-name* **type radius**.

The RADIUS accounting server configuration includes:

- Enabling/Disabling the accounting function
- Configuring the IP address or domain name of the primary/backup server
- Configuring the port number
- Configuring the Secret
- Enabling/Disabling the Offline Management of Accounting User
- Configuring the Extended Password Encryption Algorithm of SM4

Enabling/Disabling the Accounting Function

To enable/disable the accounting function of the RADIUS server, in the RADIUS server configuration mode, use the following commands:

- Enable: **accounting enable**
- Disable: **no accounting enable**

After enabling the accounting function, you can continue to configure other parameters.

Configuring the IP Address or Domain Name of the Primary/Backup Server

To configure the IP address or domain name of the primary or backup accounting server, in the RADIUS server configuration mode, use the following command:

accounting {**host** {*ip-address* | *host-name*} | **backup1** {*ip-address* | *host-name*} | **backup2** {*ip-address* | *host-name*}}

- **host** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the primary server.
- **backup1** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the backup server 1.

- **backup2** {*ip-address* | *host-name*} – Specifies the IP address or domain name of the backup server 2.

To cancel the IP address or domain name configuration of the primary or backup server, in the RADIUS server configuration mode, use the command:

no accounting {**host** | **backup1** | **backup2**}

Configuring the Port Number

To configure the port number of the accounting server, in the RADIUS server configuration mode, use the following command:

accounting port *port-number*

- *port-number* – Specifies the port number of the accounting server. The value range is 1024 to 65535. The default value is 1813.

To restore to the default value of the port number, in the RADIUS server configuration mode, use the command:

no accounting port

Configuring the Secret

To configure the secret of the accounting server, in the RADIUS server configuration mode, use the following command:

accounting secret *secret*

- *secret* – Specifies the secret string of the accounting server. The length is 1 to 31 characters.

To cancel the secret configuration of the accounting server, in the RADIUS server configuration mode, use the command:

no accounting secret

Enabling/Disabling the Offline Management of Accounting User

After the offline management of accouting user is enabled, the system will disconnect from the specified offline user and stop charging according to the offline user information on the Radius

server (including the name of the offline user, the IP address of the offline user, the accounting ID). By default, the function is disabled.

To enable the offline management of accouting user, in the RADIUS server configuration mode, use the following command:

unsolicited-message enable

To disable the offline management of accouting user, in the RADIUS server configuration mode, use the following command:

no unsolicited-message enable

Configuring the Extended Password Encryption Algorithm of SM4

The Radius server supports encrypted storage and encrypted transmission of passwords using the extended password encryption algorithm of SM4. To configure the SM4 extended password encryption algorithm for the Radius server, you need to use the relevant commands in the extended-option configuration mode.

To enter the extended-option configuration mode, in the RADIUS server configuration mode, use the following command:

extend-option

To configure the SM4 extended password encryption algorithm for the Radius server, in the extended-option configuration mode, use the following command:

encryption-algorithm SM4

- **SM4**- Specifies the SM4 extended password encryption algorithm. SM4 is not case sensitive.

To delete the specified extended password encryption algorithm of SM4, use command **no encryption-algorithm**.

Configuring Authentication and Authorization for the Server

After configuring the AAA authentication server, you need to specify one server as the authentication server for the system administrator. By default, the StoneOS system uses the local server as the authentication server, which cannot be deleted.

Configuring Authentication and Authorization for the Server

To Configure authentication and authorization for the server, in the global configuration mode, use the following command:

admin authorization-mode {**local** | **aaa-server** *server-name* [**disable-retry-local**]}

- **local** - Specifies the local server as the authorization server.
- **aaa-server** *server-name* [**disable-retry-local**] - Specifies the external server as the authorization server.
    - *server-name* - Specifies the name of the authentication server. It can be a RADIUS server (`radius`) or a TACACS+ server (`tacacs+`).
    - **disable-retry-local** - Disables the function of the local password retry. By default, if the configured external authentication server is not reachable or the server returns the notification of the password error to StoneOS, the StoneOS system will use the local server as the authentication server. You can disable the function of the local password retry, that is, disable local server authentication. If the specified external server returns the notification of the password error to StoneOS, the local server cannot be used for administrator authentication. The server unreachable is not affected by the configuration of **disable-retry-local** command.

To restore to the default authentication server, in the global configuration mode, use the command **no admin authorization-mode**.

You can, according to your own needs, preferentially use the local server for authentication for administrators who access through the Console mode. If the local server is unreachable or the authentication server is unavailable, the StoneOS system uses the default Radius server for administrator authentication. To specify the local server as the authentication server for administrators who access through the Console mode, in the global configuration mode, use the following command:

admin console local-auth-prior

To disable local server authentication, use the command **no admin console local-auth-prior**.

Viewing the Authorization Information of the Authentication Server

To view the authorization information of the authentication server, in any mode, use the following command:

show admin authorization-mode

Viewing Local Server Authentication Enabled Status

To view the local server authentication enabled status, in any mode, use the following command:

show admin console local-auth-prior

Configuring the Authentication Server for the administrator

If you select the local server authorization, you need to configure the administrator and authentication information. To configure the authentication server, use the following command in the administrator role configuration mode:

authentication-server {**local** | **aaa-server** *server-name* [**retry-local**]}

- **local** - Specifies the local server as the authentication server.
- **aaa-server***server-name* [**retry-local**] - Specifies the external server as the authentication server.
    - *server-name* -Specifies the name of the authentication server. It can be a RADIUS server (`radius`), an Active-Directory server (`active-directory`), an LDAP server (`ldap`) or TACACS+ server (`tacacs+`).
    - **retry-local** - Enables the function of the local password retry. If the external server is unreachable and the local password retry is enabled, the StoneOS system will use the local server as the authentication server. the local server is used for system administrator authentication. If the function of the local password retry is disabled, the local server cannot be used for administrator authentication. If the external server returnsthe notification of the password error to StoneOS, direct authentication fails, regardless of whether **retry-local** is configured.

Viewing and Debugging AAA

To view the configuration information of AAA server, in any mode, use the following command:

show aaa-server [*server-name*]

To view the user blacklist information, in any mode, use the following command:

show user-black-list

To view the debug information of AAA, in any mode, use the following command:

debug aaa [**accounting** | **authentication** | **authorization** | **internal** | **radius** | **ldap** | **user**]

- **accounting** - Shows debug information for accounting.
- **authentication** - Shows debug information for authentication.
- **authorization** - Shows debug information for authorization.
- **internal** - Shows debug information when local users access to the device via local authentication.
- **radius** - Shows debug information for the RADIUS authentication.
- **ldap** - Shows debug information for the LDAP (including Active-Directory server and LDAP server) authentication.
- **user** – Shows debug information when the local user attributes change.

Radius Dynamic Authorization

The Radius dynamic authorization function, includes:

- When the user is authenticated successfully, the Radius server can send a Radius CoA (Change of Authorization) request message to the authority of the authenticated user to the device. The device automatically generates the security policy rule for the user. When the user goes offline, the device delete this user's security policy rule automatically
- When the SSL VPN user is authenticated successfully, the Radius server can send a Radius DM (Disconnect Messages) request message to send the accounting user information (including the user name, user IP address, user accounting ID, etc.) to the device, and the device can disconnect the specified scvpn authentication user and end the accounting.

Enabling / Disabling Radius dynamic authorization

By default, the Radius dynamic authorization is disabled. To enable or disable the Radius dynamic authorization, in the global configuration mode, use the following command:

- Enable: **radius-server dynamic-authorization enable**
- Disable: **no radius-server dynamic-authorization enable**



Notes: If you need to use the Radius dynamic authorization function, first enable and configure the Radius accounting server. For the configuration, refer to "Configuring a RADIUS Accounting Server" on Page 1249.

Configuring a Radius Dynamic Authorization Server

To configure a Radius dynamic authorization server, in the global configuration mode, user the following command:

radius-server dynamic-authorization {**server-ip** *ip-address* [**destination-ip** *destination-ip*]} {**secret** *key-string*}

- **server-ip** *ip-address*- Specifies the IP address (IPv4 or IPv6) of the Radius dynamic authorization server.
- **destination-ip** *destination-ip* - Specifies the destination IP address of the authorization request. This option is optional.
- **secret** *key-string* - Specifies the secret string of the Radius dynamic authorization server. The length is 1 to 31 characters.

To delete the configuration of the Radius dynamic authorization server, in the global configuration mode, user the following command:

no radius-server dynamic-authorizationserver-ip*ip-address*

Configuring the Port Number

To configure the port number of the Radius dynamic authorization server, in the global configuration mode, user the following command:

radius-server dynamic-authorization port *port-number*

- *port-number*- Specifies the port number of the Radius dynamic authorization server. The value range is 1024 to 65535. The default value is 3799.

To restore to the default value of the port number, in the global configuration mode, user the following command:

no radius-server dynamic-authorization port

Viewing Radius Dynamic Authorization Server Configurations

To view the Radius dynamic authorization server configuration, in any mode, use the following command:

show radius-server dynamic-authorization

Radius Snooping

The Remote Authentication Dial-In Up Service (RADIUS) is a protocol that is used for the communication between NAS and AAA server. The RADIUS packet monitoring function analyzes the RADIUS packets that are mirrored to the device and the device will automatically obtain the mappings between the usernames of the authenticated users and the IP addresses (IPv4 or IPv6 addresses). Then the system generates user authentication information and adds it to the authenticated user list to control and audit user traffic.

Entering the Radius Snooping Configuration Mode

To enter the Radius Snooping configuration mode, use the following command in the global configuration mode:

user-sso server radius-snooping default

Enabling the Radius Snooping Function

By default, the Radius Snooping function is disabled. To enable this function, use the following command in the Radius Snooping configuration mode:

- Enable: **enable**
- Disable: **no enable**

Specifying the AAA Server

To specify the AAA server referenced by system, use the following command in the Radius Snooping configuration mode:

aaa-server*aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. The Local, AD or LDAP server is available to select on the AAA server. You're suggested to directly select the configured authentication AD server. After selecting the AAA server, system can query the

corresponding user group and role of the online user on the referenced AAA server, so as to achieve the policy control based on the user group and role.

To cancel the above configurations, use the following command in the Radius Snooping configuration mode:

no aaa-server

Configuring the Idle Time

If the device does not receive the mirrored RADIUS packets within the specified time period, it will delete the mappings between the usernames and the IP addresses. To specify the time period, namely the idle time, use the following command in the Radius Snooping configuration mode:

idle-timeout*timeout*

- *timeout* – Specifies the idle time (in minutes). The value ranges from 1 to 1440.

By default, system will not delete the user authentication information if there is no traffic. To restore the idle time to the default value, use the following command in the Radius Snooping configuration mode:

no idle-timeout

Specifying the Force Timeout Time

To specify the forced logout time, in the Radius Snooping configuration mode, use the following command:

force-timeout*time*

- *time* - Specified the forced logout time. When the online time of a user exceeds the configured force timeout time, system will kick out the user and force the user to log out. The range is 0 (the function is disabled) to 1440 minutes, and the default value is 600 minutes.

To restore the configured force timeout time to default, in the Radius Snooping configuration mode, use the following command:

no force-timeout

Configuring the Heartbeat Timeout Value

When authentication is successful, the system will automatically reconfirm login information before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time, you will log off from the system at the smaller value. To configure the heartbeat timeout value, in the Radius Snooping configuration mode, use the following command:

heartbeat-timeout {*interval* | **disable**}

- *interval* – Specifies the heartbeat timeout value. The value range is 3 to 1440 minutes. The default value is 5 minutes.
- **disable** – Disables the heartbeat timeout function.

To restore to the default heartbeat timeout value, in the Radius Snooping configuration mode, use the command:

no heartbeat-timeout

Configuring the Username Filter

With the Username Filter function, the system excludes usernames ended with a specific string and generates user authentication information only for usernames that are not excluded by the "not end with" filter condition.

To configure username filter, in the Radius Snooping configuration mode, use the following command:

username-filter not-end-with *filter-string*

- **not-end-with** *filter-string* - The "not end with" filter condition indicates that usernames ended with a specific string are excluded. The system generates user authentication information only for usernames not excluded by the "not end with" filter condition. The value range of the string is from 1 to 15 characters.

To delete username filter configuration, in the Radius Snooping configuration mode, use the following command:

no username-filter not-end-with

Viewing the Radius Snooping Configuration Information

To view the Radius Snooping configuration information, in any mode, use the following command:

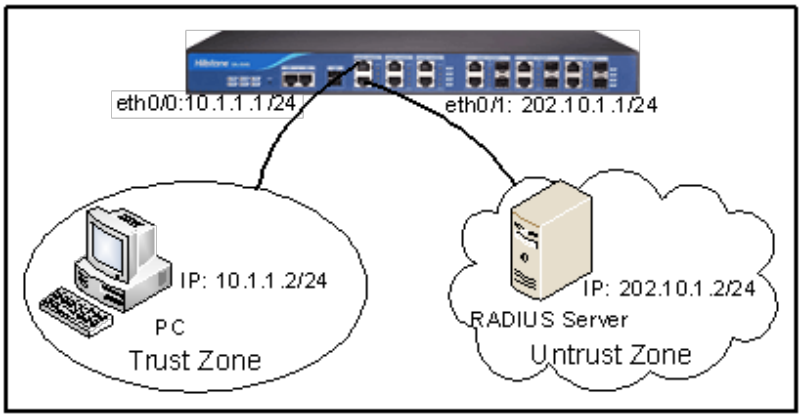
show user-sso server radius-snooping default

Configuration Example

This example shows how to use the external RADIUS authentication server to authenticate Telnet users. Specific requirements and configurations are described as below.

Requirement

The goal is to authenticate the Telnet users via RADIUS server. IP address of the RADIUS authentication server is 202.10.1.2, and there is no back-up server. The retry time is the default value 3. The response timeout is the default value 3. Port 1812 is used for RADIUS authentication. The figure below shows the networking topology.



Configuration Steps

Step 1: Configure the interface

```
hostname# configure
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# manage telnet
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.10.1.1/24
```

Step 2: Enter the AAA server configuration mode

```
hostname(config-aaa-server)# aaa-server rad type radius
```

Step 3: Configure the RADIUS authentication server

```
hostname(config-aaa-server)# host 202.10.1.2
hostname(config-aaa-server)# port 1645
hostname(config-aaa-server)# secret testing123
hostname(config-aaa-server)# exit
```

Step 4: Specify the authentication server for the system

```
hostname(config)# admin auth-server rad
```

Step 5: Verify the results of the configuration

```
hostname(config)# show aaa-server rad
==========================================================-
===========
aaa-server: radius
type: radius
role-mapping-rule :
backup-aaa-server :
server address: 202.10.1.2(trust-vr)
first backup :
```

```
second backup :
radius setting:
port: 1812 secret: a3UfKjOGP80IGeggG9kuvDJ7I8Ye
retries 3 time(s), timeout 3 second(s).
accounting: enable (optional)
accounting setting:
port: 2000 secret: hq8DNiGMUL4Pq2A9tf1422uLRWcF
server address: 202.10.1.2(trust-vr)
first backup :
second backup :
==========-
==========
```

User Identification

Overview

System supports various methods of user identification, which is used to authenticate users who access the Internet via the device.

Web Authentication

After the Web authentication (WebAuth) is configured, when you open a browser to access the Internet, the page will redirect to the WebAuth login page. According to different authentication modes, you need to provide corresponded authentication information. With the successful Web authentication, system will allocate the role for IP address according to the policy configuration, which provides a role-based access control method.

If you use HTTPS request to trigger WebAuth, it only supports unilateral SSL proxy. System will enable the SSL connection during the authentication. After the authentication is completed, SSL proxy will be invalid. The client and server communicate directly without SSL encryption.

In addition, system supports customizing WebAuth page. For more information, refer to Customizing WebAuth Login Pages.

Entering the WebAuth Configuration Mode

To enter the WebAuth configuration mode, in the global configuration mode, use the following command:

webauth

Enabling/Disabling WebAuth

By default, the WebAuth is disabled. To enable the WebAuth function, in the WebAuth configuration mode, use the following commands:

enable

To disable the WebAuth function, in the WebAuth configuration mode, use the following command:

disable

Configuring the WebAuth Mode

The WebAuth includes the following three modes:

- Password Authentication: Using username and password during the Web authentication.
- SMS Authentication: Using SMS during the Web authentication. In the login page, you need to enter the mobile number and the received SMS verification code. If the SMS verification code is correct, you can pass the authentication.
- NTLM Authentication: System obtains the login user information of the local PC terminal automatically , and then verifies the identity of the user.

Web authentication mode can be divided into the single authentication mode and combined authentication mode. OAuth2 authentication can be used together with one of the SMS authentication mode, password authentication mode, and password/SMS authentication mode.



Notes: NTLM authentication mode only supports the Active Directory servers deployed in Windows Server 2008 or older versions.

Configuring the Single Authentication Mode

To configure the single authentication mode, in the WebAuth configuration mode, use the following command:

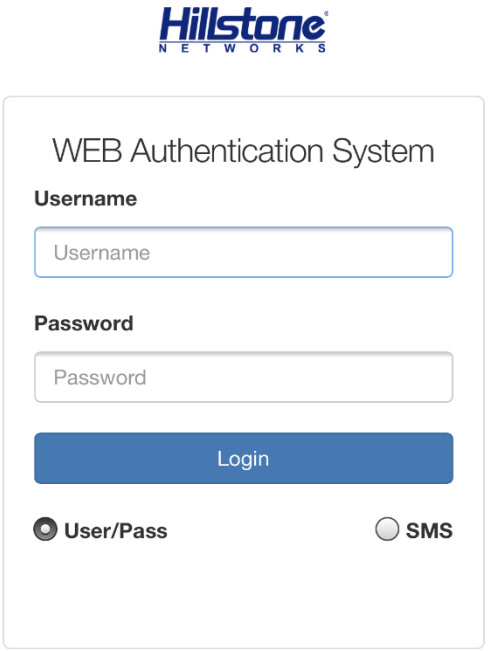
mode { password | sms | ntlm}

- **password** – Specifies the password authentication mode as the authentication mode.
- **sms** – Specifies the SMS authentication mode as the authentication mode.
- **ntlm** – Specifies the NTLM authentication mode as the authentication mode.

Configuring the Combined Authentication Mode

You can specify the combined authentications used in the Web authentication login page, that is, the combined authentication mode.

- System can integrate the password authentication with the SMS authentication, as shown in the figure: Password Authentication or SMS Authentication.



To configure the combined authentication mode, in the WebAuth configuration mode, use the following command:

modepassword-sms

- **password-sms** – Specifies the password authentication or the SMS authentication as the authentication mode in the Web authentication login page.

To restore to the default password authentication mode, in the WebAuth configuration mode, use the following command:

no mode

Configuring the Protocol Type of Authentication

System supports HTTP and HTTPS. HTTP mode is faster, and HTTPS mode is more secure. To configure the protocol type, in the WebAuth configuration mode, use the following command:

protocol {**http** | **https**}

- **http** | **https** – Specifies the protocol type, HTTP or HTTPS.

To restore to the default HTTP protocol type, in the WebAuth configuration mode, use the following command:

no protocol

Specifying the WebAuth Global Default Configuration of Interface

After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. To specify the Webauth global default configuration of the interface, in the WebAuth configuration mode, use the following command:

interface global-default {**enable** | **disable**}

- **enable** – Specifies that the WebAuth function of all interfaces is enabled by default.
- **disable** – Specifies that the WebAuth function of all interfaces is disabled by default .



Tip: For more information about configuring the WebAuth of interface, refer to Enabling/Disabling the WebAuth of Interface.

Configuring the Port Number

To configure the HTTP or HTTPS port number for the authentication server, in the WebAuth configuration mode, use the following commands:

http-port *port-number*

- *port-number* – Specifies the HTTP port number. The value range is 1 to 65535. The default value is 8181.

https-port *port-number*

- *port-number* – Specifies the HTTPS port number. The value range is 1 to 65535. The default value is 44433.

To restore to the default value of the HTTP or HTTPS port number, in the WebAuth configuration mode, use the following commands:

no http-port

no https-port



Notes: HTTP port number and HTTPS port number should be different.

Specifying HTTP Proxy Server Port

After enabling the Web authentication, the device will authenticate the HTTP request whose destination port is 80. When the HTTP traffic of accessing network needs to have a proxy by the HTTP proxy server, you need to specify the HTTP proxy server port in the device. Then, the device can authenticate the HTTP request sent to the proxy server.

To specify the HTTP proxy server port, in the WebAuth configuration mode, use the following command:

proxy-port *port-number*

- *port-number* – Specify the port that the HTTP proxy server used for the HTTP request proxy. The value ranges from 1 to 65535.

Use the **no proxy-port** command to cancel the HTTP proxy server port settings. The device will authenticate the HTTP request whose destination port is 80.

After enabling the Web authentication function and specifying the HTTP proxy server port, each user must add the IP address of the device to the **Exceptions** list in the **Proxy Settings** in the Web browser. With this operation, the Web authentication can be performed.

Configuring the HTTPS Trust Domain

To configure the HTTPS trust domain name, in the WebAuth configuration mode, use the following command:

https-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the HTTPS trust domain. Before executing this command, this new PKI trust domain must have been added into system, and you should make sure that the local certificate purchased from the certificate authority has been imported into it. By default, HTTPS trust domain is trust_domain_default, which will result in the untrusted certificate warning.

To restore to the default HTTPS trust domain trust_domain_default, in the WebAuth configuration mode, use the following command:

no https-trust-domain

Specifying the HTTPS Certificate Chain

The Web authentication function supports to configure an HTTPS certificate chain. After the certificate chain is configured, when Web authentication is triggered by HTTPS traffic, the firewall will send a digital signature of the certificate from the certificate chain to the client. This certificate, along with the root CA certificate installed on the client, forms a complete certificate trust chain. If all the certificates along the trust chain are valid, the browser on the client considers the certificate of the current user valid and trusted, and no "Your connection is not private" warning message will be displayed.

To specify the name of the HTTPS certificate chain, in Web authentication configuration mode, use the following command:

https-cert-chain*cert-chain-name*

- *cert-chain-name* - Specifies the name of the HTPPS certificate chain. This certificate chain is already configured in the system. For more information about how to configure a certificate chain, see Configuring a Certificate Chain.

In Web authentication configuration mode, use the **no https-cert-chain** command to delete a specified certificate chain.

Notes: If an HTTPS certificate chain is specified, take note of the following items:

- The levels of the certificate chain constituted by the firewall and the client needs to be consecutive. For example, for a level-3 certificate chain, if the certificate chains configured on the firewall are level 2 and level 3, the certificate chain installed on the client needs be level 1.
- The client needs to be installed with the root CA certificate of the certificate chain.
- If you have configured an HTTPS trust domain before configuring an HTTPS certificate chain, you need to cancel the configuration of the trust domain first.
- The HTTPS certificate chain has a higher priority than the default trust domain.
- The certificate of the certificate chain configured on the firewall needs to contain the item "User Optional Name", which is the IP address or domain name of the interface that has the Web Authentication function enabled.

Specifying the Address Type

By default, the address type of authentication user is IP address. To specify the address type of authentication user, in the WebAuth configuration mode, use the following command:

address-type {ip | mac}

- **ip** – Specifies IP address as the address type of authentication user.
- **mac** – Specifies MAC address as the address type of authentication user. The device needs to be deployed in the same Layer 2 network environment with the client. Otherwise, system will fail to get the MAC address of the client or get the incorrect MAC address.

To restore to the default address type, in the WebAuth configuration mode, use the following command:

no address-type

Configuring Multi-logon Function

By default, the multi-logon function is disabled. If it is enabled, you can log into multiple clients using the same username simultaneously. To enable the multi-logon function, in the WebAuth configuration mode, use the following command:

multi-logon

After executing this command, the multi-logon function is enabled, and the number of clients using one username is limited. To specify the number of clients, in the WebAuth configuration mode, use the following command:

multi-logon *number*

- *number* – Specifies how many times the same username can be logged in simultaneously. The value range is 2 to 1000 times.

To disable this function, in the WebAuth configuration mode, use the command:

no multi-logon

Configuring Auto-kickout Function

The auto-kickout function means that only one user is allowed to login on one client. When the same user logs in again, according to the configuration, system will kick out the registered user or prevent the same user from logging in again.

Kicking out the registered user, that is, the system will disconnect the original connection and use the new logon information to replace the original logon information. To kick out the registered user, in the WebAuth configuration mode, use the following commands:

auto-kickout

To prevent the same user from logging in again, in the WebAuth configuration mode, use the following commands:

no auto-kickout

Enabling/Disabling Proactive WebAuth

You can enable the proactive WebAuth under L3 interface of device. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.

To enable proactive WebAuth, in the interface configuration mode, use the following command:

webauth aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the configured AAA server.

To disable the proactive WebAuth function, in the interface configuration mode, use the following command:

no webauth aaa-server

Notes:

- When enable proactive WebAuth in L3 interface, you need to ensure that the system's WebAuth function is enabled, otherwise it will not work.
- If the HTTP/HTTPS port of the authentication server is respectively configured as the protocol’s default port 80/443, the port number of the authentication address can be omitted.
- The proactive WebAuth function only supports the mode of password and SMS authentication. If the system is configured with NTLM authentication mode, the proactive WebAuth function will take effect in the mode of password authentication.

Enabling/Disabling the WebAuth of Interface

After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. To enable the WebAuth function of the specified interface, in the interface configuration mode, use the following command:

webauth enable

To disable the WebAuth function of the specified interface, in the interface configuration mode, use the following command:

webauth disable

To specify that the interface uses the global default configuration of WebAuth, in the interface configuration mode, use the following command:

webauth global-default



Tip:

- It is recommended to use the command after the WebAuth is enabled, otherwise the configuration is invalid.
- For more information about WebAuth global default configuration, see Specifying the WebAuth Global Default Configuration of Interface.

Configuring the WebAuth Domain Name

In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name (that is, configure the domain name for the IP address of the interface), the URL of the Web authentication page shows this domain name instead of the IP address of the interface. Enable Web authentication before configuring the WebAuth domain name.

To configure a domain name for the Web authentication address, in the interface configuration mode, use the following command:

webauth domain *domain-name*

- *domain-name* - Specifies the domain name of the Web authentication address. The value range is from 1 to 255 characters.

To delete the domain name configuration of the Web authentication address, in the interface configuration mode, use the following command:

no webauth domain

Disconnecting a User

You can disconnect a specific user from a WebAuth system by CLI. To disconnect a user, in any mode, use the following command:

exec user-mapping webauth kickout {{**ip** *ip-address*| **mac** *mac-address*} **vrouter** *vrouter-name* | **username** *username* { **auth-server** *auth-server-name*}}

- *ip-address* – Specifies the IP address of the WebAuth user.
- *mac-address* – Specifies the MAC address of the WebAuth user.
- *vrouter -name* – Specifies the VRouter of the WebAuth user.
- *username* – Specifies the name of the WebAuth user.
- *auth-server-name* – Specifies the authentication server name of the WebAuth user.



Notes: You need to specify the VRouter or the authentication server to avoid disconnecting too many users with the same name from the WebAuth system.

Allowing Password Change by Local Users

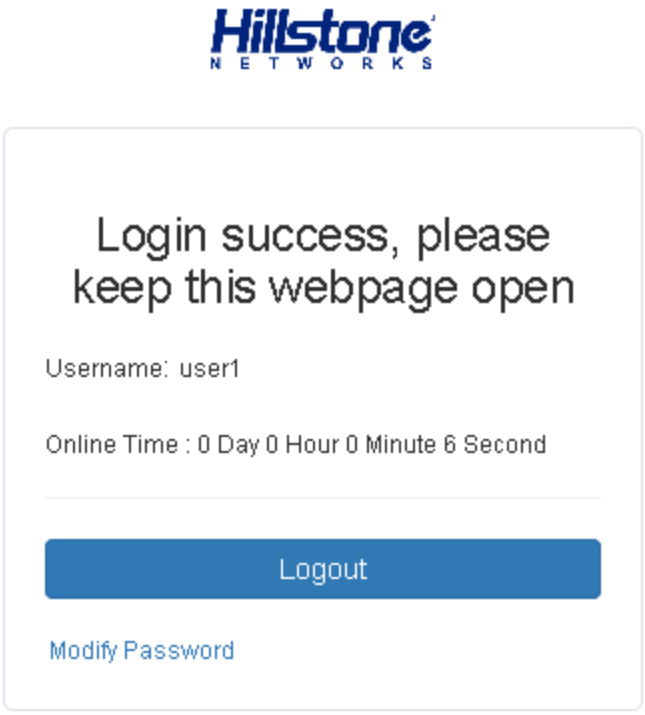
Local users can change their password on the login page after successful authentication. By default, this function is disabled. To enable or disable password change by local users, in the local sever configuration mode, in the password control mode, use the following commands:

- Enable: **allow-pwd-change**
- Disable: **no allow-pwd-change**

To change the login password, local users can take the following steps:

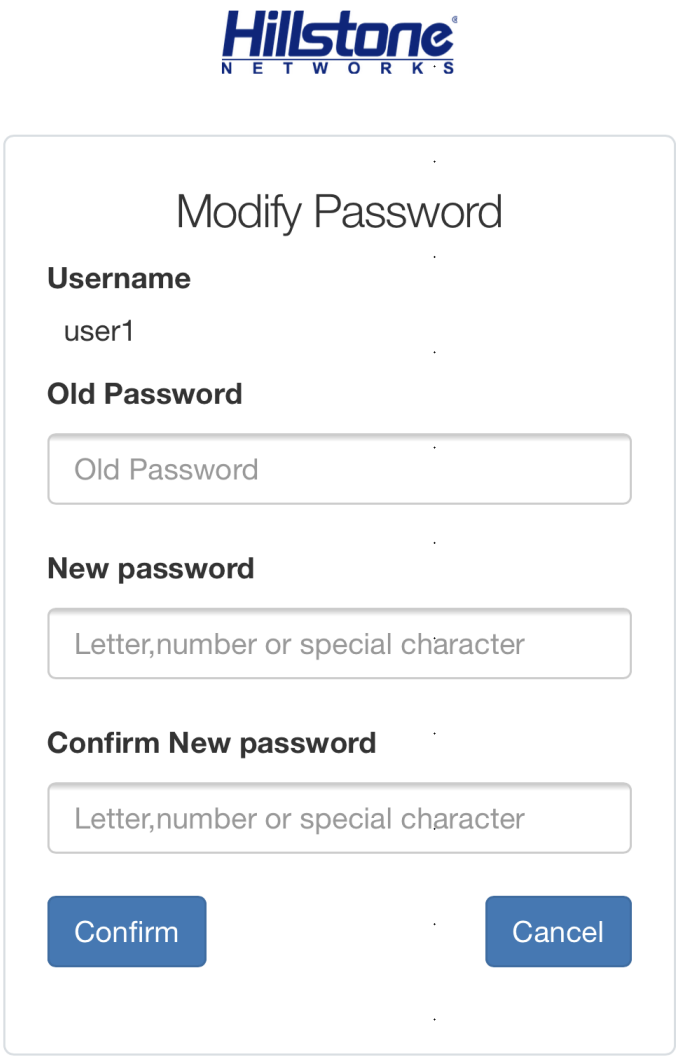
1. Enter the correct username and password on the WebAuth login page, and then click **Login**.

2. After successful login, click **Modify** on the login page. See the figure below:



3. In the password change dialog, type the correct old password into the **Old password** box, type the new password into the **New password** box, and then type the new password again

into the **Confirm New password** box to make confirmation.



4. Click **OK** to save your settings.

Configuring a Policy Rule for WebAuth

You should configure corresponding policy rules to make WebAuth take effect. To configure WebAuth parameters for a policy rule, in the policy rule configuration mode, use the following commands:

Specify the role: **role unknown**

Specify the action and authentication server for WebAuth:

action webauth *aaa-server-name*

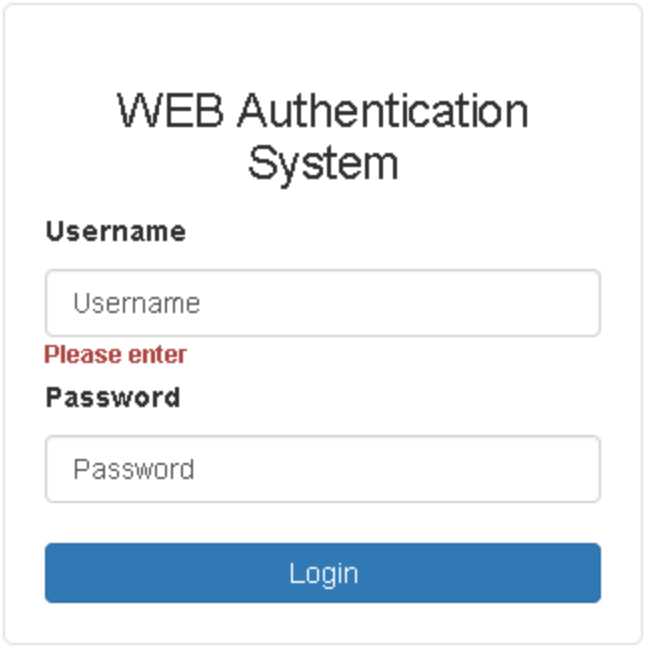
- *aaa-server-name* – Specifies the authentication server which is a configured AAA authentication server in the system.



Tip: For information about how to configure a policy rule, see Policy.

Customizing WebAuth Login Pages

The system supports the customizing WebAuth login page function. After WebAuth is enabled, the default login page is shown as the figure below:



Customizing the Login Page

You can customize the WebAuth login page by downloading the zip file and modifying the contents. To import the modified zip file you need to the system, in the execution mode, use the

following command:

import customize webauth from {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specify to get the zip file from the FTP server, and configure the IP address, VRouter, username and password of the server. If the username and password are not specified, you will login anonymously by default.
- **tftp server** *ip-address* [**vrouter** *vrouter-name*] – Specify to get the zip file from the TFTP server, and configure the IP address and VRouter of the server.
- *file-name* – Specify the name of the zip file.

To restore to the default WebAuth login page, in any mode, use the following command:

exec customize webauth default



Notes:

- After upgrading the previous version to the 5.5R6 version, the WebAuth login page you already specified will be invalid and restored to the default page. You should re-download the template after the version upgrade and customize the login page.
- After upgrading the system version, you should re-download the template, modify the source file, and then upload the custom page compression package. If the uploaded package version is not consistent with the current system version, the function of the custom login page will not be used normally.
- The zip file should comply with the following requirements: the file format should be zip; the maximum number of the file in the zip file is 50; the upper limit of the zip file is 1M; the zip file should contain "index.html".



- System can only save one file of the default template page and the customized page. When you upload the new customized page file, the old file will be covered. It is suggested to back up the old file.
- When you modify the zip file, see "readme_cn.md" file or "readme_en.md" file.

Exporting the Login Page

To export the default modified zip file, in the execution mode, use the following command:

export webauth default-page to {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specify to export the zip file to the FTP server, and configure the IP address, VRouter, username and password of the server. If the username and password are not specified, you will login anonymously by default.
- **tftp server** *ip-address* [**vrouter** *vrouter-name*] – Specify to export the zip file to the TFTP server, and configure the IP address and VRouter of the server.
- *file-name* – Specify the name of the zip file.

Password Authentication

To enable password authentication, in the WebAuth configuration mode, use the following command:

mode password

Configuring the Re-auth Interval

System can re-authenticate a user after a successful authentication. By default, the re-authentication function is inactive. To configure the re-authenticate interval, in the WebAuth

configuration mode, use the following command:

password reauth-interval {*time* | **disable**}

- *time* – Specifies the interval to re-authenticate a user. The value range is 10 to 60*24 minutes.
- **disable** – Disables the re-auth function.

To restore to the default value, in the global configuration mode, use the command:

no password reauth-interval

Configuring the Redirect URL Function

The redirect URL function redirects the client to the specified URL after successful authentication. You need to turn off the pop-up blocker of your web browser to ensure this function can work properly. To configure the redirect URL function, in the WebAuth configuration mode, use the following command:

password popup-url *url*

- *url* – Specifies the redirect URL. The length is 1 to 127 characters. The format of URL should be "http://www.abc.com" or "https://www.abc.com".

To delete the redirect URL configuration, in the WebAuth configuration mode, use the command:

no password popup-url



Notes:

- You can specify the username and password in the URL address. When the specified redirect URL is the application system page with the authentication needed in the intranet, you do not need the repeat authentication and can access the application system.



- The corresponding keywords are $USER, $PWD, or $HASHPWD. Generally, you can select one keyword between $PWD and $HASHPWD. The formart of the URL is “URL”+”username=$USER&password=$PWD”.
- When entering the redirect URL in CLI, add double quotations to the URL address if the URL address contains question mark. For example, “http://192.10.5.201/oa/-login.do?username=$USER&password=$HASHPWD”

Configuring the Forced Timeout Value

If the forced timeout function is enabled, users must re-login after the configured interval ends. By default, the forced re-login function is disabled. To configure the forced timeout value, in the WebAuth configuration mode, use the following command:

password force-timeout {*timeout-value* | **disable**}

- *timeout-value* - Specifies the forced timeout value. The value range is 10 to 60*24*100 minutes.
- **disable** – Disables the forced timeout function, that is , system does not force the user to login again.

To restore to the default value, in the WebAuth configuration mode, use the command:

no password force-timeout

Configuring the Idle Timeout Value

If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, the system will not disconnect the connection if there is no traffic after the successful authentication. To specify the idle timeout value, namely the idle time, use the following command in the WebAuth configuration mode:

password idle-timeout {*timeout* | **disable**}

- *timeout* – Specifies the idle timeout value (in minutes). The value range is 1 to 60*24 minutes.
- **disable** – Disables the idle timeout function, which indicates that system will not disconnect the connection if there is no traffic after the successful authentication.

To restore to the default value, in the WebAuth configuration mode, use the following command:

no password idle-timeout



Notes:

- If you pass the web authentication by using the mobile phones running on iOS or Android, enable this function and specify the idle time. Then the mobile phones can keep online when they generate traffic.
- SG6000-K9180/K6580 and X series devices do not support the configuration of idle time.

Configuring the Heartbeat Timeout Value

When authentication is successful, the system will automatically refresh the login page before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time,you will log off from the system at the smaller value.To configure the heartbeat timeout value, in the WebAuth configuration mode, use the following command:

password heartbeat-timeout {*interval* | **disable**}

- *interval* – Specifies the heartbeat timeout value. The value range is 1 to 60*24*100 minutes. The default value is 10 minutes.
- **disable** – Disables the heartbeat timeout function.

To restore to the default heartbeat timeout value, in the global configuration mode, use the command:

no password heartbeat-timeout

SMS Authentication

Besides using username and password during the Web authentication, the system support SMS authentication method. After enabling the SMS authentication function, the HTTP request will be redirected to the Web authentication login page. In the login page, the user needs to enter the mobile phone number and the received SMS code. If the SMS code is correct, the user can pass the authentication.

To enable SMS authentication, in the WebAuth configuration mode, use the following command:

mode sms

Configuring the Forced Timeout Value

After passing the SMS authentication successfully, the user will be re-authenticated after the timeout value reaches. To configure the timeout value, in the WebAuth configuration mode, use the following command:

sms force-timeout {*timeout-value* | **disable**}

- *timeout-value* – Specifies the forced timeout value. The value range is 10 to 60*24*100 minutes. The default value is 60 minutes.
- **disable** – Disables the forced timeout function, that is , system does not force the user to authenticate again.

To restore to the default value, in the WebAuth configuration mode, use the command:

no sms force-timeout

Configuring the Idle Timeout Value

If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, system will not disconnect the connection if there is no traffic after the successful authentication. To specify the idle timeout value, in the WebAuth configuration mode, use the following command:

sms idle-timeout {*timeout* | **disable**}

- *timeout* – Specifies the idle timeout value (in minutes). The value range is 1 to 60*24 minutes.
- **disable** – Disables the idle timeout function, which indicates that system will not disconnect the connection if there is no traffic after the successful authentication.

To restore to the default value, in the WebAuth configuration mode, use the following command:

no sms idle-timeout

Configuring the Verification Code Interval

When using SMS authentication, users need to use the SMS verification code received by the mobile phone, and the verification code will be invalid after the timeout value reaches. After the timeout value reaches, if the verification code is not used, you needs to get the new SMS verification code again, in the global configuration mode, use the following command:

webauth sms-verify-code-timeout*timeout-value*

- *timeout-value* – Specifies the verification code interval, the range is 1 to 10 minutes. The default value is 1 minute.

In the global configuration mode, use the following command to restore the timeout value to the default one.

no webauth sms-verify-code-timeout

Specifying the Sender Name or Sign Name

If the protocol type of the SMS Gateway is SGIP or USM , users can specify a message sender name to display in the message content. If the protocol type of the SMS Gateway is ALIYUNSMS, the sign name must be entered in this field and will be displayed in the message content, users must specify the sign name applied in the SMS of Alibaba Cloud to display in the message content. To specify the sender name or sign name, in the WebAuth configuration mode, use the following command:

webauth sms-sender-name*sender-name*

- *sender-name* – Specifies the sender name or sign name. The range is 1 to 63.

In the WebAuth configuration mode, use the following command to delete the sender name or sign name:

no webauth sms-sender-name



Notes: Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.

Configuring the Verification Code Length

To specify the length of the SMS verification code, in the WebAuth configuration mode, use the following command:

sms verification-code-length *length*

- *length* - Specifies the length of the SMS verification code. The range is 4 to 8 characters. The default value is 6.

In the WebAuth configuration mode, use the **no sms verification-code-length** command to restore the default value.

Specifying the Template Code

If the protocol type of the SMS Gateway is ALIYUNSMS, users must specify the code of the SMS template applied in the SMS of Alibaba Cloud. To specify the template code, in the WebAuth configuration mode, use the following command:

sms templatecode *word*

- *word* – Specifies the template code. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.

In the WebAuth configuration mode, use the following command to cancel the specified template code:

no sms templatecode

Specifying SMS Modem to Send SMS

To specify SMS modem to send SMS, in the WebAuth configuration mode, use the following command:

sms agent modem

Specifying SMS Gateway to Send SMS

To specify SMS gateway to send SMS, in the WebAuth configuration mode, use the following command:

sms agent gateway *sp-name*

- *sp-name* – Specifies the SP instance name which should be a created SP. The range is 1 to 31.

NTLM Authentication

To enable NTLM, in the WebAuth configuration mode, use the following command:

mode ntlm



Notes:

- For IE, you need to enable automatic logon with current username and password in order to complete the WebAuth automatically.
- For non-IE browsers, you need to type the username and password in the prompt each time you try to access network resources.

Configuring Forced Timeout Value

Authentication will only take effect within a limited time range after you have been authenticated by the Active Directory server; after timeout, you still need to type valid username and password in the WebAuth page to continue to access network resources. To configure the timeout, in the WebAuth configuration mode, use the following command:

ntlm force-timeout {*timeout-value* | **disable**}

- *timeout-value* - Specifies the forced timeout value. The value range is 10 to 60*24*100 minutes.
- **disable** – Disables the forced timeout function, that is , system does not force the user to login again.

To restore to the default value, in the WebAuth configuration mode, use the command:

no ntlm force-timeout

Using the Compatibility Mode

Since the NTLM function only supports users using Windows OS, you can use the compatibility mode to ensure that all users using different OSs can execute the authentication. The compatibility mode will use the password WebAuth when the following situation appears: you have enabled the NTLM function and users fail in the authentication. By default, the system will not take any action if users fail in the authentication. To use the compatibility mode, use the following command in the WebAuth configuration mode:

ntlm fallback-to-webform

To restore to the defaut value, in the WebAuth configuration mode, use the following command:

no ntlm fallback-to-webform

Configuring the Idle Timeout Value

If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, system will not disconnect the connection if there is no traffic after the successful authentication. To specify the idle timeout value, use the following command in the WebAuth configuration mode:

ntlm idle-timeout {*timeout* | **disable**}

- *timeout* – Specifies the idle timeout value (in minutes). The value ranges from 1 to 60*24 minutes.

- **disable** – Disables the idle timeout function, which indicates that system will not disconnect the connection if there is no traffic after the successful authentication.

To restore to the defaut value, in the WebAuth configuration mode, use the following command:

no ntlm idle-timeout

OAuth2 Authentication

The system can implement Web authentication by using OAuth2 authentication. After the OAuth2 authentication function is configured, when you open a browser to access the Internet, the page will be redirected to the WebAuth login page. You need to click the OAuth2 authentication icon on the login page of Web authentication to go to the login page of the OAuth2 server. After you enter the username and password for the OAuth2 server, you can pass the authentication.

Enabling/Disabling the OAuth2 Authentication Mode

By default, OAuth2 authentication is disabled. To enable/disable the OAuth2 authentication mode, in Web authentication configuration mode, use the following command:

oauth {**enable** | **disable**}

- **enable** – Enable OAuth2 authentication.
- **disable** – Disable OAuth2 authentication.

Binding the OAuth2 Server

After you enable OAuth2 authentication, you need to bind the OAuth2 server at the same time so that the OAuth2 authentication can take effect. To do this, in Web authentication configuration mode, use the following command:

oauth server*aaa-server-name*

- *aaa-server-name* – Specifies the OAuth2 server to be bound.

To delete the OAuth2 server, in Web authentication configuration mode, use the following command:

no oauth server*aaa-server-name*

Configuring the Forced Timeout Period of OAuth2 Authentication

The system can force users to log on again after a period of time. By default, this function is disabled. To configure the forced timeout period of OAuth2 authentication, in Web authentication configuration mode, use the following command:

oauth force-timeout {*timeout-value* | **disable**}

- *timeout-value* – Specifies the forced timeout period. Valid values: 10 to 60*24*100. Unit: minutes.
- **disable** – Disable the forced timeout period function. In other words, the system does not force users to log on again.

To restore the timeout period to defaults, in Web authentication configuration mode, use the following command:

no oauth force-timeout

Configuring the Heartbeat Timeout Period of OAuth2 Authentication

After successful authentication, the system will automatically refresh the Authentication Success page before the timeout period expires to confirm the login information. If both the idle timeout period and heartbeat timeout period are configured, the users will be disconnected at the earlier of the two timeout values. To configure the heartbeat timeout period of OAuth2 authentication, in Web authentication configuration mode, use the following command:

oauth heartbeat-timeout {*timeout-value* | **disable**}

- *timeout-value* – Specifies the heartbeat timeout period. Valid values: 1 to 60*24. Default value: 10. Unit: minutes.
- **disable** – Disable the heartbeat timeout period function.

To restore the timeout period to defaults, in Web authentication configuration mode, use the following command:

no oauth heartbeat-timeout

Configuring the Idle Timeout Period of OAuth2 Authentication

The idle timeout period indicates the maximum time that the Authentication Success page can remain connected in an idle state. Once the idle timeout is exceeded, the connection is closed. By default, the Authentication Success page can remain connected in an idle state. To configure the OAuth2 authentication idle timeout period, in Web authentication configuration mode, use the following command:

oauth idle-timeout {*timeout* | **disable**}

- *timeout* – Specifies the idle timeout period. Valid values: 1 to 60*24. Unit: minutes.
- **disable** – Disable the idle timeout period function. In other words, the Authentication Success page can remain connected in an idle state. This is the default setting.

To restore the timeout period to defaults, in Web authentication configuration mode, use the following command:

no oauth idle-timeout

Viewing the WebAuth Configuration Information

To view the current WebAuth configuration information, in any mode, use the following command:

show webauth

To view all the WebAuth configuration information, in any mode, use the following command:

show webauth detail

Viewing the Online User Information

To view the online WebAuth user information, in any mode, use the following commands:

show auth-user {**webauth-ntlm** | **webauth-password** | **webauth-sms** | **webauth-oauth**}[**inter-face***interface-name* | **vrouter***vrouter-name*]

show user-mapping webauth [**ip** *ip-address* | **mac** *mac-address*] [**vrouter** *vrouter-name*]

Single Sign-On

When the user authenticates successfully for one time, system will obtain the user's authentication information. Then the user can access the Internet without authentication later.

SSO can be realized through multiple methods, which are independent from each other, and they all can achieve the "no-sign-on"(don't need to enter user name and password) authentication.

Configuring AD Scripting for SSO

With the Single Sign-on (SSO) agent function enabled, users will automatic pass the authentication after they pass the Active-Directory authentication.

To use the AD Scripting function, you should firstly add the script program named Loginscript.exe, which is provided by Hillstone, to the logon/logout script of the Active-Directory server.



Notes: For the information of how to add the script program "Loginscript.exe" into the Active-Directory server, refer to Example of Configuring AD Agent for SSO.

Entering the AD Scripting Configuration Mode

To enter the AD-Scripting configuration mode, use the following command in the global configuration mode:

user-sso server ad-scripting default

Enabling the AD Scripting Function

By default, the AD Scripting function is disabled. To enable this function, use the following command in the AD-Scripting configuration mode:

enable

To disable the function, use the following command:

no enable

Specifying the AAA Server

To specify the AAA server referenced by system, use the following command in the sso-agent configuration mode:

aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. The Local, AD or LDAP server is available to select on the AAA server. You're suggested to directly select the configured authentication AD server. After selecting the AAA server, system can query the corresponding user group and role of the online user on the referenced AAA server, so as to achieve the policy control based on the user group and role.

To cancel the above configurations, use the following command in the AD-Scripting configuration mode:

no aaa-server

Configuring the Idle Time

If there is no traffic during a specified time period after the successful authentication, system will delete the user authentication information. To specify the time period, namely the idle time, use the following command in the AD Scripting configuration mode:

idle-timeout *timeout*

- *timeout* – Specifies the idle time (in minutes). The value ranges from 1 to 1440.

By default, system will not delete the user authentication information if there is no traffic. To restore the idle time to the default value, use the following command in the global configuration mode:

no idle-timeout



Notes: SG6000-K9180/K6580 and X series devices do not support the configuration of idle time. .

Configuring Simultaneously Online Settings

By default, if a user logs on again after hi or her successful logon, the system will disconnect the original connection and use the new logon information to replace the original logon information. Thus, users with the same credentials cannot be online simultaneously. If you want users with the same credentials to be online simultaneously, you can use the following commands in the AD-Scripting configuration mode:

no auto-kickout

To restore the settings to the default, use the following command in the AD-Scripting configuration mode:

auto-kickout

Viewing Configuration Information

To view the configuration information of the AD Scripting function, use the following command in any mode:

show user-sso server ad-scripting default

Viewing the User Mapping Information

To view the mapping information between user name and IP of AD Scripting, in any mode, use the following command:

show user-mapping user-sso ad-scripting default

Viewing the Authenticated User Table

The user authentication information are stored in the authenticated user table. To view the user authentication information, use the following command in any mode:

show auth-user ad-scripting

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso ad-scripting kickout ip *ip-address* **vrouter** *vrouter-name*

Configuring SSO Radius for SSO

Receiving Radius Accounting Packets

The device can receive the accounting packets that based on the Radius standard protocol, and then perform the following actions according to the content of the packets:

- Generate user authentication information and add them to the authenticated user table.
- Reset the timeout value of the authenticated user.
- Delete the authenticated user from the table.

To enable the function above, take the following steps:

To enter the SSO-Radius configuration mode, in the global configuration mode, use the following command:

user-sso server sso-radius default

In the SSO-Radius configuration mode, use the following command:

enable

To disable the function, in the SSO-Radius configuration mode, use the following command:

no enable

Note: After enabling SSO Radius, you should wait at least 5 seconds before disabling it, and vice versa. During workload peaks, the waiting time may be extended.

Specifying the AAA Server

Specify the AAA server that user belongs to. To specify the AAA server, in the SSO-Radius configuration mode, use the following command:

aaa-server *aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. You can select Local, AD or LDAP server on the AAA server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

To delete the AAA server, in the SSO-Radius configuration mode, use the following command:

no aaa-server

Specifying the Port Number for Receiving Radius Packets

To specify the port number for receiving Radius packets (Don't configure port in non-root VSYS), in the SSO-Radius configuration mode, use the following command:

port *port*

- *port* – Specifies the port number. The range is 1 to 65535. The default port is 1813.

Use the **no port** command to restore the port number to default.

Configuring the Radius Client

Specify the IP address of the Radius client. You can specify up to 8 clients. To specify the IP address of the Radius clients and enter the Radius client configuration mode, in the SSO-Radius configuration mode, use the following command:

client {**any** | *A.B.C.D* | *X:X:X:X::X*}

- **any** – Receive the packets sent from any Radius client.
- *A.B.C.D* – Receive the packets sent from the Radius Client with specified IP address.
- *X:X:X:X::X* – Receive the packets sent from the Radius client with specified IPv6 address. This specification is valid only when the system version is the IPv6 version.

To delete the configured Radius client, in the global configuration mode, use the **no client** {**any** | *A.B.C.D*| *X:X:X:X::X*} command.

Configuring the Shared Secret

System will verify the packet by the shared secret key, and parse the packet after verifying successfully. If system fails to verify the packet, the packet will be dropped. The packet can be verified successfully only when SSO Radius client is configured the same shared secret key with system or both of them aren't configured a shared secret key.. To configure the shared secret key, in the Radius client configuration mode, use the following command:

shared-secret *key-value*

- *key-value* – Specifies the shared secret key. The length range is from 1 to 31 characters.

To delete the shared secret key, use the **no shared-secret** command.

Configuring the Heartbeat Timeout

Heartbeat timeout is used to configure the effective time for user authentication information of Radius packets in the device. If there's no update or delete packet of the user during the heartbeat timeout, the device will delete the user authentication information.

To configure the heartbeat timeout, in the Radius client configuration mode, use the following command:

heartbeat-timeout*timeout*

- *timeout* – Specifies the timeout value. The unit is minute. The range is from 0-1440. The default value is 30. 0 means it will never timeout.

To restore the heartbeat timeout to default, in the Radius client configuration mode, use the **no heartbeat-timeout** command.

To disable the heartbeat timeout, in the Radius client configuration mode, use the **heartbeat-timeout disable** command.

Configuring Idle Timeout

Idle timeout refers to the longest time during which the authenticated user keeps his/her authenticated state in non-traffic state. When the configured idle timeout is exceeded, system will delete the authentication information of the user.

To specify the idle timeout, in the SSO Radius client mode, use the following command:

idle-timeout *time*

- *time* – Specify the idle timeout. The unit is minute. The range is from 0-1440. The default value is 0. If it is specified as 0, this function will be disabled, which means the authenticated user will not be kicked out in non-traffic state.

To restore the idle timeout to the default value, in the SSO Radius client mode, use the **no idle-timeout**command.

To disable the idle timeout, in the SSO Radius client mode, use the **idle-timeout disable**command.

Configuring Forced Timeout

When the online time of a user exceeds the configured force timeout time, system will force the user to log out.

To specify the forced timeout, in the SSO Radius client mode, use the following command:

force-timeout *time*

- *time* - Specify the forced timeout time. The range is 0 to 144000 minutes, and the default value is 600 minutes. If it is specified as 0, this function will be disabled.

To restore the forced timeout to the default value, in the SSO Radius client mode, use the **no force-timeout**command.

To disable the forced timeout, in the SSO Radius client mode, use the **force-timeout disable**command.

Viewing the SSO Radius Configuration Information

To view the SSO Radius configuration information, in any mode, use the following command:

show user-sso server sso-radius default

Viewing the User Mapping Information

To view the mapping information between the user name and IP of SSO Radius, in any mode, use the following command:

show user-mapping user-sso sso-radius default

Viewing the Authentication User Table

The user authentication information generated by the device is saved in the authentication user table. In any mode, use the following command:

show auth-user sso-radius

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso sso-radius kickout ip *ip-address* **vrouter** *vrouter-name*

SSO via Agile Controller

When Agile Controller is enabled, the system can receive packets sent by the Agile Controller server. The packets are sent when users log in to or log out of the server or when users update their information. To realize SSO, the system obtains user authentication information, updates online user information, and manages the user's login and logout according to the packets.

Entering the Agile Controller Configuration Mode

To enter the Agile Controller configuration mode, in the global configuration mode, use the following command:

user-sso server agile-controller default

Enabling/Disabling Agile Controller

By default, Agile Controller is disabled. To enable or disable Agile Controller, in the Agile Controller configuration mode, use the following command:

- To enable: **enable**
- To disable: **no enable**

Specifying the Port for StoneOS to Receive Agile Controller Packets

To specify the port for StoneOS to receive packets from the Agile Controller server (Port cannot be configured in non-root VSYS), in the Agile Controller configuration mode, use the following command:

local-port *port*

- *port* - Specifies the port number. The range is 1024 to 65535. The default port number is 8001.

In the Agile Controller configuration mode, use **no local-port** command to restore to the default port.

Specifying the AAA Server

Specify the AAA Server that the user belongs to. To specify the AAA server, in the Agile Controller configuration mode, use the following command:

aaa-server *aaa-server-name*

- *aaa-server-name* - Specifies the name of the AAA server. You can select the configured Local, AD, or LDAP server. After selecting the AAA server, the system can query the user group and role information associated with the username of the online user on the referenced AAA server, to realize the policy control based on the user group and role.

In the Agile Controller configuration mode, use **no aaa-server** command to cancel the specified AAA server.

Specifying Query Address Range

To specify the address range of the source IP to be queried when the system actively queries the information of the online user associated with the source IP from the Agile Controller server, in the Agile Controller configuration mode, use the following command:

sync-address *address-entry*

- *address-entry* - Specifies the address range of the source IP (the configured address entry) to be queried.

In the Agile Controller configuration mode, use the **no sync-address** command to cancel the specified query address range of the source IP.

Specifying the Query Rate

To specify the query rate when the system actively queries the information of the online user associated with the source IP from the Agile Controller server, in the Agile Controller configuration mode, use the following command:

sync-rate *number*

- *number* - Specifies the rate at which query packets are sent. The range is 5-40 times/second.

In the Agile Controller configuration mode, use **no sync-rate** command to restore to the default query rate.

Specifying the Query Interval

To specify the query interval when the system actively queries the information of the online user associated with the source IP from the Agile Controller server, in the Agile Controller configuration mode, use the following command:

ip-sync-interval *time*

- *time* - Specifies the query interval between each source IP. The range is 1-100 seconds. The default value is 20 seconds

In the Agile Controller configuration mode, use **no ip-sync-interval** command to restore to the default query interval.

Specifying the Maximum IPs Queried Each Time

To specify the maximum source IPs contained in a query packet when the system actively queries the information of the online user associated with the source IP from the Agile Controller server, in the Agile Controller configuration mode, use the following command:

max-ip-per-packet *number*

- *number* - Specifies the maximum source IPs contained in a query packet. The range is 1-50. The default value is 50.

In the Agile Controller configuration mode, use **no max-ip-per-packet** command to restore to the default value.

Specifying Forced Timeout

To specify the timeout after which access for the authenticated user is forcibly terminated, in the Agile Controller configuration mode, use the following command:

force-timeout *time*

- *time* - Specifies the timeout. The range is 5 to 1440 minutes. The default timeout is 600 minutes.

In the Agile Controller configuration mode, use **no force-timeout** command to restore to the default timeout.

Configuring an Agile Controller Client

To configure an Agile Controller client, you need to enter the configuration mode of the Agile Controller client. In the Agile Controller configuration mode, use the following command:

access-agile-controller *name*

- *name* - Specifies the name of the Agile Controller server.

In the Agile Controller configuration mode, use the **no access-agile-controller***name* command to cancel the specified Agile Controller client.

Specifying the IP Address of the Agile Controller Server

To specify the IP address of the Agile Controller server, in the configuration mode of the Agile Controller client, use the following command:

host *ip-address* [**vrouter** *vr-name*]

- *ip-address* - Specifies the IP address of the Agile Controller server.
- **vrouter** *vr-name* - Specifies the virtual router that the specified Agile Controller server belongs to. If the VRouter is not specified, the system uses trust-vr by default.

In the configuration mode of the Agile Controller client, use the **no host** command to cancel the specified IP address of the Agile Controller server.

Configuring the Shared Key

The system verifies the encrypted communication packets sent by the Agile Controller server by using the shared key. The system parses the packets only when the verification is successful. Otherwise, the system drops the packets. The Agile Controller client should be configured with the same shared key as the Agile Controller server. Otherwise, the packets cannot be successfully verified. To configure the shared key, in the configuration mode of the Agile Controller client, use the following command:

shared-secret *key-value*

- *key-value* - Specifies the shared key. The range is 1-31 characters.

To clear the shared key, in the configuration mode of the Agile Controller client, use the **no shared-secret** command.

Configuring the Encryption Algorithm

To specify the encryption algorithm applied in the communication between the system and the Agile Controller server, in the configuration mode of the Agile Controller client, use the following command:

encryption [*3des* | *aes128*]

- *3des* | *aes128* - Specifies the encryption algorithm applied in the communication between the system and the Agile Controller server. If this option is not specified, the system uses the AES128 algorithm by default.

In the configuration mode of the Agile Controller client, use the **no encryption** command to restore to the default encryption algorithm.

Enabling/Disabling Active Query

When Active Query is enabled, the system will actively query the information of the online users from the Agile Controller server. By default, Active Query is disabled. To enable or disable Active Query, in the configuration mode of the Agile Controller client, use the following command:

- To enable: **sync enable**
- To disable: **no sync enable**

Displaying Configuration Information of the Agile Controller

To display configuration information of the Agile Controller, in any mode, use the following command:

show user-sso server agile-controller default

Configuring AD Polling for SSO

Creating an AD Polling Profile

To create an AD Polling profile and enter the AD-Polling configuration mode, in the global configuration mode, use the following command:

user-sso client ad-polling *profile-name*

- *profile-name* - Specifies the name of the AD Polling profile to be created. After executing the command, system will create an AD Polling profile with the specified name and enter the AD Polling configuration mode; if the specified name has existed, system will enter the AD Polling configuration mode directly.

To delete the specified AD Polling profile, in the global configuration mode, use the following command:

no user-sso client ad-polling *name*

Enabling / Disabling the AD Polling Function

After enabling the AD Polling function, the system will regularly query the AD server to obtain the online user information and probe the terminal PCs to verify whether the users are still online. To enable the AD Polling function, in the AD-Polling configuration mode, use the following command:

enable

To disable the AD Polling function, in the AD-Polling configuration mode, use the following command:

no enable

Specifying the Authentication Server

To specify the authentication AD server in the domain, in the AD-Polling configuration mode, use the following command:

host *ip-address*

- *ip-address* - Specifies the IP address of the authentication AD server in the domain.You can only specify AD server. After specifying the authentication AD server, when the domain user logs in the AD server, the AD server will generate on the server. The length is 1 to 31 characters.

To delete the authentication servers in the domain, in the AD-Polling configuration mode, use the following command:

no host

Specifying the AAA Server

To specify the AAA server referenced by system, in the AD-Polling configuration mode, use the following command:

aaa-server *server-name*

- *server-name* - Specifies the name of the referenced AAA server. The Local, AD or LDAP server is available to select on the AAA server. You’ re suggested to directly select the

configured authentication AD server. After selecting the AAA server, system can query the corresponding user group and role of the online user on the referenced AAA server, so as to achieve the policy control based on the user group and role.

To delete the AAA server, in the AD-Polling configuration mode, use the following command:

no aaa-server

Specifying the Account

To specify the nameof domain user to log in the AD server, in the AD-Polling configuration mode, use the following command:

account *username*

- *username* – Specifies the name of domain user to log in the AD server. The format is domain\username, and the range is 1 to 63 characters. The user is required to have permission to read security log on the AD server, such as the user Administrator whose privilege is Domain Admins on the AD server.

To delete the account, in the AD-Polling configuration mode, use the following command:

no account

Specifying the Password

To specify the password corresponding to the domain user name, in the AD-Polling configuration mode, use the following command:

password *password*

- *password* - Specifies the password corresponding to the user name. The range is 1 to 31 characters.

To delete the password, in the AD-Polling configuration mode, use the following command:

no password

Specifying the AD Polling Interval

To specify the time interval for regular AD Polling probing, in the AD-Polling configuration mode, use the following command:

ad-polling-interval *interval*

- *interval* - Specifies the time interval for regular AD Polling probing. System will query the AD server to obtain the online user information at the interval. The range is 1 to 3600 seconds, the default value is 2 seconds. You are suggested to configure 2 to 5 seconds to ensure to get the online user information in real time.

To restore the configured time interval for regular AD Polling probing to default, in the AD-Polling configuration mode, use the following command:

no ad-polling-interval

Specifying the Client Probing Interval

To specify the time interval for the regular client probing, in the AD-Polling configuration mode, use the following command:

client-probing-interval *time*

- *time* – Specifies the time interval for the regular client probing. System will probe whether the online user is still online through WMI at set intervals, and system will kick out the user if cannot be probed. The range is 0 to 1440 minutes, and the default value is 0 minute(the function is disabled). You are suggested to configure a larger probing interval to save the system performance, if you have low requirements of the offline users.

To restore the configured client probing interval to default, in the AD-Polling configuration mode, use the following command:

no client-probing-interval

Specifying the Force Timeout Time

To specify the forced logout time, in the AD-Polling configuration mode, use the following command:

force-timeout *time*

- *time* - Specified the forced logout time. When the online time of a user exceeds the configured force timeout time, system will kick out the user and force the user to log out. The range is 0 (the function is disabled) to 144000 minutes, and the default value is 600 minutes.

To restore the configured force timeout time to default, in the AD-Polling configuration mode, use the following command:

no force-timeout

Viewing the AD Polling Configuration

To view the AD Polling configuration owned or specified by system, including the name, status, AAA server, client probing interval, etc., in any mode, use the following command:

show user-sso client ad-polling [*profile-name*]

- *profile-name* – Specifes the name of the AD Polling profile. Here shows the configuration information of specified AD Polling.

Viewing the User Mapping Information

To view the mapping information between user name and IP of SSO Monitor, in any mode, use the following command:

show user-mapping user-sso ad-polling *profile-name*

Viewing the Authenticated User Table

The user authentication information are stored in the authenticated user table. To view the user authentication information, use the following command in any mode:

show auth-user ad-polling

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso ad-polling kickout ip *ip-address* **vrouter** *vrouter-name*

Configuring SSO Monitor for SSO

SSO Monitor can synchronize the online status of users stored on external servers to the firewall based on specified protocol packets, generate authenticated users on the firewall, and update the username-IP (IPv4 or IPv6 address) binding relationship of online users in real time. In addition, SSO Monitor can extract the user group of users from packets so that the users can avoid repetitive login process.

StoneOS does not restrict the form and type of external servers. A server of TCP connection that can synchronize user information to the firewall over the SSO Monitor protocol can be used as an external server, such as AD Agent software.



Notes: To use AD Agent software to obtain user information in version earlier than StoneOS 5.5R10, you can connect the AD agent by using SSO Monitor or configure the security agent in Active-Directory server configuration mode. In StoneOS 5.5R10 and later, the system no longer supports the security agent function. When the version is upgraded to StoneOS 5.5R10 or later, the configured security agent function is automatically converted to the SSO Monitor function to connect to the AD Agent software configuration. You can run the **show user-sso client sso-monitor**[*profile-name*] command to view the configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

Creating SSO Monitor Profile

To create SSO Monitor profile and enter the SSO-Monitor configuration mode, in the global configuration mode, use the following command:

user-sso client sso-monitor *profile-name*

- *profile-name* - Specifies a name of the SSO Monitor profile to be created. After executing the command, system will create the SSO Monitor profile with the specified name and enter SSO-Monitor configuration mode; if the profile with the specified name has existed, system will enter the SSO-Monitor configuration mode directly.

To delete the specified SSO Monitor profile, in the global configuration model, use the following command:

no user-sso client sso-monitor *name*

Enabling/Disabling the SSO Monitor Function

After enabling SSO Monitor, the system establishes a connection with the external server over the SSO-Monitor protocol and obtains the online status of users and information about the user group of the users (optional). The system will also update the username-IP mapping information of online users in real time. To enable SSO Monitor function, in the SSO-Monitor configuration mode, use the following command:

enable

To disable SSO Monitor function, in the SSO-Monitor configuration mode, use the following command:

no enable

Configuring User Address

Users can be related to configured address book. When generating authentication users, the system only generate users within the specified IP range. To specify user address, in the SSO-Monitor configuration mode, use the following command:

user-address*address-entry*

address-entry - Specifies the name of the configured address entry in the address book.

To delete related address book entry, in the SSO-Monitor configuration mode, use the command **no user-address**.

Specifying the External Server

The external server needs to be able to send the online status of users to the firewall based on SSO-Monitor protocol packets. You need to configure at least one external server host1, host2, or host3. If you configure more than one external server, other external servers except the first one are used for redundant backup. When an address fails to be connected, the system attempts to connect to another external server. We recommend that you configure host1, host2, and host3 in sequence.

To specify the external server, run the following commands in SSO-Monitor configuration mode:

host1 {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter** *vrouter-name*]

host2 {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter** *vrouter-name*]

host3 {*ipv4-address* | *ipv6-address* | *host-name*} [**vrouter** *vrouter-name*]

- *ipv4-address* | *ipv6-address* | *host-name* - Specifies the IPv4 address, IPv6 address, or domain name of the external server, which can be 1 to 255 characters in length.
- *vrouter-name* - Specifies the name of the virtual router to which the communication interface between the firewall and external server belongs.

In SSO-Monitor configuration mode, run the following command to delete a specified external server:

no host {1 | 2 | 3}



Notes: In StoneOS 5.5R10 and later, SSO Monitor can connect to multiple external servers to implement redundant backup. Therefore, the configured "**host x.x.x.x**" of SSO Monitor will be automatically converted to "**host1 x.x.x.x**" after the system is upgraded to StoneOS 5.5R10. You can run the **show user-sso client sso-monitor**[*profile-name* command to view the converted configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

Specifying the AAA Server

In the authenticated user architecture of the firewall, all authenticated users and user groups cannot independently exist and need to be associated with an AAA server. SSO Monitor users are synchronized from the external server. By specifying an AAA server for the firewall, SSO Monitor users can be associated with this AAA server.

To specify the referenced server by system, in the SSO-Monitor configuration mode, use the following command:

aaa-server *server-name*

- *server-name* - Specifies the name of the referenced AAA server. You can select Local, AD or LDAP server on the AAA server. After selecting the AAA server, system can query the cor-

responding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

To delete the AAA server, in the SSO-Monitor configuration mode, use the following command:

no aaa-server

Specifying the Port

To specify the port number of the third-party authentication server, in the SSO-Monitor configuration mode, use the following command:

port *number*

- *number* – Specifies the port number of the third-party authentication server. System will obtain the authenticated user information through the port number. The default number is 6666. The range is 1024 to 65535.

To restore the port number to default, in the SSO-Monitor configuration mode, use the following command:

no port

Specifying the Organization Source

To specify the organization source, in the SSO-Monitor configuration mode, use the following command:

org-source [**aaa-server** | **message**]

- **aaa-server** – Specifies the organization source as AAA Server. System uses the user organization structure of AAA server as the group user belongs to. It's usually used in the scenario of the third-party authentication server being authenticated by AAA server and the user organization structure being saved in the AAA server.
- **message** - Specifies the organization source as Message. System uses the user group of authentication message as the group user belongs to. It's usually used in the scenario of the third-party authentication server saving user group.

By default, the organization source is Message. To restore to the default, in the SSO-Monitor configuration mode, use the following command:

no org-source



Notes: In the scenario where AD Agent software is used to obtain user information, if the security agent function is configured, this function will be automatically converted to the SSO Monitor function to connect AD Agent software configuration after the system is upgraded to StoneOS 5.5R10. The organization source is AAA server after the conversion. You can run the **show user-sso client sso-monitor**[*profile-name* command to view the converted configuration. The converted name of SSO Monitor Profile is the same as that of the AD server.

Specifying the Disconnection Timeout

To specify the disconnection timeout, in the SSO-Monitor configuration mode, use the following command:

disconn-del-timeout *timeout*

- *timeout* - Configure the disconnection timeout. When StoneOS disconnects with the third-party authentication server due to timeout,, system will wait during the disconnection timeout. If system still fails to connect within the configured time, it will delete online user. The range is 0 to 1800 seconds. The default value is 300. 0 means the user authentication information will never time out.

To restore the SSO Monitor disconnection timeout to default, in the SSO-Monitor configuration mode, use the following command:

no disconn-del-timeout

Specifying Forced Timeout of SSO Monitor

To control the length of time that authenticated users are online, you can configure forced timeout period of SSO Monitor to disconnect the users.

To specify forced timeout period of SSO Monitor, use the following command in SSO-Monitor configuration mode:

force-timeout *timeout*

- *timeout* - Specifies the forced timeout period. Valid values: 0 to 6000 minutes. Default value: 0, which indicates that authenticate users never times out.

In SSO Monitor configuration mode, use the following command to restore the forced timeout period of SSO Monitor to the default value:

no force-timeout



Tips: In the scenario where SSO Monitor connects AD Agent, we do not recommend that the forced timeout period of SSO Monitor is equal to or larger than the user online duration of AD Agent software.

Viewing the SSO Monitor Configuration

To view the SSO Monitor Configuration owned or specified by system, including name, status, AAA server and client probing interval, in any mode, use the following command:

show user-sso client sso-monitor [*profile-name*]

- *profile-name* – Specifies the name of the SSO Monitor profile. Here shows the configuration information of the specified SSO Monitor.

Viewing the User Mapping Information

To view the mapping information between user name and IP of SSO Monitor, in any mode, use the following command:

show user-mapping user-sso sso-monitor *profile-name*

Viewing the Authentication User Table

The user authentication information generated by machine is saved in the authentication user table. To view the authentication user table, in any mode, use the following command:

show auth-user sso-monitor

Deleting the User Mapping Information

To delete the user mapping information of the specified IP, in any mode, use the following command:

exec user-mappping user-sso sso-monitor kickout ip *ip-address* **vrouter** *vrouter-name*

Configuring TS Agent for SSO

Installing and running Hillstone Terminal Service Agent in the Windows server. After the TS Agent is configured, when users log in the Windows server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users, and achieve the "no-sign-on" authentication.

The configurations of TS Agent for SSO include:

- Configuring the TS Agent server: Installing and running Hillstone Terminal Service Agent in Windows server.
- Configuring the TS Agent client: Configuring TS Agent parameters in StoneOS.



Notes: This section mainly describes how to configure TS Agent parameters in StoneOS and the commands to view information about TS Agent. For installing and running Hillstone Terminal Service Agent in Windows server, refer to "Example of Configuring TS Agent for SSO" on Page 1343.

Creating TS Agent Profile

To create TS Agent profile and enter the TS-Agent configuration mode, in the global configuration mode, use the following command:

user-sso client ts-agent *profile-name*

- *profile-name* - Specifies a name of the TS Agent profile to be created. After executing the command, system will create the TS Agent profile with the specified name and enter TS-

Agent configuration mode; if the profile with the specified name has existed, system will enter the TS-Agent configuration mode directly.

To delete the specified TS Agent profile, in the global configuration model, use the following command:

no user-sso client ts-agent *profile-name*

Enabling / Disabling the TS Agent Function

After enabling TS Agent, StoneOS will establish SSL connection with Hillstone Terminal Service Agent, as well as obtain user and port range information. System will also update the mapping information of traffic IPs, port ranges and user names in real time for online users.

To enable TS Agent function, in the TS-Agent configuration mode, use the following command:

enable

To disable TS Agent function, in the TS-Agent configuration mode, use the following command:

no enable

Specifying the TS Agent Server

To specify the TS Agent server, in the TS-Agent configuration mode, use the following command:

host {*domain-name* | *ip-address*} [**vrouter** *vrouter-name*]

- *domain-name* | *ip-address* - Specifies the management address of the TS Agent server. It can be a domain name, or an IPv4 or IPv6 address.
- **vrouter** *vrouter-name* - Specifies the VRouter of the TS Agent server.

To delete the TS Agent server, in the TS-Agent configuration mode, use the following command:

no host

Specifying the TS Agent Port

To specify the port number of the TS Agent server, in the TS-Agent configuration mode, use the following command:

port *port-number*

- *port-number* – Specifies the port number of the TS Agent server. The default number is 5019. The range is 1025 to 65534. This port number must be the same with the listening port number of Hillstone Terminal Service Agent, otherwise, the TS Agent client and the TS Agent server cannot communicate with each other.

To restore the port number to default, in the TS-Agent configuration mode, use the following command:

no port

Specifying the AAA Server

To specify the referenced server by system, in the TS-Agent configuration mode, use the following command:

aaa-server *server-name*

- *server-name* - Specifies the name of the referenced AAA server. You can select Local, AD or LDAP server on the AAA server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

To delete the AAA server, in the TS-Agent configuration mode, use the following command:

no aaa-server

Specifying the Disconnection Timeout

To specify the disconnection timeout, in the TS-Agent configuration mode, use the following command:

disconnection-timeout *timeout*

- *timeout* - Configure the disconnection timeout. When StoneOS disconnects with Hillstone Terminal Service Agent, system will wait during the disconnection timeout. If system still

fails to connect within the configured time, it will delete online user. The range is 0 to 1800 seconds. The default value is 300. 0 means delete the online user immediately.

To restore the TS Agent disconnection timeout to default, in the TS-Agent configuration mode, use the following command:

no disconnection-timeout

Specifying the Traffic IP

To specify the traffic IP, in the TS-Agent configuration mode, use the following command:

traffic-ip *ip-address*

- *ip-address* - Specifies the traffic IP address, that is the network interface IP address of the TS Agent server. It cab be an IPv4 or IPv6 address. You can specify up to 4 IP addresses.

To delete the specified traffic IP, in the TS-Agent configuration mode, use the following command:

no traffic-ip *ip-address*

Viewing the TS Agent Configuration

To view the TS Agent configuration owned or specified by system, including name, enabling or disabling status, TS Agent server, AAA server, disconnection timeout and traffic IP, in any mode, use the following command:

show user-sso client ts-agent [*profile-name*]

- *profile-name* - Specifies the name of the TS Agent profile. Here shows the configuration information of the specified TS Agent.

Viewing the TS Agent Status

To view the TS Agent status, including connection status, port range allocated to users, number of ports per block, maximum number of block per user, keepalive interval and keepalive timeout, in any mode, use the following command:

show user-sso client ts-agent *profile-name* **status**

Viewing the User Mapping Information

To view the user mapping information of TS Agent, in any mode, use the following command:

show user-mapping user-sso ts-agent *profile-name*

Viewing the Authentication User Table

The user authentication information generated by device is saved in the authentication user table. To view the authentication user table, in any mode, use the following command:

show auth-user ts-agent [**port-range** *range* | **vrouter** *vrouter-name*]

Deleting the User Mapping Information

To delete the user mapping information of the specified IP address and port range, or the specified user name, in any mode, use the following command:

exec user-mappping user-sso ts-agent kickout {**ip** *ip-address* **vrouter** *vrouter-name* **port-range** *range* | **username** *user-name* **auth-server** *server-name*}

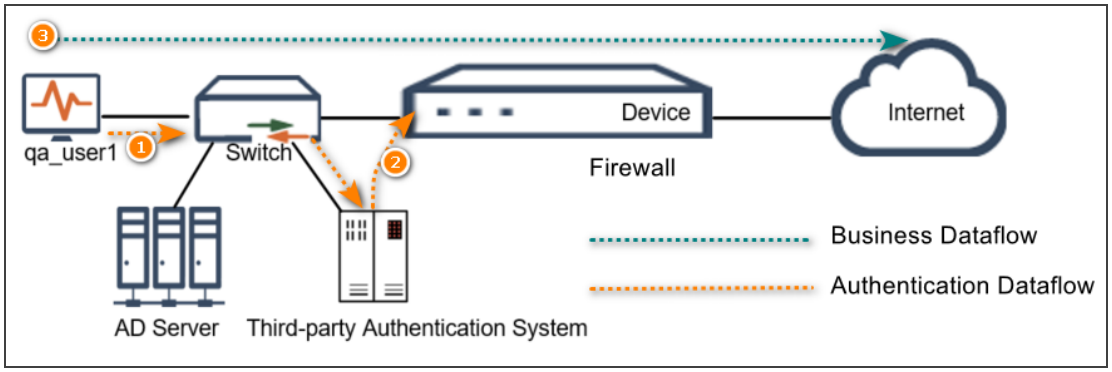
SSO Web for SSO

The firewall supports integration with a third-party authentication system by using the SSO Web function to achieve SSO and policy control based on user groups and roles. This includes:

- The firewall is integrated with a third-party authentication system, which sends user login/-logout messages and user information update messages to the firewall via HTTP(S) RESTful API requests. The firewall retrieves user authentication information based on these messages.
- When an authenticated user accesses the firewall, the firewall uses the synchronized authentication information to update online user information and manage user login/logout operations, thereby achieving SSO and policy control based on user groups and roles.

Typical Scenarios of SSO Web for SSO

The typical scenario of SSO Web for SSO is as follows:



1. Users use a third-party authentication system for authentication.

2. The third-party authentication system sends user authentication information to the firewall via HTTP(S) RESTful API requests.

   The method by which the firewall obtains the user group or role information depends on the sent user authentication messages and the configuration of the AD server on the firewall. There are four possible scenarios:

   - If the user authentication information sent to the firewall **includes user group or role information**, the firewall directly retrieves the user group or role information;
   - If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize both users and user groups, the firewall can query the user group to which the user belongs from the synchronized data in the AD server;
   - If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize only users, only user groups, or neither users nor user groups, the firewall can query the user group to which the user belongs by using the AD server;
   - If the user authentication information sent to the firewall **does not include role information**, but the firewall has a role mapping rule configured for the AD server, the firewall can assign a role to the user based on the mapping rules.

3. The firewall provides network access control for users based on user groups or roles, and users do not need to be authenticated again for network access.

Configuring SSO Web for SSO

To configure SSO Web for SSO, follow this procedure:

1. Configure the AAA server referenced by SSO Web: Local, Active-Directory, or LDAP.
2. Configure SSO Web in the firewall.
3. Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System.
4. Viewing SSO Web Configuration/Authenticated User Information/User Mapping Information
5. (Optional) Kicking out SSO Web User

Configuring SSO Web

Entering the SSO Web Configuration Mode

To enter the SSO Web configuration mode, use the following command in global configuration mode:

user-sso server sso-web default

Enabling the SSO Web Function

By default, the SSO Web function is disabled. To enable this function, use the following command in SSO Web configuration mode:

enable

To disable the function, use the following command:

no enable

Specifying the AAA Server

To specify the AAA server referenced by system, use the following command in SSO Web configuration mode:

aaa-server*aaa-server-name*

- *aaa-server-name* – Specifies the name of the AAA server. The Local, AD or LDAP server is available to select on the AAA server. After selecting the AAA server, system can query the corresponding user group and role of the online user on the referenced AAA server, so as to achieve the policy control based on the user group and role. By default, the Local server is selected.

To cancel the above configurations, use the following command in SSO Web configuration mode:

no aaa-server

Configuring Forced Timeout

To specify the forced timeout, in SSO Web configuration mode, use the following command:

force-timeout*time*

- *time* - Specifies the forced timeout time. If the system does not receive the user information update request within the enforced timeout after the user logs in, the user will be forcefully logged out and disconnected. The range is 0 to 1440 minutes, and the default value is 0 minute. If it is set to 0, this function will be disabled.

To restore the forced timeout to the default value, in SSO Web configuration mode, use the following command:

no force-timeout

Specifying IP Range of Trusted Client

To specify the IP range of the trusted client, in SSO Web configuration mode, use the following command:

trust-client-address*address-book*

- *address-book*- Specifies the IP range of the trusted client. Only SSO Web clients within the specified IP range can send user login/logout and user information update messages to the StoneOS system via HTTP(S) RESTful API. You can specify an existing IPv4 or IPv6 address book entry in the system. The default value is "Any", which indicates that any SSO Web client of IPv4 address can send user login/logout and user information update messages to the StoneOS system via HTTP(S) RESTful API.

To restore the IP range to the default value, in SSO Web configuration mode, use the following command:

no trust-client-address

Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System



Notes:

- The firewall interface communicating with a third-party authentication system needs to have HTTP or HTTPS services enabled.
- The IP address of the third-party authentication system need to fall within the trusted host range of the firewall.

The O&M personnel of the third-party authentication system use development tools to construct HTTP(S) RESTful API requests within the code. Upon successful user authentication, the third-party authentication system synchronizes the user authentication information with the firewall.

The formats of RESTful API requests are as follows:

- User login request: http(s)://*firewall's IP*/rest/api/sso-web-user?**opr=login&info=***USERINFO*

- User logout request: http(s)://*firewall's IP*/rest/api/sso-web-user?**opr=logout&info=***USERINFO*

Parameter description:

- *firewall's IP*: The IP address of the firewall receiving user authentication information.
- **opr**: Supports only two message types —**login** and **logout**
- **info=***USERINFO*: The user information for login or logout. *USERINFO* is a base64-encoded string containing the authenticated user's UserIP, UserName, Group, and Role details, which needs to be generated in the third-party authentication system's code based on the required format. UserIP and UserName are required, while Group and Role are optional. It supports multiple Group but only one Role. The format of USERINFO before encoding is as follows:

Authenticated User Information	USERINFO Format before Encoding
Contains only user IP and username	UserIP/UserName//
Contains user IP, username, and Group	UserIP/UserName//Group
Contains user IP, username, and Role	UserIP/UserName///role=Role
Contains user IP, username, Group, Role	UserIP/UserName//Group//role=Role
Contains user IP, username, multiple Group and Role	UserIP/UserName//Group1//Group2//role=Role

Example: UserIP=120.1.1.163, UserName=qa_user1, Group=QA_Group, Role=RnD-Group. The IP address of the firewall is 10.182.12.34, so USERINFO is "120.1.1.163/qa_user1//QA_Group//role=RnD-Group". After performing base64 encoding in the third-party system, the result is: MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==

Therefore, the login/logout requests from the third-party system are as follows:

- Login request: http(s)://10.182.12.34/rest/api/sso-web-user-
  ?opr-
  =login&i-
  nfo-
  o=MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==
- Logout request: http(s)://10.182.12.34/rest/api/sso-web-user-
  ?opr-
  =logout&i-
  nfo-
  o=MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==

Viewing Configuration Information

To view the configuration information about SSO Web, including the status, forced timeout, AAA server, and IP range of trusted client, in any mode, use the following command:

show user-sso server sso-web default

Viewing the Authenticated SSO Web

To view the user authentication information about SSO Web, in any mode, use the following command:

- To view control-plane SSO Web user authentication information: **show auth-user sso-web**
- To view data-plane SSO Web user authentication information: **show dp-auth-user sso-web**

Viewing the SSO Web User Mapping Information

To view the user mapping information of SSO Web, in any mode, use the following command:

show user-mapping user-sso sso-web

Kicking out SSO Web User

To kick out an SSO Web user and delete the user mapping information of the specified IP address or the specified username, in any mode, use the following command:

exec user-mappping user-sso sso-web kickout {**ip***ip-address***vrouter***vrouter-name* | **username***user-name***auth-server***server-name*}

Portal Authentication

The portal authentication function identifies and authenticates the users when they want to access the Internet via the device. After configuring the portal authentication function, the HTTP requests will be redirected to the specified authentication page of the portal server. In this page, you can visit free resources. If you want to access the other resources in the Internet, provide your username and password in this page. After passing the portal authentication succcessfully, the system will assign a role to the user's IP address according to the policy configuration. And assigning a role can control the resource that the IP address can access.

The portal server is configured by the third party and it receives the portal authentication requests, identifies and authenticates the users, exchanges the authentication information with the device.

Configuring portal authentication involves the configurations in the following modules:

- Configure interfaces, zones, and role mapping rules.
- Configure the security agent function and the authentication information exchange with the portal server.
- Create policy rules to define the traffic that will be authenticated, and trigger the portal authentication function.

This section introduces how to define the traffic that will be authenticated, and how the policy rule triggers the function.

Notes:

- For more information on security agent function, see Configuring the Security Agent.
- For more information on the third-party portal authentication server, see the third-party user guide.

Configuring a Policy Rule that Triggers the Portal Authentication

To trigger the portal authentication function, you must configure the corresponding policy rule. In the global configuration mode, use the following command:

rule [**role** {**UNKNOWN** | *role-name*} | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*] **from** *src-addr* **to** *dst-addr* **service** *service-name* **application** *app-name* {**permit** | **deny** | **tunnel** *tunnel-name* | **fromtunnel** *tunnel-name* | **webauth** | **portal-server** *portal-server-url*}

action portal-server *portal-server-url*

- *portal-server-url* – Use the portal authentication to the traffic that matches the policy rule and enter the URL of the portal server. The URL can contain up to 63 characters and the format is http://www.acertainurl.com or https://www.acertainurl.com.

Besides, you must specify the other required information in this command to define the traffic that will be authenticated. For more information, see Configuring a Policy Rule in Policy.

Example of Configuring WebAuth

Example of Configuring HTTP WebAuth

In this example, WebAuth user access control is demonstrated. It allows only user1 who is authenticated using WebAuth to access the Internet. All other accesses are denied. The WebAuth server is the local AAA server named local.

Step 1: Configure the user, role and role mapping rule

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user-group usergroup1
hostname(config-user-group)# exit
hostname(config-aaa-server)# user user1
hostname(config-user)# password hillstone1
hostname(config-user)# group usergroup1
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# role role1
hostname(config)# role-mapping-rule role-mapping1
hostname(config-role-mapping)# match user-group usergroup1 role role1
hostname(config-role-mapping)# exit
hostname(config)#
```

Step 2: Specify the role mapping rule for the local authentication server

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# role-mapping-rule role-mapping1
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure interfaces and security zones

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/10
hostname(config-if-eth0/10)# zone untrust
hostname(config-if-eth0/10)# ip address 66.1.200.1/16
```

```
hostname(config-if-eth0/10)# exit
hostname(config)#
```

Step 4: Enable WebAuth function

```
hostname(config)# webauth
hostname(config-webauth)# enable
hostname(config-webauth)# protocal http
hostname(config-webauth)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service dns permit
hostname(config-policy)# rule role UNKNOWN from 192.168.1.1/16 to any service any webauth local
Rule id 4 is created
hostname(config-policy)# exit
hostname(config)#
```

Step 5: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule role role1 from 192.168.1.1/16 to any from-zone trust to-zone untrust service any permit
hostname(config-policy)# exit
hostname(config)#
```

After above configurations, the system will authenticate all HTTP requests (external IP addresses with reachable route) from 192.168.1.1/16. Users can access the Internet after providing the username user1 and password hillstone1 on the login page.

Example of Configuring NTLM Authentication

This section describes the NTLM Authentication example. After the configuration, you can gain access to network resources if only you have been authenticated by the Active Directory server.

To configure the NTLM authentation, take the following steps:

Step 1: Configure an AAA server of Active-Directory type

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the WebAuth Server

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service any webauth ad
hostname(config-policy)# exit
hostname(config)#
```

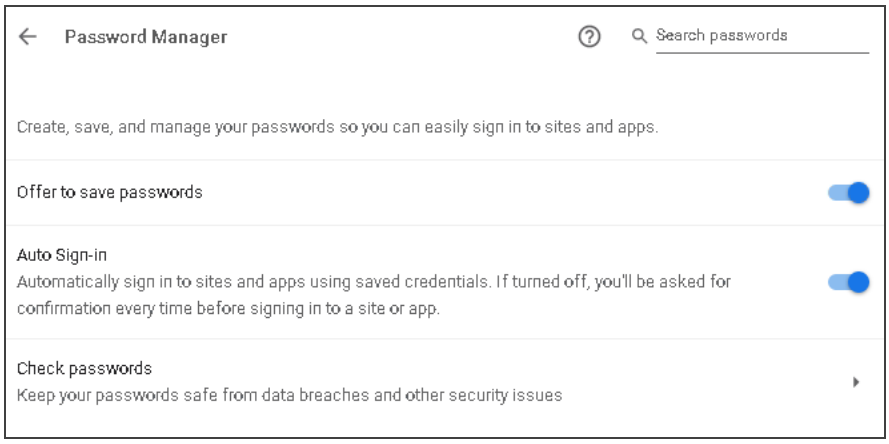
Step 3: Enable NTLM

```
hostname(config)# webauth
hostname(config-webauth)# mode ntlm
```

Step 4: Enable automatic logon with current username and password on your web browser (take Google Chrome as an example)

1. In the toolbar of Google Chrome, click **Settings** > **Autofill** > **Password Manager**.

2. On the **Password Manager** page, enable **Auto Sign-in**.



3. Log off from the system and logon again, and you can gain access to network resources without WebAuth in Chrome.

Example of Configuring SSO

Example of Configuring AD Scripting for SSO

This section describes a typical AD Scripting example. After the configuration, you can be authenticated by the device if only you have been authenticated by the Active Directory server.

The following steps only describe configurations related to AAA Server and AD Scripting, and omit other configurations.

Step 1: Configure an AAA server of Active-Directory type

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
```

```
hostname(config)#
```

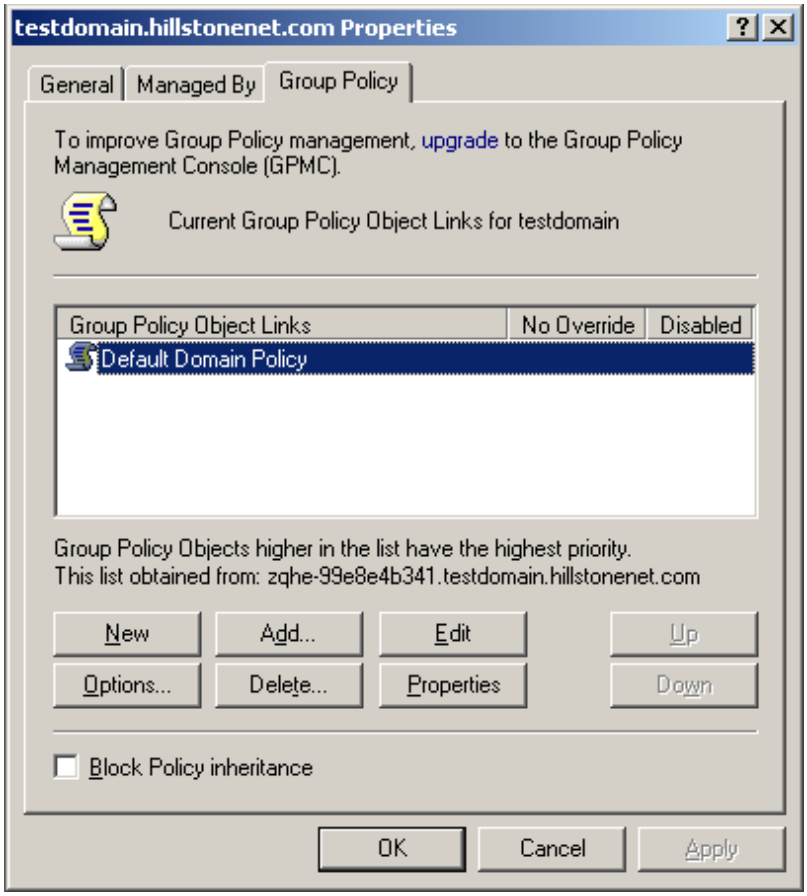
Step 2: Configure the AD Scripting

```
hostname(config)# user-sso server ad-scripting default
hostname(config-ad-scripting)# enable
hostname(config-ad-scripting)# aaa-server ad
hostname(config-ad-scripting)# exit
hostname(config)#
```

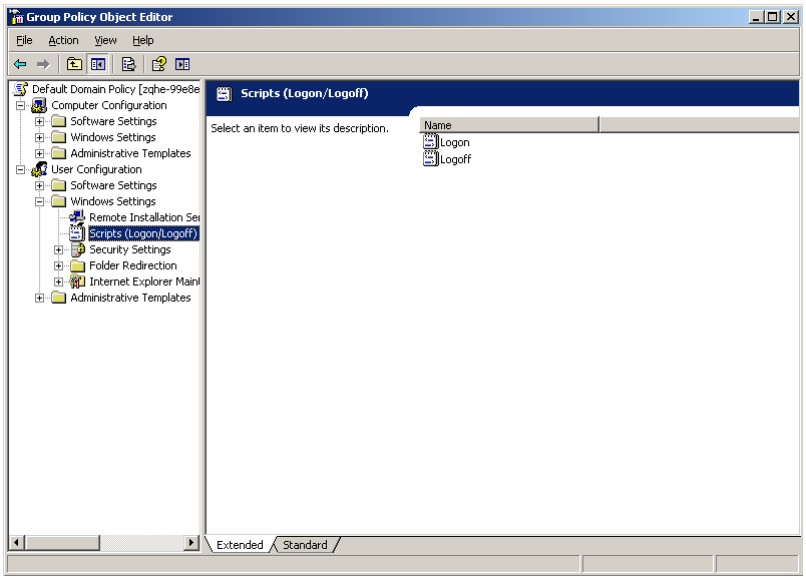
Step 3: In the Active-Directory server, import the logon/logout script

1. On the <AD Scripting> tab of the AD Agent software, click **Get AD Scripting** to get the script "Logonscript.exe", and save it under a directory where all AD server users can access.
2. In AD server, go to Start menu, select **Mangement Tools> Active Directory User and Computer**.

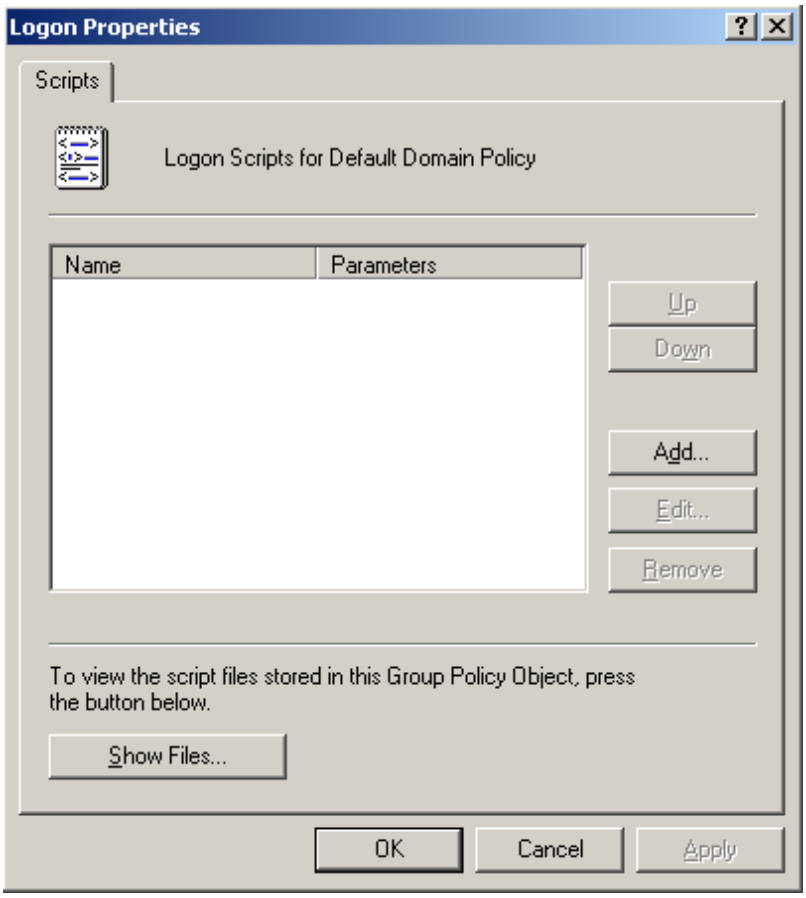
3. In the prompt, right click the domain of SSO, and select **Properties**, then click <Group Properties> tab.



4. Double click the group policy of SSO, and in the prompt, select **User Configuration>Windows>Script (Logon/Logout)**.



5. Double click **Logon** on the right, and click **Add** in the prompt.



6. In the prompt, click **Browse** and select the logon script (logonscript.exe), and then enter IP address of StoneOS for authentication, followed by a space and text Clogon".

7. Click **OK**.

8. Similarly, import the script into the logout setting, repeat 5-7, and use "logoff" in the step 6.

Notes: The directory of saving the script must be accessible to all domain users, otherwise, when a user who does not have access will not trigger the script when he logs in or out.

Example of configuring AD Polling for SSO

This section describes a typical example of configuring the AD Polling for SSO. After the configuration, when the domain user logs in via the AD server, the AD server will generate the login user information. After enabling the AD Polling function, system will query the AD server regularly to obtain the user login information and probe the terminal PC to verify whether the online users are still online, thus getting correct authentication user information to achieve SSO.

To configure the AD Polling for SSO, take the following steps:

Step 1: Configure the AAA server referenced by AD Polling. You can select Local, AD or LADP server, see Specifying the AAA Server. Take the AD server as an example:

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 192.168.2.2
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Enable the AD Polling function and configure the authentication server, AAA server-,account, password, etc.

```
hostname(config)# user-sso client ad-polling test
hostname(config-ad-polling)# enable
hostname(config-ad-polling)# host 10.180.201.8
hostname(config-ad-polling)# account adpoll\administrator
hostname(config-ad-polling)# password hillstone
hostname(config-ad-polling)# aaa-server ad
hostname(config-ad-polling)# exit
hostname(config)#
```

Configuration Examples of Using SSO Monitor for SSO

AD Agent software can send user online status within the AD domain to the firewall by using packets of SSO-Monitor protocol. Therefore, AD Agent software can be used as an external server that connects SSO Monitor for SSO. In this example, AD Agent software is used to show you how to implement SSO by connecting SSO Monitor with AD Agent.

Install AD Agent software on a PC within the AD server or domain. When a user in the domain logs in to the Active-Directory server, AD Agent records the username, IP address, and time when the user was most recently online, and sends the mapping relationships between usernames and IP addresses to StoneOS. This avoids users from repeated logins and generates authenticated users on the firewall. The system can also implements user-based security statistics, log records, and online behavior auditing by using the obtained mapping relationships between usernames and IP addresses.

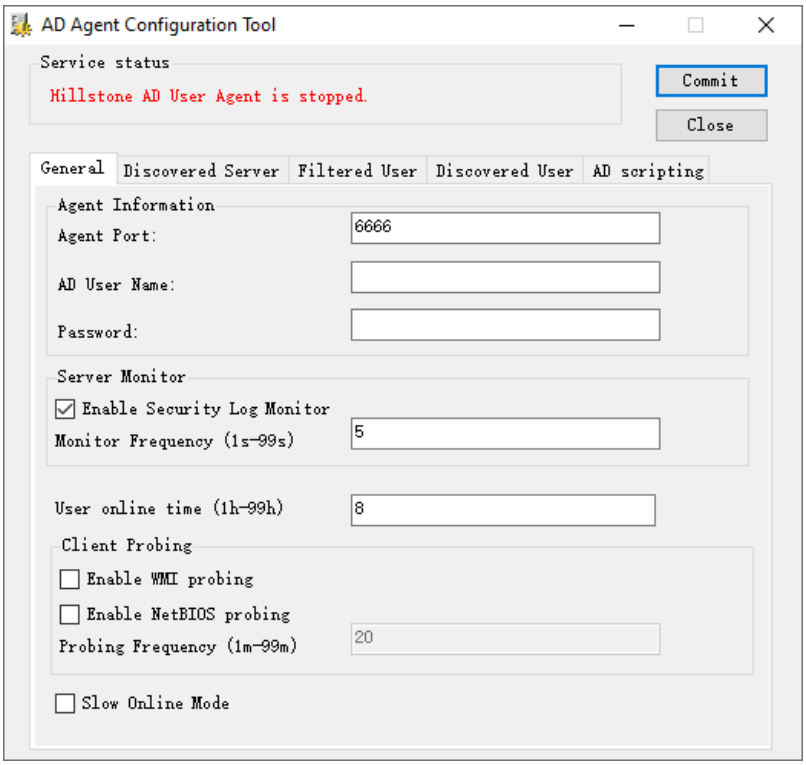
To use SSO Monitor for SSO, take the following steps:

Step 1: Install AD Agent and configure the corresponding parameters. AD Agent can be installed on an AD server or a PC within the domain. It can run in the Windows and Windows Server environment. We recommend that you install AD Agent on Windows Server 2008 /2012/2016/2019 or Windows 7/10.

To install the AD Agent to an AD server or a PC in the domain, take the following steps:

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-adagent to download an AD Agent software and copy it to a PC or a server within the domain.
2. Double-click ADAgentSetup.exe to open it and follow the installation wizard to install it.
3. Start AD Agent by using one of the following methods:
    a. Double-click the AD Agent Configuration Tool shortcut on the desktop.
    b. Click **Start** menu and select **All apps** > **Hillstone AD Agent** >**AD Agent Configuration Tool**.

4. Click the <General> tab.



On the <General> tab, configure these basic options.

Option	Description
Agent Port	Enter agent port number. AD Agent uses this port to communicate with StoneOS. The range is 1025 to 65535. The default value is 6666. This port must be the same with the configured monitoring port in StoneOS, otherwise, the AD Agent and StoneOS cannot communicate with each other.
AD User Name	Enter user name to log in the AD server. If AD Agent is running on the other PCs of the domain, this user should have high privilege to query event logs in AD server, such as the user of Administrator whose privilege is Domain

Option	Description
	Admins on AD server.
Password	Enter the password that matched with the user name. If the AD Security Agent is running on the device where the AD server is located, the user name and password can be empty.
Server Monitor	
Enable Security Log Monitor	Monitor Select to enable the function of monitoring event logs on AD Security Agent. The default query interval is 5 seconds. The function must be enabled if the AD Security Agent is required to query user information.
Monitor Frequency	Specifies the polling interval for querying the event logs on different AD servers. The default value is 5 seconds. When finishing the query of a AD server, the AD Agent will send the updated user information to system.
User online time	Specifies the online duration of a user after successful SSO. After the user expires, it will be forced to log out. The range is 1 to 99 hours and the default value is 8 hours.
Client Probing	
Enable WMI probing	Select the check box to enable WMI probing. • To enable WMI to probe the terminal PCs, the terminal PCs must open the RPC service and remote

Option	Description
	management. To enable the RPC service, you need to enter the **Control Panel** > **Administrative Tools** > **Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**. • WMI probing is an auxiliary method for security log monitor. which will probe all IPs in Discovered Users list. When the probed domain name does not match with the stored name, the stored name will be replaced by the probed name.
Probing Frequency	Specifies the interval of active probing action. The range is 1 to 99 minutes and the default value is 20 minutes.
Slow Online Mode	Select the check box to enable the slow online mode. After configuring role mapping rules in the firewall, this mode can prevent role mapping failures caused by the client users going online too quickly.

5. On the <Discovered Server> tab, click **Auto Discover** to start automatic scanning the AD servers in the domain. Besides, you can click **Add** to input IP address of server to add it manually.

6. On the <Filtered User> tab, type the user name need to be filtered into the **Filtered user** text box. Click **Add**, and the user will be displayed in the Filtered User list. You can configure 100 filtered users, which are not case sensitive.

7. Click the <Discovered User> tab to view the corresponding relationship between the user name and user address that has been detected. The user added into the Filtered User list will not be displayed in the Discovered User list.

8. Click **Commit** to submit all settings and start AD Agent service in the mean time.



Notes: After you have committed, AD Agent service will be running in the background all the time. If you want to modify settings, you can edit in the **AD Agent Configuration Tool** and click **Commit**. The new settings can take effect immediately.

Step 2: Configure the AAA server referenced by SSO Monitor.

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 192.168.2.2
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Enable and configure SSO Monitor function. Specify the authentication server, the referenced AAA server, organization source and so on.

```
hostname(config)# user-sso client sso-monitor test
hostname(config-ad-polling)# enable
hostname(config-ad-polling)# host 10.180.201.8 vrouter trust-vr
hostname(config-ad-polling)# aaa-server ad
hostname(config-ad-polling)# org-source aaa-server
```

```
hostname(config-ad-polling)# port 6666
hostname(config-ad-polling)# exit
hostname(config)#
```

Configuration Examples of SSO Radius Login

The following is a configuration example for SSO Radius function. After configuring the SSO Radius function, system can receive the accounting packets that based on the Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.

To use SSO Radius for SSO, take the following steps:

Step 1: Configure the AAA server referenced by SSO Radius. You can select the configured Local, AD or LDAP server. For the configuration method, see Configuring an AAA Server. Here take AD server as the example.

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Enable SSO Radius function, as well as specify the referenced AAA server, IP address of the client and so on.

```
hostname(config)# user-sso server sso-radius default
hostname(config-sso-radius)# enable
hostname(config-sso-radius)# aaa-server ad
hostname(config-sso-radius)# client 2.2.2.2
hostname(config-sso-radius-client)# exit
```

```
hostname(config-sso-radius)# exit
hostname(config)#
```

Example of Configuring TS Agent for SSO

This section describes a typical TS Agent for SSO example. Installing and running Hillstone Terminal Service Agent in the Windows server. After the TS Agent is configured, when users log in the Windows server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users, and achieve the "no-sign-on" authentication.

The configurations of TS Agent for SSO include:

- Configuring the TS Agent server: Installing and running Hillstone Terminal Service Agent in Windows server.
- Configuring the TS Agent client: Configuring TS Agent parameters in StoneOS.

Step 1: Installing and running Hillstone Terminal Service Agent in Windows server

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-tsagent to download a Hillstone Terminal Service Agent installation program, and copy it to the Windows server.



Notes:

- Windows Server 2008 R2, Windows Server 2016, and Windows Server 2019 are currently supported. Windows Server 2008 R2 Service Pack 1 and KB3033929 must be installed if Windows Server 2008 R2 is used.



- It's recommended to close the anti-virus software before installing Hillstone Terminal Service Agent in Windows server.

2. Double-click HSTSAgent.exe to open it and follow the installation wizard to install it.
3. Double-click the `Hillstone Terminal Service Agent` shortcut, and the **Hillstone Terminal Service Agent** dialog pops up.
4. Click the **Agent config** tab and configure as below:
   - Listening Address IPv4: 0.0.0.0
   - Listening Port (1025-65534): 5019
   - Heartbeat Interval (1-30s): 5
   - Heartbeat Timeout (10-300s): 60

   Click **Save** to save the configurations.
5. Click the **Port config** tab and configure as below:
   - User Allocable Port Range (1025-65534): 20000-39999
   - User Port Block Size (20-2000): 200
   - User Port Block Max (1-256): 1
   - Passthrough when user port exhausted: Select the check box

   Click **Save** to save the configurations.

Step 2: Configuring TS Agent parameters in StoneOS

```
host-name(config)# user-sso client ts-agent tsagent1
host-name(config-ts-agent)# host 10.1.1.1
host-name(config-ts-agent)# aaa-server local
host-name(config-ts-agent)# traffic-ip 10.1.1.1
```

```
host-name(config-ts-agent)# enable
host-name(config-ts-agent)# exit
hostname(config)#
```

Example of Configuring Agile Controller for SSO

This section describes a typical example of configuring the Agile Controller for SSO. After the configuration, system can get correct authentication user information in the following two ways to achieve SSO:

- Receiving packets sent by the Agile Controller server. The packets are sent when users log in to or log out of the server or when users update their information.
- When the traffic flowing through the device matches the configured query address range and there is no corresponding authenticated user locally, the system will actively query the user information from the Agile Controller server and update the local user information.

To configure the Agile Controller for SSO, take the following steps:

Step 1: Configure the AAA server referenced by Agile Controller. You can select Local, AD or LADP server, see Specifying the AAA Server. Take the AD server as an example:

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 192.168.2.2
hostname(config-aaa-server)# base-dn dc=hillstonenet
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

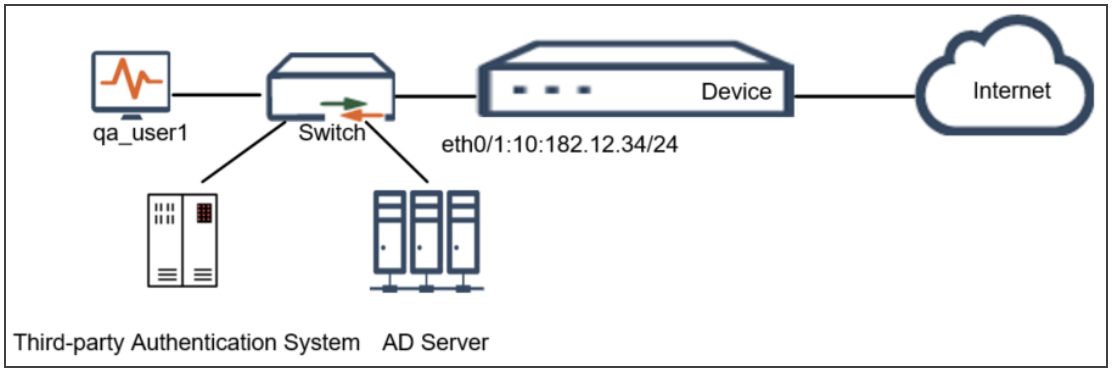
Step 2: Enable the Agile Controller function and configure the AAA server, the address range of the source IP to be queried, the IP address of the Agile Controller server and the shared key.

```
hostname(config)# user-sso server agile-controller default
```

```
hostname(config-agile-controller)# enable
hostname(config-agile-controller)# aaa-server ad
hostname(config-agile-controller)# sync-address address_book1
hostname(config-agile-controller)# access-agile-controller test
hostname(config-agile-controller-client)# host 1.1.1.1 vrouter trust-vr
hostname(config-agile-controller-client)# shared-secret Agilecon@123
hostname(config-agile-controller-client)# sync enable
hostname(config-agile-controller-client)# exit
hostname(config-agile-controller)# exit
hostname(config)#
```

Example of Configuring SSO Web for SSO

The topology is shown as follows. An enterprise has deployed a Hillstone security device as the egress gateway at the network boundary to connect the internal network and the Internet. The enterprise stores user organization structure on the AD server and performs user authentication based on the third-party authentication system. After completing the SSO Web configuration, the firewall can obtain accurate user authentication information, enabling network access control based on the user group or role of the user.



Procedure of SSO Web for SSO

1. Users use a third-party authentication system for authentication.
2. The third-party authentication system sends user authentication information to the firewall via HTTP(S) RESTful API requests.

   The method by which the firewall obtains the user group or role information depends on the sent user authentication messages and the configuration of the AD server on the firewall. There are four possible scenarios:

   - If the user authentication information sent to the firewall **includes user group or role information**, the firewall directly retrieves the user group or role information;
   - If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize both users and user groups, the firewall can query the user group to which the user belongs from the synchronized data in the AD server;
   - If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize only users, only user groups, or neither users nor user groups, the firewall can query the user group to which the user belongs by using the AD server;
   - If the user authentication information sent to the firewall **does not include role information**, but the firewall has a role mapping rule configured for the AD server, the firewall can assign a role to the user based on the mapping rules.
3. The firewall provides network access control for users based on user groups or roles, and users do not need to be authenticated again for network access.

Configuration Steps

Step 1: Configure a Local, AD, or LDAP server as the AAA server referenced by SSO Web. In this example, an AD server is used.

```
hostname(config)# aaa-server adserver type active-directroy
hostname(config-aaa-server)# exit
hostname(config)#
(Other basic AD server configurations are omitted here)
```

Step 2: Enable SSO Web and specify the AAA server

```
hostname(config)# user-sso server sso-web default
hostname(config-sso-web)# enable
hostname(config-sso-web)# aaa-server adserver
hostname(config-sso-web)# exit
hostname(config)#
```

Step 3: O&M personnel of the third-party authentication system use development tools to construct HTTP(S) RESTful API requests in the code of the system. After successful user authentication, the third-party system calls the firewall's API to synchronize the user authentication information with the firewall.



Notes:

- The firewall interface communicating with the third-party authentication system need to have HTTP or HTTPS services enabled.
- The IP address of the third-party authentication system need to fall within the trusted host range of the firewall.

```
In this example, UserIP=120.1.1.163, User-
Name=qa_user1, Group=QA_Group, and Role=RnD-
Group. The IP address of the firewall interface
is 10.182.12.34. The O&M personnel of the
third-party authentication system use devel-
opment tools to construct the following HTTP(S)
RESTful API requests in the code of the third-
party authentication system:
```

For more information, see Constructing an HTTP (S) RESTful API Request in the Third-Party Authentication System.

- User login request:

```
http(s)://10.182.12.34/rest/api/sso-web-user-
?opr-
=login&i-
nfo-
=MTIwLjEuMS4xNjMvcWF-
FfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==
```

- User logout request:

```
http(s)://10.182.12.34/rest/api/sso-web-user-
?opr-
=logout&i-
nfo-
=MTIwLjEuMS4xNjMvcWF-
FfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==
```

Sample RESTful API request responses:

GET: Login of sso-web type user

Successful login:

HTTP/1.1 200 OK

ContentType:: application/json

Content-Length: 128

Success Example:

{

"success": true,

```
}
Failed login:
HTTP/1.1 200 OK
Content-Type: application/json; charset="UTF-8"
Content-Length: 128
{
"success": false,
"exception": {
"code":"400000000",
"message":"Error: Request resolution failed",
"stack":""
}
}
```

GET: Logout of sso-web type user

```
Successful logout:
HTTP/1.1 200 OK
ContentType:: application/json
Content-Length: 128
Success Example:
{
"success": true,
}
Failed logout:
HTTP/1.1 200 OK
Content-Type: application/json; charset="UTF-8"
Content-Length: 128
```

```
{
"success": false,
"exception": {
"code":"400000000",
"message":"Error: Request resolution failed",
"stack":""
}
}
```

Step 4: Verify the results.

After the user successfully logs in, the firewall retrieves the user's user group or role information and matches it with Group and Role in the policy rules, enabling network access control.

```
hostname(config)# show auth-user
Username: qa_user1
AAA Server: adserver
Authentication: User got from sso-web, online 5s
Reference Session: 0
Virtual Router: trust-vr
IP/MAC: 120.1.1.163
Auth user id: 1
Group: QA_Group
Role: RnD-Group
Authorization:
```

Example of Configuring Portal Authentication

This section describes a typical portal authentication configuration example.

This example allows only user1 who is authenticated using portal authentication to access the Internet. All other accesses are denied. The authentication server is the portal authentication server and the URL of the portal server is 192.168.1.2.

Step 1: Configure the role and role mapping rule

```
hostname(config)# role role1
hostname(config)# role-mapping-rule role-mapping1
hostname(config-role-mapping)# match user-group usergroup1 role role1
hostname(config-role-mapping)# exit
hostname(config)#
```

Step 2: Configure interfaces and security zones

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/16
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 66.1.200.1/16
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone dmz
hostname(config-if-eth0/2)# ip address 192.168.2.1/16
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure the role mapping rule of the portal authentication server and enable the security agent function

```
hostname(config)# aaa-server AD type active-directory
hostname(config-aaa-server)# role-mapping-rule role-mapping1
```

```
hostname(config-aaa-server)# host 192.168.2.2
hostname(config-aaa-server)# base-dn “dc=hillstone”
hostname(config-aaa-server)# login-dn “user=administrators”
hostname(config-aaa-server)# login-password password1
hostname(config-aaa-server)# agent
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 4: Trigger the portal authentication function via the policy rule

```
hostname(config)# rule id 1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-ip 192.168.2.2/16
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# rule id 2
hostname(config-policy-rule)# role UNKNOWN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# action portal-server http://192.168.2.2/
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# rule id 3 from any to any service any permit
```

Step 5: Configure a policy rule that allows the access

```
hostname(config)# policy-global
hostname(config-policy)# rule role role1 from 192.168.1.1/16 to any service any per-
mit
```

```
hostname(config-policy)# exit
hostname(config)#
```

After above configurations, the system will authenticate all HTTP. Users can access the Internet after providing the username user1 and password hillstone1 on the login page.

802.1X Authentication

Overview

802.1X is a standard defined by IEEE for Port-based Network Access Control. It uses Layer 2-based authentication to verify the legality of the users accessing the network trough LAN. Before authentication, the security device only allows 802.1X message to pass through the port. And after authentication, all the normal traffic can pass through.

802.1X Architecture

802.1X authentication architecture includes three components: client, authenticator and authentication server. The figure below shows the diagram of 802.1X authentication architecture.



Only when these three components are presented will 802.1X authentication be completed.

- Client: After you start the client program and enter your username and password, the client program will send requests for 802.1X authentication to the authenticator. Clients need to support EAP protocol, and should be running 802.1X client software.
- Authentication Server: The server stores users' information, verifies whether users have the right to use network resources, and returns the authentication results to the authenticator. StoneOS support local authentication server or RADIUS server to implement authentication and authorization.
- Authenticator (Hillstone device): The authenticator provides a physical interface for clients to access to LAN. It transmits users' information to the authentication server or returns it to the client, and then enables or disables the interface according to the server's authentication results. Authenticator acts as an agent between the client and authentication server.

802.1X Authentication Process

Authentication methods of 802.1X include EAP-MD5, EAP-TLS and EAP-PEAP. Different methods have different authentication processes.

Authenticating by EAP-MD5 Method

Here, take the EAP-MD5 authentication method as the example to introduce the basic 802.1X authentication process:

1. When you need to visit network, you should start the 802.1X client program, and enter your username and password to send a connection request. The authentication process starts.
2. After the authenticator receives the connection request from the client, it will ask the client to send its username.
3. The client responds and sends its username to the authenticator.
4. Authenticator will encapsulate the data received from the client and then deliver it to the authentication server.
5. Authentication server will check the username it received, comparing with the user's information in its own database, and try to find the password of the user. After that, the server will generate random encrypted characters to encrypt the password, and send it to the authenticator.
6. Authenticator sends the encrypted characters to the client, and the client will encrypt the password and transmit it back to the authentication server.
7. Authentication server will compare the encrypted password information with their own encrypted password information. If they are matched, the authenticator will consider the user as a legitimate user, and allow the user to access the network through the interface. If not matched, authenticator will refuse the user to access network and keep the status of the interface as non-authenticated.

Authenticating by EAP-TLS Method

EAP-TLS is a kind of 802.1X authentication method that client and server can authenticate each other. Firstly, the server will send its own digital certificate to the client. When the certificate is authenticated to be valid, the client will send user's digital certificate to the server. If the certificate is valid, the server will consider the user as a legitimate user, and allow the user to access the network. If you have deployed PKI system in your network environment, Hillstone recommends that you configure EAP-TLS authentication method.

To use EAP-TLS method to realize 802.1X authentication, please install 802.1X client software which supports certificate authentication at the client side and import user's and CA's digital certificates; please set the authentication method to be EAP-TLS at the server side and import server's and CA's digital certificates.



Tip:

- Currently, the system does not support to realize EAP-TLS authentication via local authentication server.
- The 802.1X client software needs to be compatible with the 802.1X standard protocol.

Configuring 802.1X Authentication

802.1X authentication configurations include:

- Configuring an 802.1X profile.
- Specifying the 802.1X authentication server. StoneOS support local authentication server and external authentication server (RADIUS).
- Configuring 802.1X attributes on port.
- Configuring 802.1X authentication global parameters, such as configuring the maximum number of clients to connect, etc.

Configuring an 802.1X Profile

To create an 802.1X profile, in the global configuration mode, use the following command:

dot1x profile *profile-name*

- *profile-name* - Specifies the name of 802.1X profile. After executing this command, the system will create the 802.1X profile with the specified name, and enter the dot1x configuration mode. If the profile name you specified already exists, the system will directly enter the dot1x configuration mode.

To delete the specified 802.1X profile, in the global configuration mode, use the command:

no dot1x profile *profile-name*

Configuring the Maximum Retry Times

After sending an authentication request to the client and receives a response containing the expected data, the authenticator transmits the client's response data to the authentication server and waits for a response. If the authentication server does not answer, the authenticator will resend an authentication request to the client until receiving a response from the authentication server or exceeding the allowed maximum retry times. To configure the maximum times of resending the authentication request, in the dot1x configuration mode, use the following command:

retransmission-count *value*

- *value* – Specifies the maximum times of resending authentication request frame. The value range is 1 to 10 times. The default value is 2.

To restore to the default value, in the dot1x configuration mode, use the command **no retransmission-count**.

Configuring the Re-auth Period

When the client is authorized to access network, the authenticator can re-authenticate the client. To configure the re-auth period, in the dot1x configuration mode, use the following command:

reauth-period *value*

- *value* – Specify the re-auth period. The value range is 0 to 65535 seconds. The default value is 3600. If the value is set to0, the re-authentication function is disabled.

To restore the default value, in the dot1x configuration mode, use the command **no reauth-period**.

Configuring the Quiet Period

If the authentication fails, the authenticator remains idle for a period of time before go on processing the same request from the same client. To configure the authenticator's quiet period, in the dot1x configuration mode, use the following command:

quiet-period *value*

- *value* – Specifies the value of quiet time. The value range is 0 to 65535 seconds. The default value is 60. The value of 0 indicates that the system will process the request from the same client all the time.

To restore to the default value, in the dot1x configuration mode, use the comman **no quiet-period**.

Configuring the Client Timeout

When the authenticator sends a request to ask the client to submit its username, the client need to responds within a specified period. If client does not respond until timeout, the system will resend the authentication request message. To specify the client timeout value, in the dot1x configuration mode, use the following command:

tx-period *value*

- *value* – Specifies the timeout value. The value range is 1 to 65535 seconds. The default value is 30.

To restore to the default value, in the dot1x configuration mode, use the command **no tx-period**.

Configuring the Server Timeout

After sending an authentication request to the client and receives a response containing the expected data, the authenticator transmits the client's response data to the authentication server and waits for a response. If the server does not answer the authenticator within a specified time, the authenticator will resend an authentication request to the client. To specify the authentication server timeout value, in the dot1x configuration mode, use the following command:

server-timeout *value*

- *value* – Specifies the response timeout value. The value range is 1 to 65535 seconds. The default value is 30.

To restore to the default value, in the dot1x configuration mode, use the command **no server-timeout**.

Specifying the 802.1X Authentication Server

You can specify an AAA server as the 802.1X authentication server. To specify the 802.1X authentication server, in the dot1x configuration mode, use the following command:

aaa-server *server-name*

- *server-name* - Specifies the AAA authentication server name. StoneOS support local authentication server and RADIUS server.

To delete the specified 802.1X authentication server, in the dot1x configuration mode, use the command:

no aaa-server *server-name*



Notes: For information about how to configure the local authentication server and RADIUS server, see Authentication, Authorization and Accounting.

Configuring 802.1X Attributes on Port

The authenticator provides a port for the client to access LAN, and the port need to be bound to Layer 2 security zone or VLAN. You can enable the 802.1X authentication function on the port, and configure attributes according to your need.

Enabling/Disabling 802.1X Authentication

To enable or disable 802.1X authentication, in interface configuration mode, use the following command:

- Enable the 802.1X authentication: **dot1x enable**
- Disable the 802.1X authentication: **no dot1x enable**

After enabling the 802.1X authentication, you can configure 802.1X attributes on the port.

Binding 802.1X Profile to a Port

To bind the created 802.1X profile to a port, in the interface configuration mode, use the following command:

dot1x profile *profile-name*

- *profile-name* – Specifies the 802.1X profile name.

To cancel the binding, in the interface configuration mode, use the command:

no dot1x profile *profile-name*

Configuring the Port Access Control Mode

To configure the access control mode on the specified port, in the interface configuration mode, use the following command:

dot1x port-control {**auto** | **force-unauthorized**}

- **auto** - Automatic mode. This is the default setting. In this mode, the authenticator decides whether the client can access the network according to the results of 802.1X authentication.

- **force-unauthorized** - Force-unauthorized mode. In this mode, the port is always in unauthorized state, and any client attempting to connect will fail.

To restore to default settings, in the interface configuration mode, use the command:

no dot1x port-control

Configuring the Port Access Control Method

To configure the method of 802.1X port access control, in the interface configuration mode, use the following command:

dot1x control-mode {**mac** | **port**}

- **mac** - MAC address-based authentication. All the clients under the port must be authenticated and then they can access network resources.
- **port** - Port-based authentication, which is the default setting. For all the clients under a port, as long as one client is authenticated, other clients can access network without authentication.

To restore the default settings, in interface configuration mode, use the command:

no dot1x control-mode

Configuring 802.1X Global Parameters

The following section describes global parameter configuration for the 802.1X.

Configuring the Maximum User Number

To configure the maximum number of clients that are allowed to connect to the port simultaneously, in the global configuration mode, use the following command:

dot1x max-user *user-number*

- *user-number* – Specifies the maximum user number. The value range is 1 to 1000. The default value may vary from different platforms.

To restore to the default values, in the global configuration mode, use the command **no dot1x max-user**.

Configuring the Timeout of Authenticated Clients

You can configure the authentication timeout value for authenticated clients. If the client does not respond within the specified time, it need reapply an authentication. To configure the timeout value, in the global configuration mode, use the following command:

dot1x timeout *timeout-value*

- *timeout-value* − Specifies the client authentication timeout value. The value range is 180 to 3600*24 seconds. The default value is 300.

To restore to the default value, in the global configuration mode, use the command **no dot1x timeout**.

Configuring Multi-logon Function

By default, the multi-logon function is disabled. If it is enabled, you can log into multiple clients using the same username simultaneously. To enable the multi-logon function, in global configuration mode, use the following command:

dot1x allow-multi-logon

After executing this command, the multi-logon function is enabled, and the number of clients using one username is limited. To specify the number of clients, in the global configuration mode, use the following command:

dot1x allow-multi-logon *number*

- *number* − Specifies how many times the same username can be logged in simultaneouly. The value range is 2 to 1000 times.

To disable this function, in the global configuration mode, use the command:

no dot1x allow-multi-logon

Configuring Auto-kickout Function

When the multi-logon function is disabled, if you enable the auto-kickout function, the user who already logged in will be kicked out by the same user who logs in later. The system will automatically cut the connection to the user who already logged in. If the auto-kickout function is

disabled, the system will prohibit the same user to log in again. To enable or disable the auto-kick-out function, in the global configuration mode, use the following commands:

- Enable the auto-kickout function: **dot1x auto-kickout**
- Disable the auto-kickout function: **no dot1x auto-kickout**

Configuring Manual Kick-out Client

To kick out any client manually, in any mode, use the following command:

exec dot1x kickout *port-name authenticated-user-mac*

- *port-name* – Specifies the port name the client connects to.
- *authenticated-user-mac* – Specifies the MAC address of the authenticated client that is kicked out manually.

Viewing 802.1X Configurations

To view the 802.1X configurations, in any mode, use the following command:

show dot1x [**profile** *profile-name* | **port** *port-name* | **statistics** [*port-name*]]

- **show dot1x** - Shows 802.1X global parameters.
- **profile** *profile-name* – Shows configurations of the specified 802.1X profile.
- **port** *port-name* – Shows the configurations of the specified port and its binding profile's information.
- **statistics** [*port-name*] – Shows statistics information of the specified port.

PKI

Overview

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over Internet. A PKI system consists of Public Key Cryptography, CA, RA, Digital Certificate and related PKI storage library.

The following section describes PKI terminology:

- **Public Key Cryptography**: A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is known only to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by another key of the key pair.
- **CA**: A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.
- **RA**: The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.
- **CRL**: Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

PKI Function of Hillstone Devices

PKI is used in the following three situations:

- IKE VPN: PKI can be used by IKE VPN tunnel.
- HTTPS/SSH: PKI applies to the situation when a user accesses a Hillstone device over HTTPS or SSH.
- Sandbox: Support the verification for the trust certification of PE files. Refer to Importing a Trust Certificate for details.

Configuring PKI

The PKI configuration on Hillstone devices includes:

- Generating and deleting a PKI key pair
- Configuring a PKI trust domain
- Importing a CA certificate
- Generating a certificate request
- Importing a local certificate
- Downloading a CRL
- Importing and exporting a PKI trust domain
- Importing and exporting a local certificate
- Configuring a certificate chain
- Configuring certificate validity check

Generating/Deleting a PKI Key Pair

StoneOS provides a default PKI key pair named Default-Key. To generate a PKI key pair, in the global configuration mode, use the following command:

pki key generate {**rsa** | **dsa** | **sm2** | **ecc**} [**label** *key-name*] [**ec-group** { **prime256** | **prime384** | **prime 521** }] [**modulus** *size*] [**noconfirm**]

- **rsa** | **dsa** – Specifies the type of key pair, either RSA or DSA.
- **label** *key-name* – Specifies the name of the PKI key. The name must be unique in StoneOS.
- **modulus** *size* – Specifies the modulus of the key pair. Valid values for modulus of RSA: 1024, 2048 (default), 512, 768, and 4096 bits. Valid values for modulus of DSA: 1024 (default), 2048, 512, and 768 bits, and the modulus of SM2 is 256.
- **ec-group** { **prime256** | **prime384** | **prime 521** } – Specify the elliptic curve group, including Prime256, Prime384, and Prime521 elliptic curves. The default elliptic curve group is Prime256.
- **noconfirm** – Disables prompt message on the key pair. For example, if the name of the key pair exists in the system, without this parameter configured, the system will prompt whether to overwrite key pair with the same name; with this parameter configured, the system will not allow to create a key pair with the same name. In addition, users can use the command **pki key zeroize noconfirm** to disable all the prompt information on key pairs.

To delete the existing PKI key, in the global configuration mode, use the following command:

pki key zeroize {**default** | **label** *key-name*} [**noconfirm**]

- **default** | **label** *key-name* – Specifies the key that will be deleted. **Default** indicates the default-key. **Label** *key-name* indicates the key of the specified name.
- **noconfirm** – Disables prompt message on the key pair.

Configuring a PKI Trust Domain

A PKI trust domain contains all the necessary configuration information that is used to apply for a PKI local certificate, such as key pair, enrollment type, subject, etc. To configure a PKI trust domain, you need to enter the PKI trust domain configuration mode. In the global configuration mode, use the following command:

pki trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the PKI trust domain. This command creates a PKI trust domain with the specified name, and leads you into the PKI trust domain configuration mode; if the specified name exists, you will directly enter the PKI trust domain configuration mode.

To delete the specified PKI trust domain, in the global configuration mode, use the command **no pki trust-domain** *trust-domain-name*.

You can perform the following configurations in the PKI trust domain configuration mode:

- Specifying an enrollment type
- Specifying a key pair
- Configure subject content
- Adding the Subject Alternative Name
- Configuring a CRL

Specifying an Enrollment Type

To specify an enrollment type, in the PKI trust domain configuration mode, use the following command:

enrollment {**self** | **terminal**}

- **self** – Generates a self-signed certificate.
- **terminal** – Enrolls a certificate from a terminal (by cutting and pasting).

To cancel the enrollment type, in the PKI trust domain configuration mode, use the command **no enrollment**.



Notes:

- There is no default value for this command; therefore, you must use the command to specify an enrollment type.
- If the enrollment type is set to **self**, the self-signed certificate generated will contain the "SSL client authentication" or "SSL server authentication" property.

Specifying a Key Pair

To specify a key pair, in the PKI trust domain configuration mode, use the following command:

keypair *key-name*

- *key-name* – Specifies the name of the key pair.

To cancel the specified key pair, in the PKI trust domain configuration mode, use the command **no keypair**.

Configuring Subject Content

To specify subject content for the PIK trust domain, in the PKI trust domain configuration mode, use the following commands:

- Configure a common name: **subject commonName** *string*
- Configure a country (optional): **subject country** *string*



Notes: The name of the country can only contain two characters.

- Configure a locality (optional): **subject localityName** *string*
- Configure a state or province (optional): **subject stateOrProvinceName** *string*
- Configure an organization (optional): **subject organization** *string*
- Configure an organization unit (optional): **subject organizationUnit** *string*

To cancel the above configurations, in the PKI trust domain configuration mode, use the following commands:

- **no subject commonName**
- **no subject country**
- **no subject localityName**
- **no subject stateOrProvinceName**
- **no subject organization**
- **no subject organizationUnit**

Adding the Subject Alternative Name

You can add both the IP address and domain name to the Subject Alternative Name list.

To add the specified IP address to the Subject Alternative Name list, in the PKI trust domain configuration mode, use the following command:

subject-alt-name ip *ip-address*

- *ip-address* - Specifies the IP address to be added to the Subject Alternative Name list. Both IPv4 and IPv6 addresses are supported.

To remove the specified IP address from the Subject Alternative Name list, in the PKI trust domain configuration mode, use the following command:

no subject-alt-name ip *ip-address*

To add the specified domain name to the Subject Alternative Name list, in the PKI trust domain configuration mode, use the following command:

subject-alt-name dns *domain-name*

- *domain-name* - Specifies the domain name to be added to the Subject Alternative Name list. The value range is from 1 to 255 characters.

To remove the specified domain name from the Subject Alternative Name list, in the PKI trust domain configuration mode, use the following command:

no subject-alt-name dns *domain-name*

Configuring a CRL

CRL is used to help you check whether a certificate within its validity period has been revoked by the CA. To configure a CRL check, in the PKI trust domain configuration mode, use the following command:

crl {**nocheck** | **optional** | **required**}

- **nocheck** – StoneOS will not check the CRL. This is the default option.
- **optional** – StoneOS will still accept the peer's authentication even if the CRL is not available.
- **required** – StoneOS will not accept the peer’s authentication unless the CRL is available.

In addition, you can configure the URL that is used to retrieve the CRL information. The configuration needs to be performed in the CRL configuration mode. To enter the CRL configuration mode, in the PKI trust domain configuration mode, use the following command:

crl configure

To configure the URL that is used to retrieve CRL information, in the CRL configuration mode, use the following command:

url *index* {*url-http* | *url-ldap* [**username** *user-name* **password** *password* **auth-method** *auth-method*]} [**vrouter** *vrouter-name*]

- *index* – Specifies the URL index. StoneOS supports up to three URLs, and uses them by turn of URL1, URL2 and URL3.
- *url-http* – Specifies the HTTP URL that is used to retrieve CRL information. The URL entered should begin with http:// and the length is 1 to 255 characters.
- *url-ldap* – Specifies the LDAP URL that is used to retrieve CRL information. The URL entered should begin with ldap:// and the length is 1 to 255 characters.
- **username** *user-name* **password** *password* **auth-method** *auth-method* – Specifies the username (**username** *user-name*), password (**password** *password*) and authentication mode (**auth-method** *auth-method*) when the system is configured to retrieve CRL information via LDAP. If this parameter is not configured, the system will retrieve CRL information anonymously by default.
  - **username** *user-name* - Specifies the login DN of the LDAP server. The login DN is typically a user account with query privilege predefined in the LDAP server.
  - **password** *password* – Specifies the password for login DN.
  - **auth-method** *auth-method* - Specifies the authentication mode for the LDAP server. Plain text authentication (`plain`) is supported.

) when the system is configured to retrieve CRL information via LDAP. If this parameter is not configured, the system will retrieve CRL information anonymously by default.
- **vrouter** *vrouter-name* – Specifies the VRouter from which the CRL information is retrieved. The default value is the default VRouter (trust-vr).

Configuring Online Certificate Status Protocol

The Online Certificate Status Protocol (OCSP), having the same function as CRL, is used to obtain the revocation status of certificates. Compared with CRL, OCSP can online check the

status of certificates, thus providing more accurate result. You can configure CRL and OCSP simultaneously. If it fails to validate the certificate using either CRL or OCSP, the system will conclude that the certificate cannot be used.

In the PKI trust domain configuration mode, use the following command to make you check the certificate status using OCSP:

ocsp required

To disable this function, use the following command in the PKI trust domain configuration mode:

ocsp nocheck

To enter the OCSP configuration mode, use the following command in the PKI trust domain configuration mode:

ocsp configure

In the OCSP configuration mode, you can configure the following settings:

- Specifying the OCSP responder
- Configuring the random number for OCSP requests
- Specifying the invalidity time for OCSP response information

Specifying the OCSP Responder

To specify the OCSP responder, use the following command in the OCSP configuration mode:

url *url*

- *url* – Specifies the URL of the OCSP responder. The URL must begin with "http://".

To cancel the configurations, use the following command:

no url。

Configuring the Random Number for OCSP Requests

When the device sends OCSP requests, you can choose to add the random number to the requests, which improves the security between the device and the OCSP responder. By default,

the device adds the random number to the requests. To add random number, use the following command in the OCSP configuration mode:

nonce enable

To cancel the configurations, use the following command:

nonce disable

Specifying the Invalidity Time for OCSP Response Information

StoneOS provides the function of OCSP response information cache, which improves the efficiency of certificate verification. You can specify the invalidity time for the OCSP request information that is stored in the cache of the device and the OCSP request information will be deleted from the cache after the invalidity time reaches. To specify the invalidity time, use the following command in the OCSP configuration mode:

response-cache-refresh-interval *time*

- *time* - Specifies the invalidity time (in minutes) for the OCSP response information that stored in the cache. The value ranges from 0 to 1440. 0 represents the device will not store the OCSP response information. And when the device receives the request of certificate verification, it will send request to the OCSP responder to check the certificate status. When the specified value is between 1 and 1440, the invalidity time for stored OCSP response information is calculated by comparing the time of "current system time + time" with the time when the OCSP response information will be updated. The invalidity time is the one which is shorter.

In the OCSP configuration mode, use the following command to cancel the configurations:**no response-cache-refresh-interval**

After you cancel the configurations, the invalidity time for OCSP response information is the time when the OCSP response information will be updated. This is also the default settings.

Importing a CA Certificate

To import a CA certificate, in the global configuration mode, use the following command:

pki authenticate *trust-domain-name*

- *trust-domain-name* – Specifies the name of PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the CA certificate.

If ht enrollment type is to enroll a certificate from the register server, the CA certificate will be obtained via SCEP.



Notes: The system will check the validity of the imported certificate. "Subject Type=CA" needs to be included in the "Basic Constraints" field of the imported CA certificate.

Importing a Key

To import a key to the PKI trust domain, in the global configuration mode, use the following command:

pki key import {**rsa** | **dsa** | **sm2**} [**label** *label-name*]

- **rsa** – Specifies the RSA key imported to PKI.
- **dsa** – Specifies the DSA key imported to PKI.
- **sm2** – Specifies the SM2 key imported to PKI.
- *label-name* – Specifies the name of key pair. The name should be the unique in system. If the parameter is not specified, the default key Default-Key will be selected.

Importing a Key Pair

To import the key pair to the PKI trust domain, in the execution mode, use the following commands:

import pki key *key-name* **enc-key** *sig-key-name* **from** {**ftp server** *ip-address* [**vrouter** *VR-name*] [**user** *user-name* **password** *password*] *file-name* | **tftp server** *ip-address* [**vrouter** *VR-name*] *file-name*}

- *key-name* – Specifies the name of the imported key pair.
- **enc-key** – Specifies the key type as encryption key.
- *sig-key-name* – Specifies the signature key pair.
- **ftp** | **tftp** – Specifies the uploading method as FTP or TFTP.
- **server** *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **vrouter** *VR-name* - Specifies the name of VRouter.
- **user** *user-name* **password** *password* – Specifies the user name and password of the specified server.
- *file-name* – Specifies the name of locol encryption key pair file.

Generate a Certificate Request

After completing the PKI trust domain configuration, you need to generate a certificate request based on the content of the PKI trust domain, and then send the request to the CA server to enroll the corresponding local certificate. To generate a certificate request, in the global configuration mode, use the following command:

pki enroll *trust-domain-name*

- *trust-domain-name* – Specifies the name of the PKI trust domain to generate the corresponding certificate request.

Importing a Local Certificate

After obtaining a local certificate from the CA server, you need to import the local certificate to the device. To import a local certificate, in the global configuration mode, use the following command:

pki import *trust-domain-name* **certificate**

- *trust-domain-name* – Specifies the name of the PKI trust domain where the local certificate will be imported from.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the local certificate.

Obtaining a CRL

To obtain the CRL of the PKI trust domain, in the global configuration mode, use the following command:

pki crl request *trust-domain-name*

- *trust-domain-name* – Specifies the name of PKI trust domain. The system will obtain the current CRL based on CRL configuration in the specified PKI trust domain.

Importing/Exporting a PKI Trust Domain

To facilitate configuration, you can export a PKI trust zone's certificate (CA and local certificate) and the private key for the local certificate in PKSC12 format, and import them on another Hillstone device.

Exporting the PKI Trust Domain Information

To export the PKI trust domain information, in the global configuration mode, use the following command:

pki export *trust-domain-name* **pkcs12** *pass-phrase*

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *pass-phrase* – Specifies the passphrase that is used to decrypt PKCS12 data.

You can also export the PKI trust domain information in form of a file to an FTP server, TFTP server or USB disk via CLI.

To export the PKI trust domain information to an FTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- **pkcs12** *password* – Specifies the password used to decrypt the private key.
- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name for the exported file.

To export the PKI trust domain information to a TFTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to tftp server** *ip-address* [*file-name*]

To export the PKI trust domain information to a USB disk, in the execution mode, use the following command:

export pki *trust-domain-name* **pkcs12** *password* **to** {**usb0** | **usb1**} [*file-name*]

Importing the PKI Trust Domain Information

To import the PKI trust domain information, in the global configuration mode, use the following command:

pki import *trust-domain-name* **pkcs12** *pass-phrase*

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *pass-phrase* – Specifies the passphrase that is used to decrypt PKCS12 data.

After executing this command, the system will prompt the user to copy the content of the PKI trust domain to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the PKI trust domain.

You can also import the PKI trust domain information in form of a file from an FTP server, TFTP server or USB disk via CLI.

To import the PKI trust domain information from an FTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- **pkcs12** *password* – Specifies the password used to decrypt the private key.
- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password file-name* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the imported file.

To import the PKI trust domain information from a TFTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from tftp server** *ip-address file-name*

To import the PKI trust domain information from a USB disk, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **pkcs12** *password* **from** {**usb0** | **usb1**} *file-name*

Importing a Trust Certificate

If enabling Sandbox function, when importing a trust certificate of PE file, System will not detect the PE file. In the global configuration mode, use the following command to import a trust certificate:

import pki trusted-ca {**package** | **single**} **from** {**ftp server** *ip-address* [**vrouter** *VR-name*] [**user** *user-name* **password** *password*] *file-name* | **tftp server** *ip-address* [**vrouter** *VR-name*] *file-name*}

- **package** – Specifies the certificate package that you need to import.
- **single** – Specifies the single certificate that you need to import.
- **ftp** | **tftp** – Specifies the uploading method as FTP or TFTP.
- **server** *ip-address* – Specifies the FTP server IP or the TFTP server IP.
- **vrouter** *VR-name* - Specifies the VRouter name.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the username and password of the FTP server.

Exporting/Importing a Local Certificate

To facilitate configuration, you can export a PKI trust zone's local certificate, and import it on another Hillstone device.

Exporting a Local Certificate

To export a local certificate, in the global configuration mode, use the following command:

pki export *trust-domain-name* **certificate**

- *trust-domain-name* – Specifies the name of the PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to export the local certificate.

You can also export the local certificate in form of a file to an FTP server, TFTP server, or USB disk via CLI.

To export the local certificate to an FTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to ftp server** *ip-address* [**user** *user-name* **password** *password* [*file-name*] | *file-name*]

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *ip-address* – Specifies the IP address of the FTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the exported file.

To export the local certificate to a TFTP server, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to tftp server** *ip-address* [*file-name*]

To export the local certificate to a USB disk, in the execution mode, use the following command:

export pki *trust-domain-name* **cert to** {**usb0** | **usb1**} [*file-name*]

Importing a Local Certificate

To import a local certificate, in the global configuration mode, use the following command:

pki import *trust-domain-name* **certificate**

- *trust-domain-name* – Specifies the name of the PKI trust domain.

After executing this command, the system will prompt the user to copy the content of the certificate to the specified location. Press Enter, type a period (.), and then press Enter again. The system will begin to import the local certificate.

You can also import the local certificate in form of a file from an FTP server, TFTP server or USB disk via CLI.

To export the local certificate from an FTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from ftp server** *ip-address* {**user** *user-name* **password** *password file-name* | *file-name*}

- *trust-domain-name* – Specifies the name of the PKI trust domain.
- *ip-address* – Specifies the IP address of the FTP server.

- **user** *user-name* **password** *password file-name* – Specifies the username and password of the FTP server, and name of the imported file.
- *file-name* – Specifies the name of the exported file.

To export the local certificate from a TFTP server, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from tftp server** *ip-address file-name*

To export the local certificate from a USB disk, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cert from** {**usb0** | **usb1**} *file-name*

Importing Customized Certificate for HTTPS WebAuth

Importing Customized Certificate

When HTTPS mode is selected in Web authentication (WebAuth), the security certificate is usually not trusted by browser. You will need to click the Continue button to start Web authentication. In order to avoid this situation, you can purchase a local certificate signed by a certificate authority and import this certificate into a new PKI trust domain. Then you can import the trusted certificate by configuring this feature. The public key of CA certificate in the browser will authenticate the imported certificate signed by the private key of CA. Therefore, the situation that security certificate is trusted by browser of client will not occurs any more.

To configure importing customized certificate for HTTPS WebAuth, in the WebAuth configuration mode, use the following command:

https-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of the HTTPS trust domain. Before executing this command, this new PKI trust domain must have been added into StoneOS, and you should make sure that the local certificate purchased from the certificate authority has been imported

into it. By default, HTTPS trust domain is trust_domain_default, which will result in the untrusted certificate warning.



Notes: Make sure that the trusted CA certificate has been imported into PC’ s browser, , otherwise the browser will still prompt that security certificate is not being trusted.

In the WebAuth configuration mode, use **no https-trust-domain** to cancel the above configuration.

Viewing Importing Customized Certificate Information

To view information on imported customized certificate, in any mode, use the following command:

show webauth

Certificate Expiry Configurations

In order to ensure the validity of the user certificate and to avoid the problems caused by certificate expiry, the system provides the following solutions:

- For the certificate or CA certificate that will expire soon, the system will generate a log of the Warning level one week before the date of expiry;
- For the certificate or the CA certificate that have already expired, the system will generate a log of the Critical level everyday;
- For the self-signed certificate, the system provides a refreshing option to allow you to re-sign the certificate.

The system defines the validity period of a self-signed certificate is 10 years. To refresh the self-signed certificate and re-sign the certificate, in the global configuration mode, use following command:

pki refresh *trust-domain-name*

- *trust-domain-name* – Specifies the name of the PKI trust domain.

Viewing the PKI Configuration Information

To view the configuration information of key pair, in any mode, use the following command:

show pki key [**label** *key-name*] [**ssh-pubkey**]]

- **label** *key-name* – Shows the configuration information of the specified key pair. If the parameter is not specified, the command will show the configuration information of all the key pairs in the system.
- **ssh-pubkey** - Shows the public key of the specified key pair in the SSH format. Only the public key of the key pair of the RSA type in the SSH format can be displayed.

To view the configuration information of PKI trust domain, in any mode, use the following command:

show pki trust-domain [*trust-domain-name*]

- *trust-domain-name* – Shows the configuration information of the specified PKI trust domain. If the parameter is not specified, the command will show the configuration information of all the PKI trust domains in the system.

Configuring a Certificate Chain

A certificate chain consists of a root CA certificate, any intermediate CA certificates, and a CA-signed user certificate. Browsers consider that the certificate of the current user is valid and trusted only if each certificate in the certificate chain is valid. A root CA certificate lies in the top most position of the chain of trust hierarchy. Intermediate certificates branch off root certificates like branches of trees. They act as middle-men between the protected root certificates and the server certificates issued out to the public. There will always be at least one intermediate certificate in a chain, but there can be more than one.

Creating a Certificate Chain

To create a certificate chain, use the following command in global configuration mode:

pki cert-chain *cert-chain-name*

- *cert-chain-name* - Specifies the name of the certificate chain, which can be 1 to 31 characters. After the command is executed, the system generates a certificate chain with the specified name and enters the certificate chain configuration mode. If the specified name already exists, the system directly enters the certificate chain configuration mode.

To delete a specified certificate chain, use the following command in global configuration mode:

no pki cert-chain*cert-chain*

Importing a Certificate Chain

The system allows you to import certificate chain files from servers or by copying the certificate chain content. A certificate chain can contain at most 6 certificates. These certificates need to be able to complete a chain but there is no limitation on the order of these certificates.

To import a certificate chain file from the FTP, FTPS, or SFTP server, use the following command in execution mode:

import pki cert-chain *cert-chain-name* {**pkcs7** | **pkcs12-der** *password* | **cert-bundle**} **from** {**ftp** | **ftps** | **sftp server**} *ip-address* **vrouter** *vrouter-name* **user** *user-name* **password** *password file-name*

- *cert-chain-name* - Specifies the name of the certificate chain.
- **pkcs7** | **pkcs12-der** *password* | **cert-bundle** - Specifies the format of the certificate chain file, which can be PKCS#7, PKCS#12, or CERT-BUNDLE. The certificate chain file in the CERT-BUNDLE format is PEM-encoded. For certificate chain files in the PKCS#12 format, you need to specify the password of the files.
- *ip-address* - Specifies the address of the FTP, FTPS, or SFTP server.
- **vrouter** *vrouter-name* - Specifies the name of the virtual router.
- **user** *user-name* **password** *password*- Specifies the username and password used to access the server.
- *file-name* - Specifies the name of the certificate chain file.

To import a certificate chain file from the TFTP server, use the following command in execution mode:

import pki cert-chain *cert-chain-name* {**pkcs7** | **pkcs12-der** *password* | **cert-bundle**} **from tftp server** *ip-address* **vrouter** *vrouter-name file-name*

To import a certificate chain file by copying the certificate chain content, use the following command in global configuration mode:

pki import cert-chain *cert-chain-name* {**pkcs7** | **cert-bundle**}

After the command is executed, copy the certificate chain file content as prompted and enter "." on a new line to end the input.

Exporting a Certificate Chain

The system allows you to export a certificate chain file to a specified server or display the certificate chain content on the endpoint.

To export a certificate chain file to a server, use the following command in execution mode:

export pki cert-chain *cert-chain-name* {**pkcs7** | **pkcs12-der** *password* } **to** {**ftp** | **ftps** | **sftp server**} *ip-address* **vrouter** *vrouter-name* **user** *user-name* **password** *password file-name*

To export a certificate chain file and display the file content on the endpoint, use the following command in global configuration mode:

pki export cert-chain *cert-chain-name*

Viewing Certificate Chain Information

To view configuration information about a specified certificate chain, use the following command in any mode:

show pki cert-chain *cert-chain-name*

To view configuration information about all certificate chains, use the following command in any mode:

show pki cert-chain

To view information about certificates in a specified certificate chain, use the following command in any mode:

show pki cert-chain *cert-chain-name***cert** *subject-name*

- cert-chain-name - Specifies the name of the certificate chain.
- subject-name - Specifies the subject name of the certificate.

Configuring Certificate Validity Check

Enabling/Disabling Certificate Validity Check

Certificate validity check is effective for all certificates in the certificate chain and certificates in the trusted domain. By default, certificate validity check is enabled. To disable certificate validity check, use the following command in global configuration mode:

pki cert-validity-check disable

To enable certificate validity check, use the following command in global configuration mode:

pki cert-validity-check enable

Configuring Certificate Validity Check

By default, the system sends an alarm per day a week before the certificate expires. When the certificate expires, the system records an event log at critical level.

To configure check interval of certificate validity and warning days before certificate expiration, use the following command in global configuration mode:

pki cert-validity-check {**interval** *value* | **pre-warning-time** *time*}

- **interval** *value* - Specifies the check interval of certificate validity. Valid values: 1 to 100, in hours. Default value: 24.
- **pre-warning-time** *time* - Specifies the warning days before certificate expiration. Valid values: 1 to 1000, in hours. Default value: 168.

Viewing Check Configuration and Check Result of Certificate Validity

To view the configuration of certificate validity check, use the following command in any mode:

show pki cert-validity-check

The last check result is displayed in the command output:

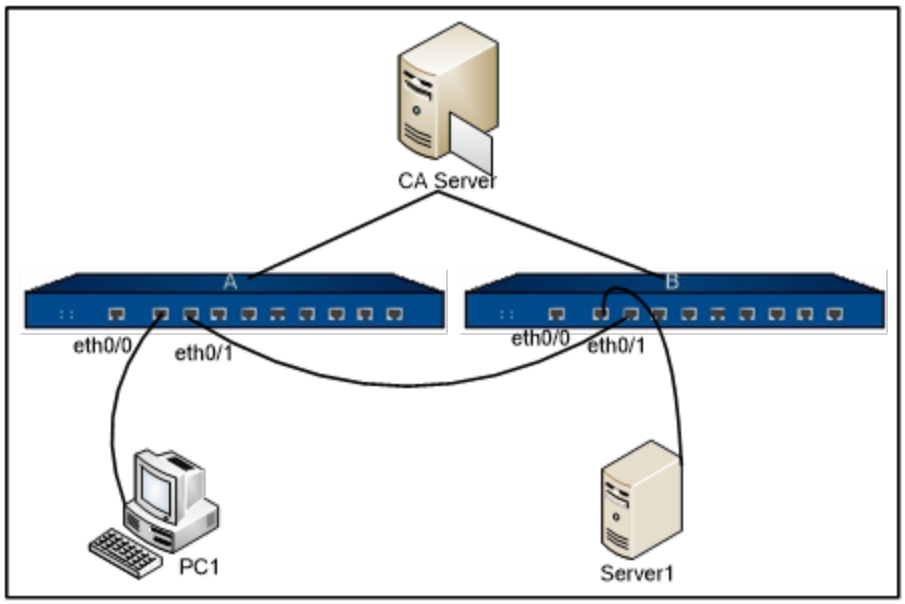
- not checked yet: The check is not started.
- valid: The certificate is valid.
- expired: The certificate has expired.
- null cert: The certificate is not imported in the trusted domain or certificate chain because no certificate exists.

Example for Configuring IKE

This section describes an example of creating a security alliance by IKE. The authentication policy of IKE adopts PKI certificate system.

Requirement

The goal is to create a secure tunnel between Hillstone Device A and Hillstone Device B. PC1 is used as the host of Hillstone Device A, whose IP address is 10.1.1.1, and the gateway address is 10.1.1.2; Server1 is used as the server of Hillstone Device B, whose IP address is 192.168.1.1, and the gateway address is 192.168.1.2. The requirement is: protecting the traffic between the subnet represented by PC1 (10.1.1.0/24) and the subnet represented by server1 (192.168.1.0/24). The authentication policy adopts PKI certificate system, using security protocol ESP and encryption algorithm 3DES, and the Hash algorithm is SHA1. The networking topology is shown in the figure below:



Configuration Steps

Step 1: Configure Hillstone devices' interfaces

Hillstone Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

Hillstone Device B

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

Step 2: Configure policy rules

Hillstone Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Hillstone Device B

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 3: Configure Phase1 proposal

Hillstone Device A

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication rsa-sig
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Hillstone Device B

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication rsa-sig
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Step 4: Configure PKI

Hillstone Device A

Generate a key pair

```
hostname(config)# pki key generate rsa label 111 modulus 1024
Configure a PKI trust domain
hostname(config)# pki trust-domain td1
hostname(config-trust-domain)# keypair 111
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# subject commonName aa
hostname(config-trust-domain)# subject country cn
hostname(config-trust-domain)# subject stateOrProvinceName bj
```

```
hostname(config-trust-domain)# subject localityName hd
hostname(config-trust-domain)# subject organization hillstone
hostname(config-trust-domain)# subject organizationunit rd
hostname(config-trust-domain)# exit
Generate a certificate request and send it to the CA
server to enroll local certificate
hostname(config)# pki enroll td1
Authenticate the CA certificate
hostname(config)# pki authenticate td1
Import a local certificate
hostname(config)# pki import td1 certificate
```

Hillstone Device B

```
Generate a key pair
hostname(config)# pki key generate rsa label 222 modulus 1024
Configure a PKI trust domain
hostname(config)# pki trust-domain td2
hostname(config-trust-domain)# keypair 222
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# subject commonName aa
hostname(config-trust-domain)# subject country cn
hostname(config-trust-domain)# subject stateOrProvinceName bj
hostname(config-trust-domain)# subject localityName hd
hostname(config-trust-domain)# subject organization hillstone
hostname(config-trust-domain)# subject organizationunit rd
hostname(config-trust-domain)# exit
Generate a certificate request and send it to the CA
server to enroll local certificate
```

```
hostname(config)# pki enroll td2
```

Authenticate the CA certificate

```
hostname(config)# pki authenticate td2
```

Import a local certificate

```
hostname(config)# pki import td2 certificate
```

Step 5: Configure ISAKMP gateways

Hillstone Device A

```
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
hostname(config-isakmp-peer)# local-id asn1dn
hostname(config-isakmp-peer)# peer-id asn1dn CN=-
bb,OU=rd,O=hillstone,L=hd,ST=bj,C=cn
hostname(config-isakmp-peer)# trust-domain td1
hostname(config-isakmp-peer)# exit
```

Hillstone Device B

```
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# local-id asn1dn
hostname(config-isakmp-peer)# peer-id asn1dn CN=aa,O-
OU=rd,O=hillstone,L=hd,ST=bj,C=cn
hostname(config-isakmp-peer)# trust-domain td2
hostname(config-isakmp-peer)# exit
```

Step 6: Configure Phase2 proposal

Hillstone Device A

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
```

Hillstone Device B

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
```

Step 7: Configure a tunnel named VPN

Hillstone Device A

```
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

Hillstone Device B

```
hostname(config)# tunnel ipsec vpn auto
```

```
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

Step 8: Configure routes

Hillstone Device A

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Hillstone Device B

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Chapter 9 VPN

This chapter introduces the following topics:

- IPSec Protocol
- SSL VPN
- Dial-up VPN
- PnPVPN
- GRE Protocol
- L2TP Protocol
- VXLAN

IPsec Protocol

Overview

IPsec is a widely used protocol suite for establishing VPN tunnel. IPsec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPsec protocol defines how to choose the security protocols and algorithms, as well as the method of exchanging security keys among communication peers, offering the upper layer protocols with network security services including access control, data source authentication and data encryption, etc.

- Authentication Header (AH): AH is a member of the IPsec protocol suite. AH guarantees connectionless integrity and data source verification of IP packets, and furthermore, it protects against replay attacks. AH can provide sufficient authentications for IP headers and upper-layer protocols.
- Encapsulating Security Payload (ESP): ESP is a member of the IPsec protocol suite. ESP provides encryption for confidential data and implements data integrity check of IPsec ESP data in order to guarantee confidentiality and integrity. Both ESP and AH can provide service of confidentiality (encryption), and the key difference between them is the coverage.
- Internet Key Exchange (IKE): IKE is used to negotiate the AH and ESP password algorithm and put the necessary key of the algorithm to the right place.



Notes: The Russia version does not support the IPsec protocol and the related IPsec VPN function.

Security Association

IPsec provides encrypted communication between two peers which are known as IPsec ISAKMP gateways. Security Association (SA) is the basis and essence of IPsec. SA defines some factors of

communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the life-time of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

Establishing a SA

You can establish a SA in two ways: manual and IKE auto negotiation (ISAKMP).

Manually configuring a SA is complicated as all the information will be configured by yourself and some advanced features of IPsec are not supported (e.g. timed refreshing), but the advantage is that the manually configured SA can independently fulfill IPsec features without relying on IKE. This method applies to the condition of a small number of devices, or the environment of static IP addresses.

IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining a SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates an IPsec SA using the established ISAKMP. Establishing a SA in two phases can speed up key exchanging.

Phase 1 SA

The Phase 1 SA refers to the Security Association for establishing the channel. The negotiation procedure is:

1. Parameter configuration, including:
    - Authentication method: Pre-shared key or digital signature
    - Diffie-Hellman group selection

2. Policy negotiation, including:

    - Encryption algorithm: DES, 3DES, AES-128, AES-192 or AES-256
    - Hash algorithm: MD5, SHA-1 or SHA-2

3. DH exchange. Although it is known as key exchange, actually the two hosts will not exchange any real key at any time during the communication, and instead they only exchange the basic element information that is used by the DH algorithm to generate shared key. The DH exchange can be either open to the public or protected. After exchanging elements for generating the key, the two hosts of the both ends can generate the identical shared master key respectively to protect the authentication process hereafter.

4. Authentication. The DH exchange needs to be further authenticated. If the authentication fails, the communications will not continue. The master key, along with the negotiation algorithm specified in the Phase 1, will be used for authentication of the communication entities and communication channel. During this procedure, the entire payload that will be authenticated, including the entity type, port number and protocol, will be protected by the previously generated master key to assure the confidentiality and integrity.

Phase 2 SA

The Phase 2 SA, a fast SA, refers to the Security Association established for data transmission. This phase will negotiate to establish an IPsec SA, and provide IPsec service for data exchange. The negotiation messages in Phase 2 are protected by the Phase 1 SA, and any message that is not protected by the Phase 1 SA will be rejected. The Phase 2 negotiation (fast negotiation mode) procedure is:

1. Policy negotiation. The peers exchange protection requirements:

    - IPsec protocol: AH or ESP
    - Hash algorithm: MD5, SHA-1, SHA-2 or NULL

- Encryption: DES, 3DES, AES-128, AES-192, AES-256 or NULL
- Compression algorithm: DEFLATE
- After the above four requirements reach an agreement, two SAs will be established and used for inbound and outbound communications respectively.

2. Refreshing or exchanging session key elements.
   In this step, the session key for IP packet encryption will be generated through DH exchange.
3. Submitting the SA to the IPsec driver.
   During the Phase 2 negotiation process, if the response is timeout, then the system will automatically retry the Phase 2 SA negotiation.

Hash Algorithm

Both AH and ESP can verify the integrity of IP packets, and determine whether the packets have been tampered during transmission. The verification algorithm is mainly implemented by the hash function. The hash function can accept a message input of random length, and produces an output of fixed length. The output is known as the message digest. IPsec peers will compute the message digest. If the two digests are identical, the message proves to be complete and not having been tampered. In general IPsec adopts the following Hash algorithms:

- MD5: Use message input of a random length to produces a 128-bit message digest.
- SHA-1: Use a message with a length less than 264 bits to produce a 160-bit message digest. The digest of SHA-1 is longer than that of MD5, so it is more secure.
- SHA-2: Consists of SHA-256, SHA-384 and SHA-512. This algorithm can produce a longer message digest. For SHA-256, a message input with a length less than 264 bits can produce a 256-bit message digest; for SHA-384, a message input with a length less than 2128 bits produces a 384-bit message digest; for SHA-512, a message input with a length less than 2128 bits produces a 512-bit message digest.

Encryption Algorithm

ESP can provide encryption protection for the content of IP packets, and prevent against sniffing during the transmission. The encryption algorithm is implemented mainly through symmetric key system which uses the same key to encrypt and decrypt data. StoneOS supports 3 encryption algorithms:

- DES (Data Encryption Standard): Uses a 56-bit key to encrypt each 64-bit plain text block.
- 3DES (Triple DES): Uses three 56-bit DES keys (168 bits in total) to encrypt plain text.
- AES (Advanced Encryption Standard): StoneOS supports AES algorithms of 128-bit, 192-bit and 256-bit keys.

Compression Algorithm

IPComp (IP Payload Compression) is a protocol designed to reduce the length of IP datagram. This protocol compresses the IP datagram payload by different compression algorithms, and achieves the effect of transmitting data of heavy payload under the conditions of low bandwidth.

The prerequisite for a successful IPComp communication is to establish an IPComp Association (IPCA) between the two ends of the communication. The association includes all the information needed for IPComp operation, such as the compression algorithm and the parameters for the compression algorithm. When compressing the network data stream of IPsec by IPComp, you can create an IPCA manually or by dynamic negotiation. For the dynamic negotiation approach, ISAKMP gateway offers all the mechanisms necessary for establishing the IPCA. The IPsec function of Hillstone devices provides the following IPComp compression algorithm:

- DEFLATE: A free lossless compression algorithm that can be implemented in IPComp, adopts LZ77 algorithm and Huffman decoding.

References

The IPsec function of Hillstone devices follows the IPsec protocol specifications defined in RFC. For more detailed information about IPsec Protocol, see the relevant sections of the RFC

documents below:

- Security Architecture for the Internet Protocol: RFC2401/RFC4301
- ESP: RFC2406/RFC4303
- AH: RFC2402/RFC4302
- Encryption algorithm: RFC2410 (Null Encryption), RFC2405 (DES-CBC), RFC2451 (3DES-CBC) and RFC3602 (AES-CBC)
- Hash algorithm: FIPS180-2 (SHA), RFC2404 (SHA-1), RFC4868 (SHA-2) and RFC2403 (MD5)
- Compression algorithm: RFC2393 (IPComp) and RFC2394 (DEFLATE)

Applying an IPsec VPN

You can apply the configured VPN tunnels to Hillstone devices through the policy-based VPN and route-based VPN to assure the security of traffic encryption and decryption.

- Policy-based VPN: Applies a configured VPN tunnel in a policy rule, and only permits the matched traffic to pass through the VPN tunnel.
- Route-based VPN: Bind the configured VPN tunnel to a tunnel interface; when configuring the static route, you need to specify the tunnel interface as the next-hop route.

Configuring an IPsec VPN

You can configure IPsec VPN in two ways:

- Manual key VPN
- IKE VPN. The system supports both IKEv1 and IKEv2.

Improving the Decrypting Performance of IPSec VPN

This feature is only supported for CloudEdge. When more than 2 vCPUs are used, you can enable the function to improve the decrypting performance of IPSec VPN as needed. After it is enabled, system will decrypt the packet with multi-core decryption technology, which will also increase the throughput of device. To improve the decrypting performance of IPSec VPN, in the global configuration mode, use the following command:

tunnel-core-unbind

In the global configuration mode, use the command **no tunnel-core-unbind** to restore the default configuration.

Improving the New Session Processing Performance of IPSec VPN

You can configure the function to improve the new session processing performance of IPSec VPN as needed. After this function is configured, system will adopt multi-core and multi-processor technology for VPN negotiation.

Configuring the Number of CPU Cores Used By the System Data Plane

To improve the new session processing performance of IPSec VPN, you need to configure the number of CPU cores used by the system data plane first. After the configuration, The number of VPN processor is the total number of system CPU cores minus the number of CPU cores used by the system data plane. To configure the number of CPU cores used by the system data plane, in the global configuration mode, use the following command:

flow-core-num *number*

- *number* - Specifies the number of CPU cores used by the system data plane. The range is max_core_number/2 to max_core_number, max_core_number is the total number of system CPU cores. After configuration, the formula is: number of VPN processor = max_core_number (the total number of system CPU cores) - flow-core-number (the number of CPU cores used by the system data plane).

In the global configuration mode, use the command **no flow-core-num** to cancel the configuration.

Enabling/Disabling the VPN Multi-Process Function

By default, the VPN multi-process function is disabled. To enable or disable this function, in the global configuration mode, use the following command:

- Enable:**cp-multi-cores vpnd**
- Disable:**no cp-multi-cores vpnd**



Notes:

- After configuring the number of CPU cores used by the system data plane or canceling the number already configured, you must reboot the device to make the configuration take effect.
- After enabling /disabling the VPN multi-process function, you must reboot the device to make the configuration take effect.
- You need to configure both "Configuring the Number of CPU Cores Used By the System Data Plane and "Enable VPN multi-process function", and after restarting the device, the VPN multi-process function can be fully enabled.
- This function supports IKEv1 VPN, Dial-up VPN, PnPVPN and XAUTH.
- SG-6000-X8180 and devices with less than or equal to two CPU cores do not support this function.

The asynchronous mode of IPSec

The IPSec asynchronous mode applies to platforms (X8180 and A-series) that integrate hardware accelerators. IPSec encryption and decryption support asynchronous mode, where data encryption and decryption are accelerated, and IPSec throughput performance is improved through hardware accelerators.

Enabling/Disabling the asynchronous mode of IPSec

The asynchronous mode of IPSec is enabled by default . In the global configuration mode, use the following commands to enable or disable this function:

- Enableing IPSec asynchronous mode: **no ipsec-async-crypto-disable**
- Disableing IPSec asynchronous mode: **ipsec-async-crypto-disable**

Viewing the Information of the Hardware Accelerator

To view the information and algorithms of the hardware accelerator supported by the system, use the following command in any mode:

show dp-dpdk-crypto-device



Notes: If the hardware accelerator is occupied by other functions (such as SSL Proxy), the content of "device Status" changes to "device Status: disable(crypto is used by other Module)".

View Statistics on Encryption and Decryption Queues

To view statistics for encryption and decryption queues, use the following commands in any mode:

show ipsec-async-crypto statistic [*tunnel_id*] [*clear*]

- **show ipsec-async-crypto statistic**: Displays the statistics of the IPSec encryption and decryption queues of the device in asynchronous mode.
- *tunnel_id*: Specifies the tunnel ID number. The system displays the the statistics of the IPSec encryption and decryption queue of the specified tunnel.
- *clear*: Displays the statistics of the IPSec encryption and decryption queues of the device or the specified tunnel, and then clear the statistics.

Manual Key VPN

The configuration options of manual key VPN include the operation mode of IPsec protocol, SPI, protocol type, encryption algorithm, hash algorithm and compression algorithm.

Creating a Manual Key VPN

To create a manual key VPN, in the global configuration mode, use the following command:

tunnel ipsec *name* **manual**

- *name* – Specifies the name of the manual key VPN tunnel that will be created.

After executing the above command, the CLI is in the manual key VPN configuration mode. You need to configure all the parameters of the manual key VPN in this mode.

To delete the specified manual key VPN, in the global configuration mode, use the following command:

no tunnel ipsec *name* **manual**

Specifying the Encapsulation Mode of IPsec Protocol

To specify the encapsulation mode of IPsec protocol (either transport mode or tunnel mode), in the manual key VPN configuration mode, use the following command:

mode {**transport** | **tunnel**}

- **transport** – Specifies the encapsulation mode of IPsec protocol as transport.
- **tunnel** – Specifies the encapsulation mode of IPsec protocol as tunnel. This is the default mode.

To restore to the default mode, in the manual key VPN configuration mode, use the command **no mode**.

Specifying a SPI

SPI (Security Parameter Index) is a unique 32-bit identifier generated by SA and transmitted in the AH and ESP header. SPI is used to find the corresponding VPN tunnel for decryption. To specify a SPI, in the manual key VPN configuration mode, use the following command:

spi *spi-number out-spi-number*

- *spi-number* – Specifies the local SPI.
- *out-spi-number* – Specifies the remote SPI.

To cancel the SPI, in the manual key VPN configuration mode, use the command **no spi**.

When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.

Specifying a Protocol Type

The IPsec protocol types include ESP and AH. To specify the protocol type for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

protocol {**esp** | **ah**}

- **esp** – Uses ESP. This is the default protocol type.
- **ah** – Uses AH.

To restore to the default protocol type, in the manual key VPN configuration mode, use the command **no protocol**.

Specifying an Encryption Algorithm

To specify an encryption algorithm for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **null**}

- **3des** – Uses the 3DES encryption. The key length is 192-bit. This is the default algorithm.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.

- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.
- **null** – No encryption.

To restore to the default encryption algorithm, in the manual key VPN configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

To specify a hash algorithm for the manual key VPN tunnel, in the manual key VPN configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**}

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.
- **null** – No hash algorithm.

To restore to the default hash algorithm, in the manual key VPN configuration mode, use the command **no hash**.

Specifying a Compression Algorithm

By default, the manual key VPN does not use any compression algorithm. To specify a compression algorithm (DEFLATE for the manual key VPN tunnel), in the manual key VPN configuration mode, use the following command:

compression deflate

To cancel the specified compression algorithm, in the manual key VPN configuration mode, use the command **no compression**.

Specifying a Peer IP Address

To specify a peer IP address, in the manual key VPN configuration mode, use the following command:

peer *ip-address*

- *ip-address* – Specifies the IP address of the peer.

To cancel the specified peer IP address, in the manual key VPN configuration mode, use the command **no peer**.

Configuring a Hash Key for the Protocol

You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the peer's inbound hash key. To configure a hash key, in the manual key VPN configuration mode, use the following command:

hash-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – Configures the local inbound hash key.
- **outbound** *hex-number-string* – Configures the local outbound hash key.

To cancel the specified hash key, in the manual key VPN configuration mode, use the command **no hash-key**.

Configuring an Encryption Key for the Protocol

You should configure the keys of both ends of the tunnel. The local inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key. To configure an encryption key for the protocol, in the manual key VPN configuration mode, use the following command:

encryption-key inbound *hex-number-string* **outbound** *hex-number-string*

- **inbound** *hex-number-string* – Configures the local inbound encryption key.
- **outbound** *hex-number-string* – Configures the local outbound encryption key.

To cancel the specified encryption key, in the manual key VPN configuration mode, use the command **no encryption-key**.

Specifying an Egress Interface

To specify an egress interface, in the manual key VPN configuration mode, use the following command:

- **interface** *interface-name*
- **interface-name** – Specifies the name of the egress interface.

To cancel the specified egress interface, in the manual key VPN configuration mode, use the command **no interface**.



Notes: The egress interface in the non-root VSYS cannot be the VSYS shared interface.

IKEv1 VPN

The configurations of IKEv1 VPN include:

- Configuring a P1 proposal
- Configuring an ISAKMP gateway
- Configuring a P2 proposal
- Configuring the smart link
- Configuring a tunnel

Configuring a P1 Proposal

P1 proposal is the IKE security proposal that can be applied to the ISAKMP gateway, and is used in the Phase 1 SA. The configurations of IKE security proposal include specifying an authentication method, encryption algorithm, hash algorithm and lifetime of SA and DH group.

Creating a P1 Proposal

To create a P1 proposal, i.e., an IKE security proposal, in the global configuration mode, use the following command:

isakmp proposal *p1-name*

- *p1-name* – Specifies the name of the P1 proposal that will be created. After executing the command, the CLI will enter the P1 proposal configuration mode. You can configure parameters for P1 proposal in this mode.

To delete the specified P1 proposal, in the global configuration mode, use the command **no isakmp proposal** *p1-name*.

Specifying an Authentication Method

Specify the method of IKE identity authentication. Identity authentication is used to confirm the identities of both the ends during the communication. There are two methods: pre-shared key authentication and digital signature authentication. For the pre-shared key authentication, the authentication string is used as an input to generate a key, and different authentication strings will definitely generate different keys. In the non-root VSYS, only the pre-share key authentication mode is supported. To specify the authentication method of IKE security proposal, in the P1 proposal configuration mode, use the following command:

authentication {**pre-share** | **rsa-sig** | **dsa-sig** |**ecdsa-sig** | **gm-de** }

- **pre-share** – Uses the pre-shared key authentication. This is the default method.
- **rsa-sig** – Uses the RSA digital signature authentication.
- **dsa-sig** – Uses the DSA digital signature authentication. The corresponding Hash algorithm can only be SHA-1.
- **ecdsa-sig** – Uses the ECDSA digital signature authentication. When the authentication mode is selected, only encryption algorithm SM1 and SM4 are not supported and verification algorithm SHA-256, SHA-384 or SHA-512 are supported.

- **gm-de** – Uses the envelope authentication mode. When the authentication mode is selected, only encryption algorithm SM1 and SM4 are supported and verification algorithm SHA or SM3 are supported.

To restore to the default authentication method, in the P1 proposal configuration mode, use the command **no authentication**.

Specifying an Encryption Algorithm

StoneOS provides the following five encryption algorithms: 3DES, DES, 128bit AES, 192-bit AES and 256-bit AES. To specify the encryption algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** | **sm1** | **sm4**}

- **3des** – Uses the 3DES encryption. The key length is 192 bits. This is the default algorithm for StoneOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.
- **sm1** – Uses the SM1 block cipher algorithm. The key length is 128 bits.
- **sm4** – Uses the SM4 block cipher algorithm. The key length is 128 bits.

To restore to the default encryption algorithm, in the P1 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

StoneOS supports the following hash algorithms: MD5, SHA-1 and SHA-2 (including SHA-256, SHA-384 and SHA-512). To specify the hash algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**}

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.
- **sm3** – Uses the SM3 hash algorithm. The digest length is 256 bits. The algorithm can be used in the digital signature and verification, generating message verification code and other application scenarios.

To restore to the default hash algorithm, in the P1 proposal configuration mode, use the command **no hash**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. The longer the key element is, the more secure the generated key will be, and the more difficult it will be to decrypt it. The selection of DH group is important, because the DH Group is only determined in the Phase 1 SA negotiation, and the Phase 2 negotiation will not re-select a DH group. The two phases use the same DH group; therefore the selection of DH group will have an impact on the keys generated for all sessions. During negotiation, the two ISAKMP gateways should select the same DH group, i.e., the length of key element should be equal. If the DH groups do not match, the negotiation will fail.

To select a DH group, in the P1 proposal configuration mode, use the following command:

group {1 | 2 | 5 | 14 | 15 |16| 18 | 19 | 20 | 21 | 24}

- **1** – Selects DH Group1. The key length is 768 bits（MODP Group）.
- **2** – Selects DH Group2. The key length is 1024 bits（MODP Group）.This is the default value.
- **5** – Selects DH Group5. The key length is 1536 bits（MODP Group）.
- **14** – Selects DH Group14. The key length is 2048 bits（MODP Group）.
- **15** – Selects DH Group15. The key length is 3072 bits（MODP Group）.
- **16** – Selects DH Group16. The key length is 4096 bits（MODP Group）.
- **18** – Selects DH Group18. The key length is 8192 bits（MODP Group）.
- **19** – Select DH Group 19. The key length is 256 bits (ECP Group).
- **20** – Select DH Group 20. The key length is 384 bits (ECP Group).
- **21** – Select DH Group 21. The key length is 521 bits (ECP Group).
- **24** – Select DH Group 24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

When configuring PFS in the P2 proposal, you can also select the DH group.

Specify the Lifetime of SA

The Phase 1 SA is configured with a default lifetime. When the SA lifetime expires, the device will send an SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation. To specify the lifetime of SA, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400.

To restore to the default lifetime, in the P1 proposal configuration mode, use the command **no lifetime**.

Configuring an ISAKMP Gateway

After creating an ISAKMP gateway, you can configure the IKE negotiation mode, IP address and type of the ISAKMP gateway, IKE security proposal, pre-shared key, PKI trust zone, local ID, ISAKMP gateway ID, ISAKMP connection type, NAT traversal, etc.

Creating an ISAKMP Gateway

To create an ISAKMP gateway, in the global configuration mode, use the following command:

isakmp peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

After executing the command, the CLI will enter the ISAKMP gateway configuration mode. You can configure parameters for the ISAKMP gateway in this mode.

To delete the specified ISAKMP gateway, in the global configuration mode, use the command **no isakmp peer** *peer-name*.

Binding an Interface to the ISAKMP Gateway

To bind an interface to the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the binding interface.

To cancel the binding, in the ISAKMP gateway configuration mode, use the command **no interface** *interface-name*.

Configuring an IKE Negotiation Mode

The IKE negotiation consists of two modes: the main mode and aggressive mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation that the IP address of the center device is static and the IP address of client device is dynamic. To configure the IKE negotiations mode, in the ISAKMP gateway configuration mode, use the following command:

mode {**main** | **aggressive**}

- **main** – Uses the main mode, and provides ID protection. This is the default mode.
- **aggressive** – Uses the aggressive mode.

To restore to the default negotiations mode, in the ISAKMP gateway configuration mode, use the command **no mode**.

Configuring the Custom IKE Negotiation Port

You can configure a custom UDP port for IKE negotiation, and establish the IPSec connection. To configure a custom IKE negotiation port, in the ISAKMP gateway configuration mode, use the following command:

ipsec-over-udp port *port-number*

- *port-number* – Specifie the UDP port number, the range is 1 to 65535. To avoid port number conflicts, you are advised to use port numbers ranging from 1024 to 65535.

To cancel the configuration, in the ISAKMP gateway configuration mode, use the command **no ipsec-over-udp**.

Configuring the Custom IKE Negotiation Port Pool

You can configure a custom port pool for IKE negotiation. When the first packet negotiation over port 500 or 4500 is failed, the system can use the port in the custom port pool for IKE negotiation and establish an IPSec connection.

To configure a custom IKE negotiation port pool, you need to enter the IKE port pool configuration mode. To enter the IKE port pool configuration mode, in the global configuration mode, use the following command:

ike-port-pool

To delete the custom IKE negotiation port pool, in the global configuration mode, use the command **no ike-port-pool**.

To configure a port range for the custom IKE negotiation port pool, in the IKE port pool configuration mode, use the following command:

port-range min *min_port* **max** *max_port*

- **min** *min_port* **max** *max_port*- Specifies the minimum port number and maximum port number of the port range. The value range is 1024 to 65535.

Repeat the above commands to configure multiple port ranges. You can configure up to 120 port ranges.

To delete the specified port range, in the IKE port pool configuration mode, use the command **no port-range min** *min_port* **max** *max_port*.



Notes:

- VPN can use the ports in the custom IKE negotiation port pool for IKE negotiation after the port pool is bound to the ISAKMP gateway. For how to bind the custom IKE negotiation port pool, see Binding the Custom IKE Negotiation Port Pool.
- After configuring the custom IKE negotiation port pool function, it is recommended to configure the DPD (Dead Peer Detection) fuction or the VPN Track function at the same time. If port 500 or 4500 is disabled, the system will disconnect the old VPN connection and continue to use port 500 or 4500 to initiate the IKE negotiation. If the first packet negotiation fails, the system will use the port in the custom port pool for IKE negotiation.

- If the successfully negotiated VPN port is disabled, the VPN connection will be disconnected for at least 1 minute between disconnecting the old VPN connection and renegotiating using the port in the custom port pool.
- It is recommended that you configure the custom IKE negociation port function and the custom IKE negotiation port pool function separately.

Binding the Custom IKE Negotiation Port Pool

VPN can use the ports in the custom IKE negotiation port pool for IKE negotiation after the port pool is bound to the ISAKMP gateway.

To bind the custom IKE negotiation port pool, in the ISAKMP gateway configuration mode, use the following command:

bind ike-port-pool

To cancel the binding, in the ISAKMP gateway configuration mode, use the command **no bind ike-port-pool**.

Specifying the IP Address and Peer Type

You can specify the IP address and address type (static or dynamic) for the peer of the created ISAKMP gateway. To specify the IP address and the type of the peer, in the ISAKMP gateway configuration mode, use the following command:

type {**dynamic** | **static**}

- **dynamic** – Specifies the dynamic IP address.
- **static** – Specifies the static IP address. This is the default option.

To restore to the default type, in the ISAKMP gateway configuration mode, use the command **no type**.

peer *ip-address*

- *ip-address* - Specifies the IP address or the host name of the peer. This parameter is only valid when the IP address of the peer is static.

To cancel the IP address or the host name, in the ISAKMP gateway configuration mode, use the command **no peer**.

Accepting the Peer ID

To make the ISAKMP gateway accept any peer ID without check, in the ISAKMP gateway configuration mode, use the following command:

accept-all-peer-id

To disable the function, use the command **no accept-all-peer-id**.

Specifying a P1 Proposal

To specify the P1 proposal for the ISAKMP gateway, in ISAKMP the gateway configuration mode, use the following command:

isakmp-proposal p1-proposal1 [p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – Specifies the name of the P1 proposal. You can specify up to four P1 proposals for the ISAKMP gateway.

To cancel the specified P1 proposal, in ISAKMP the gateway configuration mode, use the command **no isakmp-proposal**.

Configuring a Pre-shared Key

If the pre-shared key authentication method is used, you need to specify a pre-shared key. To specify the pre-shared key for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

pre-share *string*

- *string* – Specifies the content of the pre-shared key.

To cancel the specified pre-shared key, in the ISAKMP gateway configuration mode, use the command **no pre-share**.

Configuring a PKI Trust Domain

If the digital signature authentication mode is used, you need to specify a PKI trust domain for the digital signature. To specify the PKI trust domain for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

trust-domain *string*

- *string* – Specifies the PKI trust domain.

To cancel the specified PKI trust domain, in the ISAKMP gateway configuration mode, use the command **no trust-domain**.



Tip: For more information about how to configure a PKI trust domain, see "PKI" in the "User Authentication".

Configuring the Trust Domain of Peer Certificate

The peer certificate is used for encrypting and authenticating data in the negotiation. The initiator of VPN connection should import the peer certificate first. The command is supported only in the GM 1.0 version. To configure the trust domain of peer certificate , in the ISAKMP gateway configuration mode, use the following command:

remote-trust-domain *string*

- *string* – Specifies the trust domain for the peer certificate.

To cancel the configuration, use the command **no remote-trust-domain**.

Configuring the Trust Domain of Encryption Certificate

The encryption certificate is used for encrypting data in the negotiation. The command is supported only in the GM 1.1 version. To configure the trust domain for the encryption certificate,

in the ISAKMP gateway configuration mode, use the following command:

trust-domain-enc *string*

- string – Specifies the trust domain for the encryption certificate.

To cancel the configuration, use the command **no trust-domain-enc**.

Configuring the Negotiation Protocol Standard

There are three negotiation protocol standards: IKEv1, IKEv2 and GM standard. By default, IKEv1 is used in system. To configure the negotiation protocol standard, in the ISAKMP gateway configuration mode, use the following command:

protocol-standard {**ikev1** | **guomi**[**v1.0** | **v1.1**]}

- **ikev1** – Specifies the IKEv1 as the negotiation protocol standard.
- **guomi**[**v1.0** | **v1.1**] – Specifies the GM standard as the negotiation protocol standard. If the version is specified as v1.0 or v1.1, the versions for the devices in the negotiation should be the same.

To cancel the configuration, use the command **no protocol-standard**.

Configuring a Local ID

To configure the local ID, in the ISAKMP gateway configuration mode, use the following command:

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** [*string*] – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID, but this parameter is optional. If *string* is not specified, the system will obtain the ID from the certificate.

- **u-fqdn** *string* – Specifies the ID type of U-FQDN, i.e., the email address type, such as user-1@hillstonenet.com.
- **key-id** *string* - Specifies the ID that uses the Key ID type. This type is applicable to the XAUTH function.
- **ip** *ip-address* - Specifies the ID type of IP address. *string* is the specific content of the ID.

To cancel the specified local ID, in the ISAKMP gateway configuration mode, use the command **no local-id**.

Configuring a Peer ID

StoneOS supports the ID types of FQDN and Asn1dn. To configure the peer ID, in the ISAKMP gateway configuration mode, use the following command:

peer-id {**fqdn** | **asn1dn** | **u-fqdn** | **key-id** | **ip** } *string*

- **fqdn** – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID.
- **u-fqdn string** – Specifies the ID type of U-FQDN, i.e., the email address type, such as user-1@hillstonenet.com.
- **key-id** - Specifies the ID using key ID type. The type is only supported for XAUTH function.
- **ip** - Specifies the ID type of IP address.

To cancel the specified peer ID, in the ISAKMP gateway configuration mode, use the command **no peer-id**.

Specifying a Connection Type

The created ISAKMP gateway can be an initiator, responder, or both the initiator and responder. To specify the connection type, in the ISAKMP gateway configuration mode, use the following command:

connection-type {bidirectional | initiator-only | responder-only}

- **bidirectional** – Specifies the ISAKMP gateway as both the initiator and responder. This is the default option.
- **initiator-only** – Specifies the ISAKMP gateway as the initiator only.
- **responder-only** – Specifies the ISAKMP gateway as the responder only.

To restore to the default connection type, in the ISAKMP gateway configuration mode, use the command **no connection-type**.

Enabling NAT Traversal

The NAT traversal function must be enabled when there is a NAT device in the IPsec or IKE tunnel and the device implements NAT. By default, NAT traversal is disabled. To enable NAT traversal, in the gateway ISAKMP configuration mode, use the following command:

nat-traversal

To disable NAT traversal, in the gateway ISAKMP configuration mode, use the command **no nat-traversal**.

Configuring Auto Routing

For IKEv1 VPN, if the address type for the peer of the created ISAKMP gateway is specified to be static or dynamic, route entry whose destination IP address is the local ID of the peer and next hop is tunnel interface will be added to the routing table automatically after you configure auto routing function and an IPSec SA is created. The auto routing function allows the device to automatically add routing entries from center to branch to avoid complexity of manual routing. When an IPSec SA is deleted, the corresponding route entry will be deleted from the routing table.

By default the auto routing is disabled. To enable it, in the ISAKMP gateway configuration mode, use the following command:

generate-route

To disable auto routing, use the command **no generate-route**.

Configuring DPD

DPD (Dead Peer Detection) is used to detect the state of the security tunnel peer. After the DPD function is enabled, the system will periodically send DPD requests to the peer in a specified time to detect whether the ISAKMP gateway exists. By default, this function is disabled.

To enable DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd

To configure DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd [**interval** *seconds*] [**retry** *times*] {**on memand** | **periodic**}

- **interval** *seconds* – Specifies the interval of sending DPD requests to the peer. The value range is 1 to 10 seconds. The default value is 10.
- **retry** *times* – Specifies the times of sending DPD requests to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 20 times. The default value is 3.
- **periodic** – Specify the periodic mode for DPD detection. In this mode, the system continuously sends DPD requests to the peer at a specified interval. If no response packet is received from the peer within a DPD detection period, the system determines that the peer does not exist. DPD detection period=DPD Interval * DPD Retries.
- **on memand** – Specify the on-demand mode for DPD detection. In this mode, the device does not send DPD requests if it receives no IPSec traffic. If the device receives IPSec traffic and needs to forward it, the system queries when the last receipt of the peer IPSec traffic happens. If the interval is shorter than the DPD detection period, it indicates that the peer ISAKMP gateway exists. In this case, the device does not send DPD detection requests. If the interval exceeds the DPD detection period, it indicates that the device needs to send DPD requests to detect the existence of the peer ISAKMP gateway. If the device does not receive the

response packet during the DPD detection period, the system ages SA information in phase 1 and phase 2 and initiates a new IPSec negotiation.

To resort the settings to the default DPD settings, use the command **no dpd**.

Specifying Description

To specify description for the ISAKMP Gateway, in the ISAKMP gateway configuration mode, use the following command:

description *string*

- *string* – Specifies the description for the ISAKMP gateway.

To delete the description, in the ISAKMP gateway configuration mode, use the command **no description**.

Enabling/Disabling ISAKMP SA and IPSec SA Negotiation Separation Mode

The ISAKMP SA and IPSec SA negotiation separation mode is disabled by default. That means when ISAKM SA times out, if only ISAKMP SA is negotiated and IPSec SA is not, ISAKMP SA will time out and disconnect after a certain period of time, resulting in IPSec VPN disconnection. When the ISAKMP SA and IPSec SA negotiation separation mode is enabled, the system allows negotiation of only ISAKMP SA when it times out. The original IPSec SA will continue to work, and ISAKMP will not time out because a new IPSec SA is not negotiated.

To enable the ISAKMP SA and IPSec SA negotiation separation mode, in the ISAKMP gateway configuration mode, use the following command:

phase1-phase2-sa unbind

To disable the ISAKMP SA and IPSec SA negotiation separation mode, in the ISAKMP gateway configuration mode, use the following command:

phase1-phase2-sa bind

Configuring a P2 Proposal

P2 proposal is used in the Phase 2 SA. The configurations of P2 proposal include encryption algorithm, hash algorithm, compression algorithm and lifetime.

Creating a P2 Proposal

To create a P2 proposal, i.e., an IPsec security proposal, in the global configuration mode, use the following command:

ipsec proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal that will be created. After executing the command, the CLI is in the P2 proposal configuration mode. You can configure parameters for P2 proposal in this mode.

To delete the specified P2 proposal, in the global configuration mode, use the command **no ipsec proposal** *p2-name*.

Specifying a Protocol Type

The protocol types available to P2 proposal include ESP and AH. To specify a protocol type for P2 proposal, in the P2 proposal configuration mode, use the following command:

protocol {**esp** | **ah**}

- **esp** – Uses ESP. This is the default protocol type.
- **ah** – Uses AH.

To restore to the default protocol type, in the P2 proposal configuration mode, use the command **no protocol**.

Specifying an Encryption Algorithm

You can specify 1 to 4 encryption algorithms for P2 proposal. To specify the encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256** |**aes-gcm-128**|**aes-gcm-192**|**aes-gcm-256** | **sm1** | **sm4** | **null**} [**3des** | **des** | **aes** | **aes-192** | **aes-256** | **aes-gcm-128**|**aes-gcm-192**|**aes-gcm-256** | **sm1** | **sm4** | **null**] [**3des** | **des** | **aes** | **aes-192** | **aes-256** |**aes-gcm-128**|**aes-gcm-192** | **aes-gcm-256** | **sm1** | **sm4** | **null**]……

- **3des** – Uses the 3DES encryption. The key length is 192-bit. This is the default method for StoneOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.
- **aes-gcm-128** – Uses the 128-bit AES-GCM encryption. The key length is 128 bits.
- **aes-gcm-192** – Uses the 192-bit AES-GCM encryption. The key length is 192 bits.
- **aes-gcm-256** – Uses the 256-bit AES-GCM encryption. The key length is 256 bits.
- **sm1** – Uses the SM1 block encryption algorithm. The key length is 128 bits.
- **sm4** – Uses the SM4 block encryption algorithm. The key length is 128 bits.
- **null** – No encryption.

To restore to the default encryption algorithm, in the P2 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

You can specify 1 to 3 hash algorithms for P2 proposal. To specify the hash algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**]

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.

- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.
- **sm3** – Uses the SM3 hash algorithm. The digest length is 256 bits.
- **null** – No hash algorithm.

To restore to the default hash algorithm, in the P2 proposal configuration mode, use the command **no hash**.

Specifying a Compression Algorithm

By default, the P2 proposal does not use any compression algorithm. To specify a compression algorithm (DEFLATE) for the P2 proposal, in the P2 proposal configuration mode, use the following command:

compression deflate

To cancel the specified compression algorithm, in the P2 proposal configuration mode, use the command **no compression**.

Configuring PFS

The PFS (Perfect Forward Security) function is designed to determine how to generate the new key instead of the time of generating the new key. PFS ensures that no matter what phase it is in, one key can only be used once, and the element used to generate the key can only be used once. The element will be discarded after generating a key, and will never be re-used to generate any other keys. Such a measure will assure that even if a single key is disclosed, the disclosure will only affect the data that is encrypted by the key, and will not threaten the entire communication. PFS is based on the DH algorithm. To configure PFS, in the P2 proposal configuration mode, use the following command:

group {nopfs | 1 | 2 | 5 | 14 | 15 |16| 18 | 19 | 20 | 21 | 24}

- **nopfs** – Disables PFS. This is the default option.
- **1** – Selects DH Group1. The key length is 768 bits（MODP Group）.
- **2** – Selects DH Group2. The key length is 1024 bits（MODP Group）.This is the default value.
- **5** – Selects DH Group5. The key length is 1536 bits（MODP Group）.
- **14** – Selects DH Group14. The key length is 2048 bits（MODP Group）.
- **15** – Selects DH Group15. The key length is 3072 bits（MODP Group）.
- **16** – Selects DH Group16. The key length is 4096 bits（MODP Group）.
- **18** – Selects DH Group18. The key length is 8192 bits（MODP Group）.
- **19** – Select DH Group 19. The key length is 256 bits (ECP Group).
- **20** – Select DH Group 20. The key length is 384 bits (ECP Group).
- **21** – Select DH Group 21. The key length is 521 bits (ECP Group).
- **24** – Select DH Group 24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore to the default PFS configuration, in the P2 proposal configuration mode, use the command **no group**.

Specifying a Lifetime

You can evaluate the lifetime by two standards which are time length and traffic volume. When the SA lifetime runs out, the SA will get expired and requires a new SA negotiation. To specify the lifetime for the P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies the lifetime of time length type. The value range is 180 to 86400 seconds. The default value is 28800.

lifesize *kilobytes*

- *kilobytes* – Specifies the lifetime of traffic volume type. The default value is 0.

To cancel the specified lifetime, in the P2 proposal configuration mode, use the following commands:

no lifetime

no lifesize

Configuring the smart link

When there are multiple communication links (ethernet0/1、ethernet0/2、ethernet0/3) between branches and the headquarter data center, you can configure Smart Link on branch firewalls to realize dynamic switch between IPSec links.

Each link has a unique ID. With the Smart Link function, the system select the link by order to negotiate the IPSec tunnel. All links are arranged from top to bottom. To view the link order, use the **show ipsec smart-link** command. In the initial state, the system selects the top link to negotiate an IPSec tunnel. When the IPSec tunnel is established, the system sends detection packets to detect link quality. If the packet loss rate or latency exceeds the specified threshold, the system would switch the current link to the next one to establish a new IPSec tunnel.



Notes: The smart link function can only be configured when the type of the VPN peer is static IP.

This section introduces the following smart link configuration:

- Configuring the Smart Link Profile
- Creating a Link
- Configuring the Link Detection Parameters
- Configuring the Threshold of Link Quality Parameters

- Configuring the Threshold of Cycle Switching Times
- Enabling/Disabling Link Detection and Switch
- Activating a Link for Negotiation
- Adjusting Link Order
- Configuring Silence Period

Configuring the Smart Link Profile

To configure the smart link profile and go to the smart link profile configuration mode, use the following command in the global configuration mode:

ipsec smart-link profile *profile-name*

- *profile-name* - Specifies the name of the smart link profile. The value is from 1 to 31 characters. If the specified name already exists, you will go to the configuration mode of this smart link profile.

In the global configuration mode, use the following command to delete the specified smart link profile:

no ipsec smart-link profile *profile-name*

Creating a Link

You can configure both IPv4 and IPv6 addresses for the link to negotiate an IPSec tunnel. But one smart link profile only supports one IP type (either IPv4 or IPv6). Newly created link will be added to the end of all links. Use the **move link** command to adjust link sequence.

To create a link, in the smart link profile configuration mode, use the following command:

link *id* **interface** *interface-name* **peer** *ip-address*

- *id* - Specifies the ID of the link. The value range is from 1 to 30.
- *interface-name* - Specifies the name of the local interface of the link. This interface should be configured with IP address.
- *ip-address* - Specifies the peer IP address of the link.

To delete the specified link, in the smart link profile configuration mode, use the following command:

no link *id*

Configuring the Link Detection Parameters

When an IPSec tunnel is built, the system will send detection packets based on the configured link detection parameters.

To configure the link detection parameters, in the smart link profile configuration mode, use the following command:

link-track [**source** *source-ipv4-address* **destination** *destination-ip-address*] [**interval** *interval-value*] [**count** *count-value*]

- **source** *source-ip-address* - Specifies the source IP address of the detection packets. Both IPv4 and IPv6 addresses are supported. If this parameter is not specified, the IP address of the IPSec tunnel's local interface is used as the source IP address of the detection packets.
- **destination** *destination-ip-address* - Specifies the destination IP address of the detection packets. Both IPv4 and IPv6 addresses are supported. If this parameter is not specified, the IP address of the IPSec tunnel's peer interface is used as the destination IP address of the detection packets.
- **interval** *interval-value* - Specifies the interval to send detection packets. The value range is from 1 to 5 seconds. The default value is 3 seconds.
- **count** *count-value* - Specifies the total number of detection packets sent in a detection period. The value range is from 1 to 30. The default value is 10.

To restore to the default link detection parameters, in the smart link profile configuration mode, use the **no link-track** command.

Configuring the Threshold of Link Quality Parameters

After a detection period, the system calculates the link's latency and packet loss rate, and compares the value to the threshold. The system will switch the current link to the next one if either parameter exceeds its threshold.

To configure the threshold of link quality parameters, in the smart link profile configuration mode, use the following command:

link-track-threshold { [**delay** *delay-value*] [**loss-rate** *loss-rate*] }

- **delay** *delay-value* - Specifies the latency threshold of the link The value range is from 100 to 3000 milliseconds. The default value is 500.
- **loss-rate** *loss-rate* - Specifies the threshold of the loss rate of the link. The value range is from 1 to 100 percent. The default value is 30.

To delete configured threshold of the link quality parameters, in the smart link profile configuration mode, use the **no link-track-threshold** command.

Configuring the Threshold of Cycle Switching Times

When all links are switched in turn, it is called a switch cycle. If the cycle switching times exceed the threshold, the system will no longer detect and switch links and will switch the current link to the one with the best quality.

To configure the threshold of cycle switching times, in the smart link profile configuration mode, use the following command:

link-switch-cycles *cycle-value*

- *cycle-value* - Specifies the threshold for the cycle switching times. The value range is from 0 to 5. The default value is 5. The value 0 indicates that there is no limit to the cycle switching times.

In the smart link profile configuration mode, use the **no link-switch-cycles** command to restore to the default cycle switching times.

Enabling/Disabling Link Detection and Switch

Link detection and switch is enabled by default.

To enable link detection and switch, in smart link profile configuration mode, use the following command:

smart-link enable

To disable link detection and switch, in smart link profile configuration mode, use the following command:

smart-link disable

Activating a Link for Negotiation

To activate the specified link for immediate IPSec tunnel negotiation, in smart link profile configuration mode, use the following command:

active link *id*

- *id* - Specifies the ID of the existing link.

Adjusting Link Order

Newly created link will be added to the end of all links. To adjust the sequence of the links, in smart link profile configuration mode, use the following command:

move link *id* {**after** | **before** *id*}

- *id* - Specifies the ID of the link whose sequence needs to be adjusted.
- **after** | **before** *id* - Specifies ID of the link before or after which the specified link is placed after the sequence adjustment.

Configuring Silence Period

If the cycle switching times exceed the threshold, the system will no longer detect and switch links. The default silence period is 600 seconds. When the silence period expires, the system starts to detect the quality of active links again.

To set the silence period, in smart link profile configuration mode, use the following command:

link-switch-back-time *value*

- *value* - Specifies the silence period. The value range is from 600 to 1800 seconds. The default value is 600.

To restore to the default silence period, use the **no link-switch-back-time** command.

Configuring a Tunnel

When configuring an IPSec tunnel through IKE, you need to configure the following options: the protocol type, ISAKMP gateway, IKE security proposal, ID, DF-bit and anti-replay.

Creating an IKE Tunnel

To create an IKE tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - Specifies the name of the IKE tunnel that will be created.

After executing the above command, the CLI will enter the IKE tunnel configuration mode. All the parameters of the IKE tunnel need to be configured in the IKE tunnel configuration mode.

To delete the specified IKE tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **auto**.

Enabling /Disabling an IKE Tunnel

The function is enabled by default. To enable or disable an IKE tunnel, in the IKE tunnel configuration mode, use the following command:

- Enable an IKE tunnel: **enable**
- Disable an IKE tunnel: **disable**

Specifying the Encapsulation Mode of IPsec Protocol

To specify the encapsulation mode of IPsec protocol for the IKE tunnel (either transport mode or tunnel mode), in the IKE tunnel configuration mode, use the following command:

mode {**transport** | **tunnel**}

- **transport** – Specifies the encapsulation mode of IPsec as transport.
- **tunnel** – Specifies the encapsulation mode of IPsec as tunnel. This is the default mode.

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no mode**.

Specifying an ISAKMP Gateway

To specify an ISAKMP gateway for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

isakmp-peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

To cancel the specified ISAKMP gateway, in the IKE tunnel configuration mode, use the command **no isakmp-peer**.

Specifying a Smart Link Profile

To specify a smart link profile for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

smart-link-profile *profile-name*

- *profile-name* - Specifies the name of the smart link profile.

To cancel the specified smart link profile, use the **no smart-link-profile** command.

Specifying a P2 Proposal

To specify a P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

ipsec-proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal.

To cancel the specified P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the command **no ipsec-proposal**.

Specifying a Phase 2 ID

Users need to specify the IKE phase 2 ID to distribute and limit IPSec VPN traffic. Phase 2 ID consists of a local network segment, a remote network segment, and the service. During the configuration, you need to configure phase 2 IDS on the local and remote devices. Then, the local and remote devices negotiate to create an IKE IPSec tunnel. You can specify one or more phase 2 IDs to create one or more IKE IPSec tunnels. The system distributes and limits tunnel traffic according to the phase 2 ID of each tunnel.

If you do not need to distribute or limit IPSec VPN traffic, you do not need to configure this parameter. For details about how to enable IPSec VPN traffic distribution and Limitation function, see Configuring IPsec VPN Traffic Distribution and Limitation.

To specify a Phase 2 ID for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – Automatically assigns the Phase 2 ID. This is the default option.
- **local** *ip-address/mask* – Specifies the IP/ mask of the local network segment in phase 2.
- **remote** *ip-address/mask* – Specifies the IP/ mask of the remote network segment(peer device) in phase 2.
- **service** *service-name* – Specifies the service or protocol name of the traffic that can be transmitted by IKE IPSec tunnels in phase 2.

You can configure up to 256 phase 2 IDs and use them to establish multiple IKE tunnels.

To restore the settings to the default ones, in the IKE tunnel configuration mode, use the command **no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}



Notes: By default, the Phase 2 IDs of the local and peer device need to be configured accordingly. If the IDs configured on the two device cannot match, the negotiation will fail. In this case, if you enable the Accepting All Proxy ID function on the responder's device, the negotiation succeeds. For details about how to enable **Accepting All Proxy ID** function, see Accepting All Proxy ID

Configuring IPsec VPN Traffic Distribution and Limitation

This function is disabled by default. Before configuring, ensure that the phase 2 ID has been configured and phase 2 negotiations has been successful. After this function is enabled, the device filters the inbound and outbound traffic of the IKE tunnel according to phase 2 ID and then distributes and limits the inbound and outbound traffic. Traffic that does not match phase 2 IDs is discarded. Details are as follows:

- **Distribution**: Based on the configuration of Phase 2 IDs, the traffic distribution function can distribute the traffic at the IKE tunnel ingress interface when the traffic flow into the IKE tunnel. If the elements of source IP address, destination IP address, and the type of the traffic can match the configuration of a certain Phase 2 ID, this kind of traffic will flow into the corresponding IKE tunnel for encapsulation and sending. If the traffic cannot match any Phase 2 IDs, it will be dropped.
- **Limitation**: Based on the configuration of Phase 2 IDs, the traffic limitation function can limit the traffic at the IKE tunnel egress interface when the traffic flows out of the IKE tunnel. After the traffic was de-encapsulated, StoneOS checks the elements of source IP address, destination IP address, and the type of the traffic to see whether this kind of traffic matches a certain Phase 2 ID or not. If matched, the traffic will be dealt with. If not matched, the traffic will be dropped.

To enable the traffic distribution and limitation, use the following command in the IKE tunnel configuration mode:

check-id

Use the no form of the command to cancel this function.

Accepting All Proxy ID

This function needs to be configured on the responder device of IKE tunnel negotiation. After it is enabled, the responder device will accept the second-phase ID configured by the peer (negotiation initiator) and set its phase 2 ID according to the peer. In this way, the two ends of the IKE tunnel can successfully negotiate. This function is often used in scenarios where the responder device cannot perceive or is not interested in the initiator's Phase 2 ID. To enable the accepting all proxy ID function, in the IKE tunnel configuration mode, use the following command:

accept-all-proxy-id

To disable the function, in the IKE tunnel configuration mode, use the following command:

no accept-all-proxy-id



Notes: When multiple Phase 2 IDs are configured on the responder device (that is, multiple IKE tunnels are configured), you need to disable this function. Otherwise, only one tunnel can be negotiated.

Configuring Auto-connection

The device will be triggered to establish SA in two modes: auto and traffic intrigued.

- In the auto mode, the device detects the SA status every 60 seconds and initiates negotiation request when SA is not established;
- In the traffic intrigued mode, the tunnel sends negotiation requests only when there is traffic passing through the tunnel.

By default, the traffic intrigued mode is used. To use the auto mode, in the IKE tunnel configuration mode, use the following command:

auto-connect

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no auto-connect**.



Notes: Auto connection works only when the peer IP is static and the local device is acting as the initiator.

Configuring DF-bit

You can specify whether to allow the forwarding device to fragment the packets. To configure DF-bit for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

df-bit {**copy** | **clear** | **set**}

- **copy** – Copies the IP packet DF options from the sender directly. This is the default value.
- **clear** – Allows the device to fragment packets
- **set** – Disallows the device to fragment packets.

To restore to the default value, in the IKE tunnel configuration mode, use the command **no df-bit**.

Configuring Anti-replay

Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled. To configure anti-replay for the IKE IPsec tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** – Specifies the anti-replay window as 32.
- **64** – Specifies the anti-replay window as 64.
- **128** – Specifies the anti-replay window as 128.
- **256** – Specifies the anti-replay window as 256.
- **512** – Specifies the anti-replay window as 512.

When the network condition is poor, for example, under the condition of serious packet disorder, choose a larger window.

To disable the function, in the IKE IPsec tunnel configuration mode, use the command **no anti-replay**.

Configuring VPN Track and Redundant Backup

Hillstone devices can monitor the connectivity status of the specified VPN tunnel, and also allow backup or load sharing between two or more VPN tunnels. This function is applicable to both the route-based VPN and policy-based VPN. The practical implementation environments include:

- Configuring a backup VPN tunnel for the remote peer, at any time only one tunnel is active. Initially, the main VPN tunnel is active, if disconnection of the main tunnel is detected, the device will re-transmit the information flow through the backup tunnel;
- Configuring two or more VPN tunnels for the remote peer. All tunnels are active simultaneously, and load balance the traffic via equal-cost multi-path routing (ECMP). If disconnection of any tunnel is detected, the device will re-transmit the information flow through other tunnels.

The VPN track function tracks the status of the target tunnel by Ping packets. By default, the function is disabled. To configure the VPN track function, in IKE IPsec tunnel configuration mode, use the following command:

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

- *A.B.C.D* – Specifies the IP address of the tracked object. When the peer is a Hillstone device and the parameter is not specified, the system will use the IP address of the peer by default. This IP address can not be 0.0.0.0 or 255.255.255.255.
- **src-ip** *A.B.C.D* – Specifies the source IP address that sends Ping packets. When the peer device is a Hillstone device and the parameter is not specified, the system will use the IP address of egress interface by default. This IP address cannot be 0.0.0.0 or 255.255.255.255.
- **interval** *time-value* – Specifies the interval of sending Ping packets. The value range is 1 to 255 seconds. The default value is 10.

- **threshold** *value* – Specifies the threshold for determining the track failure. If the system did not receive the specified number of continuous response packets, it will identify a track failure, i.e., the target tunnel is disconnected. The value range is 1 to 255. The default value is 10.

To disable the VPN track function, in IKE IPsec tunnel configuration mode, use the command **no vpn-track**.

The VPN track function can be in active or dead status. To view the VPN track status and configuration information via CLI, use the following commands:

- Show the status of VPN track: **show ipsec sa** {*id*}
- Show the configuration of VPN track: **show tunnel ipsec** {**manual** | **auto**} {*tunnel-name*}

For example:

Show the status of VPN track

hostname(config)# **show ipsec sa 5**

ID: 1

scpu: 0

VPN Name: vpn1

L2tp port: 1

Duration(S): 1375459

Last setup time: 2022-03-08 22:09:53

Last teardown time: 2022-03-09 06:09:54

Tear down reason: a lifetime timeout occurred

Teardowns today: 0

Outbound

Gateway: 1.1.1.2

.....

Sending rate(KB/s): 0

Status: Active

Inbound

Gateway: 1.1.1.2

.....

Receiving rate(KB/s): 0

Status: Active

VPN track status: alive

Show the configuration of VPN track

hostname(config)# **show tunnel ipsec auto vpn1**

Name: vpn1

mode: tunnel

.....

vpn-track: enable

tracknotify: enable

vpntrack destination 1.1.1.1

vpntrack source ip: 2.2.2.2



Tip: For more examples of VPN track and redundant backup, see Example of Configuring Route-based VPN Track and Redundant Backup.

Enabling/Disabling Notification of VPN Tunnel Status

By default, the notification of VPN tunnel status is disabled. When the notification is enabled, for route-based VPN, when system detects disconnection of a VPN tunnel, it will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route information; for policy-based VPN, when system detects disconnection of a VPN tunnel, it will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy information. You can enable/disable the tunnel state notification function via CLI, so that the system will not send any tunnel track failure notification. To enable or disable the tunnel state notification function, in the IKE IPsec tunnel configuration mode, use the following command:

- Enable: **tunnel-state-notify**
- Disable: **no tunnel-state-notify**

Setting a Commit Bit

You can set a commit bit to avoid packet loss and time difference. However, the commit bit may slow down the responding speed. To set a commit bit, in the IKE IPsec tunnel configuration mode, use the following command:

Responder sets a commit bit: **responder-set-commit**

Responder does not set a commit bit: **no responder-set-commit**

Specifying Description

To specify the description of IKE tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

description *string*

- *string* – Specifies the description of the IKE tunnel.

To delete the description, in the IKE IPsec tunnel configuration mode, use the command **no description**.

IKEv2 VPN

The configurations of IKEv2 VPN include:

- Configuring a P1 proposal
- Configuring an ISAKMP gateway
- Configuring a P2 proposal
- Configuring a tunnel

Configuring a P1 Proposal

P1 proposal is the IKE security proposal that can be applied to the ISAKMP gateway, and is used in the Phase 1 SA. The configurations of IKE security proposal include specifying an authentication method, encryption algorithm, hash algorithm, PRF (pseudo-random function) algorithm, lifetime of SA and DH group.

Creating a P1 Proposal

To create a P1 proposal, i.e., an IKE security proposal, in the global configuration mode, use the following command:

isakmp proposal *p1-name*

- *p1-name* – Specifies the name of the P1 proposal that will be created. After executing the command, the CLI will enter the P1 proposal configuration mode. You can configure parameters for P1 proposal in this mode.

To delete the specified P1 proposal, in the global configuration mode, use the command **no isakmp proposal** *p1-name*.

Specifying an Authentication Method

Specify the method of IKE identity authentication. Identity authentication is used to confirm the identities of both the ends during the communication. There are two methods: pre-shared key authentication and digital signature authentication. For the pre-shared key authentication, the authentication string is used as an input to generate a key, and different authentication strings will definitely generate different keys. In the non-root VSYS, only the pre-share key authentication mode is supported. To specify the authentication method of IKE security proposal, in the P1 proposal configuration mode, use the following command:

authentication {**pre-share** | **rsa-sig** | **ecdsa-sig** }

- **pre-share** – Uses the pre-shared key authentication. This is the default method.
- **rsa-sig** – Uses the RSA digital signature authentication.
- **ecdsa-sig** – Uses the ECDSA digital signature authentication. When the authentication mode is selected, only verification algorithm SHA-256, SHA-384 or SHA-512 are supported.

To restore to the default authentication method, in the P1 proposal configuration mode, use the command **no authentication**.

Specifying an Encryption Algorithm

StoneOS provides the following five encryption algorithms: 3DES, DES, 128bit AES, 192-bit AES and 256-bit AES. To specify the encryption algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256**}

- **3des** – Uses the 3DES encryption. The key length is 192 bits. This is the default algorithm for StoneOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes** – Uses the AES encryption. The key length is 128 bits.

- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.

To restore to the default encryption algorithm, in the P1 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

StoneOS supports the following hash algorithms: MD5, SHA-1 and SHA-2 (including SHA-256, SHA-384 and SHA-512). To specify the hash algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

hash {md5 | sha | sha256 | sha384 | sha512}

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.

To restore to the default hash algorithm, in the P1 proposal configuration mode, use the command **no hash**.

Specifying a PRF Algorithm

StoneOS support the following PRF algorithms: MD5, SHA-1, and SHA-2. SHA-2 includes SHA-256, SHA-384, and SHA-512. You can specify up to four PRF algorithms. To specify the PRF algorithm, in the P1 proposal configuration mode, use the following command:

prf {md5 | sha | sha256 | sha384 | sha512}

- **md5** – Uses the MD5 algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 algorithm. The digest length is 256 bits.
- **sha384** – Uses the SHA-384 algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 algorithm. The digest length is 512 bits.

To restore to the default algorithm, in the P1 proposal configuration mode, use the command **no prf**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. The longer the key element is, the more secure the generated key will be, and the more difficult it will be to decrypt it. The selection of DH group is important, because the DH Group is only determined in the Phase 1 SA negotiation, and the Phase 2 negotiation will not re-select a DH group. The two phases use the same DH group; therefore the selection of DH group will have an impact on the keys generated for all sessions. During negotiation, the two ISAKMP gateways should select the same DH group, i.e., the length of key element should be equal. If the DH groups do not match, the negotiation will fail.

To select a DH group, in the P1 proposal configuration mode, use the following command:

group {1 | 2 | 5 | 14 | 15 |16| 18 | 19 | 20 | 21 | 24}

- **1** – Selects DH Group1. The key length is 768 bits（MODP Group）.
- **2** – Selects DH Group2. The key length is 1024 bits（MODP Group）.This is the default value.
- **5** – Selects DH Group5. The key length is 1536 bits（MODP Group）.
- **14** – Selects DH Group14. The key length is 2048 bits（MODP Group）.

- **15** – Selects DH Group15. The key length is 3072 bits（MODP Group）.
- **16** – Selects DH Group16. The key length is 4096 bits（MODP Group）.
- **18** – Selects DH Group18. The key length is 8192 bits（MODP Group）.
- **19** – Select DH Group 19. The key length is 256 bits (ECP Group).
- **20** – Select DH Group 20. The key length is 384 bits (ECP Group).
- **21** – Select DH Group 21. The key length is 521 bits (ECP Group).
- **24** – Select DH Group 24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

When configuring PFS in the P2 proposal, you can also select the DH group.

Specify the Lifetime of SA

The Phase 1 SA is configured with a default lifetime. When the SA lifetime expires, the device will send an SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation. To specify the lifetime of SA, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400.

To restore to the default lifetime, in the P1 proposal configuration mode, use the command **no lifetime**.

Configuring an ISAKMP Gateway

After creating an ISAKMP gateway, you can configure the IKE negotiation mode, IP address and type of the ISAKMP gateway, IKE security proposal, pre-shared key, PKI trust zone, local ID,

ISAKMP gateway ID, ISAKMP connection type, NAT traversal, etc.

Creating an ISAKMP Gateway

To create an ISAKMP gateway, in the global configuration mode, use the following command:

isakmp peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

After executing the command, the CLI will enter the ISAKMP gateway configuration mode. You can configure parameters for the ISAKMP gateway in this mode.

To delete the specified ISAKMP gateway, in the global configuration mode, use the command **no isakmp peer** *peer-name*.

Binding an Interface to the ISAKMP Gateway

To bind an interface to the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the binding interface.

To cancel the binding, in the ISAKMP gateway configuration mode, use the command **no interface** *interface-name*.

Configuring the Negotiation Protocol Standard

There are three negotiation protocol standards: IKEv1, IKEv2 and GM standard. By default, IKEv1 is used in system. To configure the IKEv2 protocol standard, in the ISAKMP gateway configuration mode, use the following command:

protocol-standard ikev2

- **ikev2** – Specifies the IKEv2 as the negotiation protocol standard.

To cancel the configuration, use the command **no protocol-standard**.

Configuring the Custom IKE Negotiation Port

You can configure a custom UDP port for IKE negotiation, and establish the IPSec connection. To configure a custom IKE negotiation port, in the ISAKMP gateway configuration mode, use the following command:

ipsec-over-udp port *port-number*

- *port-number* – Specifie the UDP port number, the range is 1 to 65535. To avoid port number conflicts, you are advised to use port numbers ranging from 1024 to 65535.

To cancel the configuration, in the ISAKMP gateway configuration mode, use the command **no ipsec-over-udp**.

Specifying the IP Address and Peer Type

You can specify the IP address for the peer of the created ISAKMP gateway. To specify the IP address and the type of the peer, in the ISAKMP gateway configuration mode, use the following command:

peer *ip-address*

- *ip-address* - Specifies the IP address or the host name of the peer.

To cancel the IP address or the host name, in the ISAKMP gateway configuration mode, use the command **no peer**.

Specifying a P1 Proposal

To specify the P1 proposal for the ISAKMP gateway, in ISAKMP the gateway configuration mode, use the following command:

isakmp-proposal p1-proposal1 [p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – Specifies the name of the P1 proposal. You can specify up to four P1 proposals for the ISAKMP gateway.

To cancel the specified P1 proposal, in ISAKMP the gateway configuration mode, use the command **no isakmp-proposal**.

Configuring a Pre-shared Key

If the pre-shared key authentication method is used, you need to specify a pre-shared key. To specify the pre-shared key for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

pre-share *string*

- *string* – Specifies the content of the pre-shared key.

To cancel the specified pre-shared key, in the ISAKMP gateway configuration mode, use the command **no pre-share**.

Configuring a PKI Trust Domain

If the digital signature authentication mode is used, you need to specify a PKI trust domain for the digital signature. To specify the PKI trust domain for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

trust-domain *string*

- *string* – Specifies the PKI trust domain.

To cancel the specified PKI trust domain, in the ISAKMP gateway configuration mode, use the command **no trust-domain**.



Tip: For more information about how to configure a PKI trust domain, see "PKI" in the "User Authentication".

Configuring the Trust Domain of Peer Certificate

The peer certificate is used for encrypting and authenticating data in the negotiation. The initiator of VPN connection should import the peer certificate first. The command is supported only in the GM 1.0 version. To configure the trust domain of peer certificate , in the ISAKMP gateway configuration mode, use the following command:

remote-trust-domain *string*

- *string* – Specifies the trust domain for the peer certificate.

To cancel the configuration, use the command **no remote-trust-domain**.

Configuring a Local ID

To configure the local ID, in the ISAKMP gateway configuration mode, use the following command:

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* | **key-id** *string* |**ip** *ip-address* }

- **fqdn** *string* – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** [*string*] – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID, but this parameter is optional. If *string* is not specified, the system will obtain the ID from the certificate.
- **u-fqdn** *string* – Specifies the ID type of U-FQDN, i.e., the email address type, such as user-1@hillstonenet.com.
- **key-id** *string* - Specifies the ID that uses the Key ID type. This type is applicable to the XAUTH function.
- **ip** *ip-address* - Specifies the ID type of IP address. *string* is the specific content of the ID.

To cancel the specified local ID, in the ISAKMP gateway configuration mode, use the command no local-id.

Configuring a Peer ID

StoneOS supports the ID types of FQDN and Asn1dn. To configure the peer ID, in the ISAKMP gateway configuration mode, use the following command:

peer-id {**fqdn** | **asn1dn** | **ip** } *string*

- **fqdn** – Specifies the ID type of FQDN. *string* is the specific content of the ID.
- **asn1dn** – Specifies the ID type of Asn1dn. This type is only applicable to the case of using a certificate. *string* is the specific content of the ID.
- **ip** - Specifies the ID type of IP address.

To cancel the specified peer ID, in the ISAKMP gateway configuration mode, use the command **no peer-id**.

Specifying a Connection Type

The created ISAKMP gateway can be an initiator, responder, or both the initiator and responder. To specify the connection type, in the ISAKMP gateway configuration mode, use the following command:

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – Specifies the ISAKMP gateway as both the initiator and responder. This is the default option.
- **initiator-only** – Specifies the ISAKMP gateway as the initiator only.
- **responder-only** – Specifies the ISAKMP gateway as the responder only.

To restore to the default connection type, in the ISAKMP gateway configuration mode, use the command **no connection-type**.

Configuring Auto Routing

For IKEv1 VPN, if the address type for the peer of the created ISAKMP gateway is specified to be static or dynamic, route entry whose destination IP address is the local ID of the peer and next hop is tunnel interface will be added to the routing table automatically after you configure auto routing function and an IPSec SA is created. The auto routing function allows the device to automatically add routing entries from center to branch to avoid complexity of manual routing. When an IPSec SA is deleted, the corresponding route entry will be deleted from the routing table.

By default the auto routing is disabled. To enable it, in the ISAKMP gateway configuration mode, use the following command:

generate-route

To disable auto routing, use the command **no generate-route**.

Configuring DPD

DPD (Dead Peer Detection) is used to detect the state of the security tunnel peer. After the DPD function is enabled, the system will periodically send DPD requests to the peer in a specified time to detect whether the ISAKMP gateway exists. By default, this function is disabled.

To enable DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd

To configure DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd [**interval** *seconds* [**retry** *times*] [**periodic**]]

- **interval** *seconds* – Specifies the interval of sending DPD requests to the peer. The value range is 1 to 10 seconds. The default value is 10.
- **retry** *times* – Specifies the times of sending DPD requests to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 20 times. The default value is 3.
- **periodic** – Specify the periodic mode for DPD detection. In this mode, the system continuously sends DPD requests to the peer at a specified interval. If no response packet is received from the peer within a DPD detection period, the system determines that the peer does not exist. DPD detection period=DPD Interval * DPD Retries.

To resort the settings to the default DPD settings, use the command **no dpd**.

Specifying Description

To specify description for the ISAKMP Gateway, in the ISAKMP gateway configuration mode, use the following command:

description *string*

- *string* – Specifies the description for the ISAKMP gateway.

To delete the description, in the ISAKMP gateway configuration mode, use the command **no description**.

Configuring a P2 Proposal

P2 proposal is used in the Phase 2 SA. The configurations of P2 proposal include encryption algorithm, hash algorithm, compression algorithm and lifetime.

Creating a P2 Proposal

To create a P2 proposal, i.e., an IPsec security proposal, in the global configuration mode, use the following command:

ipsec proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal that will be created. After executing the command, the CLI is in the P2 proposal configuration mode. You can configure parameters for P2 proposal in this mode.

To delete the specified P2 proposal, in the global configuration mode, use the command **no ipsec proposal** *p2-name*.

Specifying a Protocol Type

The protocol types available to P2 proposal include ESP. To specify a protocol type for P2 proposal, in the P2 proposal configuration mode, use the following command:

protocol esp

- **esp** – Uses ESP. This is the default protocol type.

To restore to the default protocol type, in the P2 proposal configuration mode, use the command **no protocol**.

Specifying an Encryption Algorithm

You can specify 1 to 4 encryption algorithms for P2 proposal. To specify the encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

encryption {**3des** | **des** | **aes-192** | **aes-256** } [**3des** | **des** | **aes** | **aes-192** | **aes-256**] [**3des** | **des** | **aes** | **aes-192** | **aes-256**]……

- **3des** – Uses the 3DES encryption. The key length is 192-bit. This is the default method for StoneOS.
- **des** – Uses the DES encryption. The key length is 64 bits.
- **aes-192** – Uses the 192-bit AES encryption. The key length is 192 bits.
- **aes-256** – Uses the 256-bit AES encryption. The key length is 256 bits.

To restore to the default encryption algorithm, in the P2 proposal configuration mode, use the command **no encryption**.

Specifying a Hash Algorithm

You can specify 1 to 3 hash algorithms for P2 proposal. To specify the hash algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** } [**md5** | **sha** | **sha256** | **sha384** | **sha512**] [**md5** | **sha** | **sha256** | **sha384** | **sha512**]

- **md5** – Uses the MD5 hash algorithm. The digest length is 128 bits.
- **sha** – Uses the SHA-1 hash algorithm. The digest length is 160 bits. This is the default hash algorithm.
- **sha256** – Uses the SHA-256 hash algorithm. The digest length is 256 bits.

- **sha384** – Uses the SHA-384 hash algorithm. The digest length is 384 bits.
- **sha512** – Uses the SHA-512 hash algorithm. The digest length is 512 bits.

To restore to the default hash algorithm, in the P2 proposal configuration mode, use the command **no hash**.

Specifying a Compression Algorithm

By default, the P2 proposal does not use any compression algorithm. To specify a compression algorithm (DEFLATE) for the P2 proposal, in the P2 proposal configuration mode, use the following command:

compression deflate

To cancel the specified compression algorithm, in the P2 proposal configuration mode, use the command **no compression**.

Configuring PFS

The PFS (Perfect Forward Security) function is designed to determine how to generate the new key instead of the time of generating the new key. PFS ensures that no matter what phase it is in, one key can only be used once, and the element used to generate the key can only be used once. The element will be discarded after generating a key, and will never be re-used to generate any other keys. Such a measure will assure that even if a single key is disclosed, the disclosure will only affect the data that is encrypted by the key, and will not threaten the entire communication. PFS is based on the DH algorithm. To configure PFS, in the P2 proposal configuration mode, use the following command:

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**| **18** | **19** | **20** | **21** | **24**}

- **nopfs** – Disables PFS. This is the default option.
- **1** – Selects DH Group1. The key length is 768 bits（MODP Group）.
- **2** – Selects DH Group2. The key length is 1024 bits（MODP Group）.This is the default value.

- **5** – Selects DH Group5. The key length is 1536 bits（MODP Group）.
- **14** – Selects DH Group14. The key length is 2048 bits（MODP Group）.
- **15** – Selects DH Group15. The key length is 3072 bits（MODP Group）.
- **16** – Selects DH Group16. The key length is 4096 bits（MODP Group）.
- **18** – Selects DH Group18. The key length is 8192 bits（MODP Group）.
- **19** – Select DH Group 19. The key length is 256 bits (ECP Group).
- **20** – Select DH Group 20. The key length is 384 bits (ECP Group).
- **21** – Select DH Group 21. The key length is 521 bits (ECP Group).
- **24** – Select DH Group 24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore to the default PFS configuration, in the P2 proposal configuration mode, use the command **no group**.

Specifying a Lifetime

You can evaluate the lifetime by two standards which are time length and traffic volume. When the SA lifetime runs out, the SA will get expired and requires a new SA negotiation. To specify the lifetime for the P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies the lifetime of time length type. The value range is 180 to 86400 seconds. The default value is 28800.

lifesize *kilobytes*

- *kilobytes* – Specifies the lifetime of traffic volume type. The default value is 0.

To cancel the specified lifetime, in the P2 proposal configuration mode, use the following commands:

no lifetime

no lifesize

Configuring a Tunnel

When configuring an IPSec tunnel through IKE, you need to configure the following options: the protocol type, ISAKMP gateway, IKE security proposal, ID, DF-bit and anti-replay.

Creating an IKE Tunnel

To create an IKE tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - Specifies the name of the IKE tunnel that will be created.

After executing the above command, the CLI will enter the IKE tunnel configuration mode. All the parameters of the IKE tunnel need to be configured in the IKE tunnel configuration mode.

To delete the specified IKE tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **auto**.

Enabling /Disabling an IKE Tunnel

The function is enabled by default. To enable or disable an IKE tunnel, in the IKE tunnel configuration mode, use the following command:

- Enable an IKE tunnel: **enable**
- Disable an IKE tunnel: **disable**

Specifying the Encapsulation Mode of IPsec Protocol

To specify the encapsulation mode of IPsec protocol for the IKE tunnel (either transport mode or tunnel mode), in the IKE tunnel configuration mode, use the following command:

mode {**transport** | **tunnel**}

- **transport** – Specifies the encapsulation mode of IPsec as transport.
- **tunnel** – Specifies the encapsulation mode of IPsec as tunnel. This is the default mode.

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no mode**.

Specifying an ISAKMP Gateway

To specify an ISAKMP gateway for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

isakmp-peer *peer-name*

- *peer-name* – Specifies the name of the ISAKMP gateway.

To cancel the specified ISAKMP gateway, in the IKE tunnel configuration mode, use the command **no isakmp-peer**.

Specifying a P2 Proposal

To specify a P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

ipsec-proposal *p2-name*

- *p2-name* – Specifies the name of the P2 proposal.

To cancel the specified P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the command **no ipsec-proposal**.

Specifying a Phase 2 ID

Users need to specify the IKE phase 2 ID to distribute and limit IPSec VPN traffic. Phase 2 ID consists of a local network segment, a remote network segment, and the service. During the configuration, you need to configure phase 2 IDS on the local and remote devices. Then, the local and remote devices negotiate to create an IKE IPSec tunnel. You can specify one or more phase 2

IDs to create one or more IKE IPSec tunnels. The system distributes and limits tunnel traffic according to the phase 2 ID of each tunnel.

If you do not need to distribute or limit IPSec VPN traffic, you do not need to configure this parameter. For details about how to enable IPSec VPN traffic distribution and Limitation function, see Configuring IPsec VPN Traffic Distribution and Limitation.

To specify a Phase 2 ID for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

id local *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*

- **local** *ip-address/mask* – Specifies the IP/ mask of the local network segment in phase 2.
- **remote** *ip-address/mask* – Specifies the IP/ mask of the remote network segment(peer device) in phase 2.
- **service** *service-name* – Specifies the service or protocol name of the traffic that can be transmitted by IKE IPSec tunnels in phase 2.

You can configure up to 256 phase 2 IDs and use them to establish multiple IKE tunnels.

To restore the settings to the default ones, in the IKE tunnel configuration mode, use the command **no id local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*

Notes: By default, the Phase 2 IDs of the local and peer device need to be configured accordingly. If the IDs configured on the two device cannot match, the negotiation will fail.

Configuring IPsec VPN Traffic Distribution and Limitation

This function is disabled by default. Before configuring, ensure that the phase 2 ID has been configured and phase 2 negotiations has been successful. After this function is enabled, the device filters the inbound and outbound traffic of the IKE tunnel according to phase 2 ID and then distributes and limits the inbound and outbound traffic. Traffic that does not match phase 2 IDs is discarded. Details are as follows:

- **Distribution**: Based on the configuration of Phase 2 IDs, the traffic distribution function can distribute the traffic at the IKE tunnel ingress interface when the traffic flow into the IKE tunnel. If the elements of source IP address, destination IP address, and the type of the traffic can match the configuration of a certain Phase 2 ID, this kind of traffic will flow into the corresponding IKE tunnel for encapsulation and sending. If the traffic cannot match any Phase 2 IDs, it will be dropped.
- **Limitation**: Based on the configuration of Phase 2 IDs, the traffic limitation function can limit the traffic at the IKE tunnel egress interface when the traffic flows out of the IKE tunnel. After the traffic was de-encapsulated, StoneOS checks the elements of source IP address, destination IP address, and the type of the traffic to see whether this kind of traffic matches a certain Phase 2 ID or not. If matched, the traffic will be dealt with. If not matched, the traffic will be dropped.

To enable the traffic distribution and limitation, use the following command in the IKE tunnel configuration mode:

check-id

Use the no form of the command to cancel this function.

Configuring Auto-connection

The device will be triggered to establish SA in two modes: auto and traffic intrigued.

- In the auto mode, the device detects the SA status every 60 seconds and initiates negotiation request when SA is not established;
- In the traffic intrigued mode, the tunnel sends negotiation requests only when there is traffic passing through the tunnel.

By default, the traffic intrigued mode is used. To use the auto mode, in the IKE tunnel configuration mode, use the following command:

auto-connect

To restore to the default mode, in the IKE tunnel configuration mode, use the command **no auto-connect**.



Notes: Auto connection works only when the peer IP is static and the local device is acting as the initiator.

Configuring DF-bit

You can specify whether to allow the forwarding device to fragment the packets. To configure DF-bit for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

df-bit {copy | clear | set}

- **copy** – Copies the IP packet DF options from the sender directly. This is the default value.
- **clear** – Allows the device to fragment packets
- **set** – Disallows the device to fragment packets.

To restore to the default value, in the IKE tunnel configuration mode, use the command **no df-bit**.

Configuring VPN Track and Redundant Backup

Hillstone devices can monitor the connectivity status of the specified VPN tunnel, and also allow backup or load sharing between two or more VPN tunnels. This function is applicable to both the route-based VPN and policy-based VPN. The practical implementation environments include:

- Configuring a backup VPN tunnel for the remote peer, at any time only one tunnel is active. Initially, the main VPN tunnel is active, if disconnection of the main tunnel is detected, the device will re-transmit the information flow through the backup tunnel;
- Configuring two or more VPN tunnels for the remote peer. All tunnels are active simultaneously, and load balance the traffic via equal-cost multi-path routing (ECMP). If disconnection of any tunnel is detected, the device will re-transmit the information flow through other tunnels.

The VPN track function tracks the status of the target tunnel by Ping packets. By default, the function is disabled. To configure the VPN track function, in IKE IPsec tunnel configuration mode, use the following command:

vpn-track [*A.B.C.D*] [**src-ip** *A.B.C.D*] [**interval** *time-value*] [**threshold** *value*]

- *A.B.C.D* – Specifies the IP address of the tracked object. When the peer is a Hillstone device and the parameter is not specified, the system will use the IP address of the peer by default. This IP address can not be 0.0.0.0 or 255.255.255.255.
- **src-ip** *A.B.C.D* – Specifies the source IP address that sends Ping packets. When the peer device is a Hillstone device and the parameter is not specified, the system will use the IP address of egress interface by default. This IP address cannot be 0.0.0.0 or 255.255.255.255.
- **interval** *time-value* – Specifies the interval of sending Ping packets. The value range is 1 to 255 seconds. The default value is 10.
- **threshold** *value* – Specifies the threshold for determining the track failure. If the system did not receive the specified number of continuous response packets, it will identify a track failure, i.e., the target tunnel is disconnected. The value range is 1 to 255. The default value is 10.

To disable the VPN track function, in IKE IPsec tunnel configuration mode, use the command **no vpn-track**.

The VPN track function can be in active or dead status. To view the VPN track status and configuration information via CLI, use the following commands:

- Show the status of VPN track: **show ipsec sa** {*id*}
- Show the configuration of VPN track: **show tunnel ipsec** {**manual** | **auto**} {*tunnel-name*}

For example:

Show the status of VPN track

hostname(config)# **show ipsec sa 5**

ID: 1

scpu: 0

VPN Name: vpn1

L2tp port: 1

Duration(S): 1375459

Last setup time: 2022-03-08 22:09:53

Last teardown time: 2022-03-09 06:09:54

Tear down reason: a lifetime timeout occurred

Teardowns today: 0

Outbound

Gateway: 1.1.1.2

.....

Sending rate(KB/s): 0

Status: Active

Inbound

Gateway: 1.1.1.2

.....

Receiving rate(KB/s): 0

Status: Active

VPN track status: alive

Show the configuration of VPN track

hostname(config)# **show tunnel ipsec auto vpn1**

Name: vpn1

mode: tunnel

.....

vpn-track: enable

tracknotify: enable

vpntrack destination 1.1.1.1

vpntrack source ip: 2.2.2.2



Tip: For more examples of VPN track and redundant backup, see Example of Configuring Route-based VPN Track and Redundant Backup.

Enabling/Disabling Notification of VPN Tunnel Status

By default, the notification of VPN tunnel status is disabled. When the notification is enabled, for route-based VPN, when system detects disconnection of a VPN tunnel, it will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route information; for policy-based VPN, when system detects disconnection of a VPN tunnel, it will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy information. You can enable/disable the tunnel state notification function via CLI, so that the system will not send any tunnel track failure notification. To enable or disable the tunnel state notification function, in the IKE IPsec tunnel configuration mode, use the following command:

- Enable: **tunnel-state-notify**
- Disable: **no tunnel-state-notify**

Specifying Description

To specify the description of IKE tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

description *string*

- *string* – Specifies the description of the IKE tunnel.

To delete the description, in the IKE IPsec tunnel configuration mode, use the command **no description**.

XAUTH

XAUTH, an extension and enhancement to IKE, allows a device to authenticate users who are trying to gain access to IPsec VPN network combined with the authentication server (RADIUS and local AAA server) configured on the device. XAUTH is now widely used on mobile devices. When a remote user initiates a request for VPN connection, the XAUTH server on the device will interrupt the VPN negotiation and prompt the user to type a valid username and password. If succeeded, the XAUTH server will go on with the subsequent VPN negotiation procedure and assign IP addresses for legal clients, otherwise it will drop the VPN connection.

If an AXUTH address pool is configured, when a client successfully connects to its server, the server will go on with the VPN negotiation procedure, take an IP address from the address pool, and assign the IP address for the legal client. If the XAUTH address pool is not configured, after the auto routing function is enabled, the device can automatically generate VPN route entries based on the configured Phase 2 ID of the IKE IPsec tunnel. For more information about the auto routing, see "VPN > IPsec Protocol > Configuring an IPsec VPN > IKEv1 VPN > Configuring a Tunnel > Configuring Auto Routing". For more information about the phase 2 ID, see "VPN > IPsec Protocol > Configuring an IPsec VPN > IKEv1 VPN > Configuring a Tunnel > Specifying a Phase 2 ID".



Tip: For more information abount how to configure an authentication server, see "Authentication".

The configuration of XAUTH includes:

- Enabling an XAUTH server
- Configuring an XAUTH address pool
- Binding an address pool to the XAUTH server
- Configuring an IP binding rule
- Configuring a WINS/DNS server

Enabling an XAUTH Server

XAUTH server is disabled by default. To enable the XAUTH server, in the ISAKMP configuration mode, use the following command:

xauth server

To disable the XAUTH server, in the ISAKMP configuration mode, use the following command:

no xauth server

Configuring an XAUTH Address Pool

This parameter is optional. XAUTH address pool is used to store IP addresses allocated to clients. When a client connects to its server, the server will take an IP address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

To configure an XAUTH IPv4 address pool, in the global configuration mode, use the following command:

xauth pool *pool-name*

- *pool-name* - Specifies a name for the IPv4 address pool, and enter the XAUTH IPv4 address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete the specified XAUTH IPv4 address pool, in the global configuration mode, use the following command:

no xauth pool *pool-name*

To configure an XAUTH IPv6 address pool, in the global configuration mode, use the following command:

xauth pool-ipv6*pool-name*

- *pool-name* - Specifies a name for the IPv6 address pool, and enter the XAUTH IPv6 address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly. Up to 16 IPv6 address pools can be configured.

To delete the specified XAUTH IPv6 address pool, in the global configuration mode, use the following command:

no xauth pool-ipv6*pool-name*

This parameter is optional. To configure the allocatable IP range of an XAUTH address pool, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

address *start-ip end-ip*{**netmask***mask* | **prefix-len***prefix*}

- *start-ip* - Specifies the start IP address.
- *end-ip* - Specifies the end IP address.
- *mask* - Specifies the network mask for the IPv4 address.
- *prefix* - Specifies the prefix length for the IPv6 address.

To delete the specified IP range of an address pool, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

no address

This parameter is optional. Some addresses in the address pool need to be reserved for other devices. These reserved IP addresses are not allowed to allocate to XAUTH clients.

To configure the start IP and end IP of reserved IP range, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

exclude-address *start-ip end-ip*

- *start-ip* - Specifies the start IP for reserved IP range.
- *end-ip* - Specifies the end IP for reserved IP range.

To delete the reserved address range, in the XAUTH address pool configuration mode, use the following command:

no exclude-address

Binding an Address Pool to the XAUTH Server

This parameter is optional. The XAUTH address pool will not take effect until being bound to an XAUTH server. To bind the specified XAUTH address pool to the XAUTH server, in the

ISAKMP configuration mode, use the following command:

xauth pool-name *pool-name*

- *pool-name* - Specifies the name of binding IPv4 address pool.

xauth pool6-name*pool-name*

- *pool-name* - Specifies the name of binding IPv6 address pool.

To cancel the binding, in the ISAKMP configuration mode, use the following command:

no xauth pool-name

no xauth pool6-name

Configuring IP Binding Rules

This parameter is optional. If an XAUTH client needs static IP address, IP-user binding rule can be applied to meet this requirement. Binding the user of XAUTH client to an IP address in the address pool can guarantee that this IP address is allocated to the XAUTH client when it reaches the server. In addition, IP address for an XAUTH client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IP addresses bound to this role.

When an XAUTH server allocates IP addresses, it follows the rules below:

1. If the client which needs a static IP has had its IP-user binding configured, the server allocates the bound IP to it. Note that if such a bound IP address is in use, the client applying for the address is not allowed to log into the server.
2. If a client uses IP-role binding rule, the server takes an IP address from the bound IP range and allocates it to the client. Otherwise, the server takes an IP address from the unbound IP range and allocates it to the client. If IP addresses in the IP range is not available, the user cannot log into the server.



Notes: IP addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

To bind an IP address to a user, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* - Specifies the username.
- **ip** *ip-address* - Specifies an available IP address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

no ip-binding user *user-name*

To bind an IP address to a role, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

ip-binding role *role-name* **ip-range** *start-ip end-ip*

- **role** *role-name* - Specifies the role name.
- **ip-range** *start-ip end-ip* - Specifies the available IP range (start IP address and end IP address) in the address pool.

To cancel a binding between an IP range and a role, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

This parameter is optional. Normally, if a user belongs to multiple roles which bind to different IP addresses, the system searches for the first rule which matches the user and applies the IP address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after***role-name2*| **top** | **bottom**}

- *role –name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a WINS/DNS Server

This parameter is optional. To specify a DNS server, in the XAUTH IPv4/IPv6 address pool configuration mode, use the following command:

dns *address1* [*address2*]

- *address1* - Specifies the IP address of DNS servers. You can specify up to two addresses.

To cancel the DNS setting, in the XAUTH address pool configuration mode, use the following command:

no dns

This parameter is optional. To specify a WINS server, in the XAUTH address pool configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* - Specifies the IP address of WINS servers. You can specify up to two addresses.

To cancel the WINS setting, in the XAUTH address pool configuration mode, use the following command:

no wins

Kicking out an XAUTH Client

The XAUTH server can force to disconnect with a client. To kick out an XAUTH client, in the execution mode, use the following command:

exec xauth *isakmp-peer-name* **kickout** *user-name*

- *isakmp-peer-name* - Specifies the ISAKMP peer name.
- *user-name* - Specifies the name of client to be kicked out of the server.

Configuring Tunnel Quota for Non-root VSYS

To configure the tunnel resource quota for non-root VSYS, use the following command in the VSYS Profile configuration mode:

tunnel-ipsec max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – Specifies the maximum quota （*max-num* **reserve**）and the reserved quota （**reserve** *reserve-num*）for the IPsec tunnel numbers of the VSYS. The maximum quota and the reserved quota differ according to different platforms. The reserved quota cannot exceed the maximum quota. The maximum quota ranges from 1 to max , and the default value is max. The minimum reserved quota is 0.



Notes: "Max" indicates the maximum number of IPSec VPN supported by the device. To view the maximum quota , use the following command in the global configuration mode: **show capacity all**

To delete the quota, use the following command in the VSYS Profile configuration mode:

notunnel-ipsec max *max-num* **reserve** *reserve-num*

Viewing IPsec Configuration

To view the configuration information of IPsec, in any mode, use the following commands:

Show the configuration information of IKEv1 P1 proposal: **show isakmp proposal** [*p1-name*]

Show the configuration information of IKEv2 P1 proposal: **show ikev2 proposal** [*p1-name*]

Show the configuration information of IKEv1 ISAKMP gateway: **show isakmp peer** [*peer-name*]

Show the configuration information of IKEv2 peer: **show ikev2 peer** [*peer-name*]

Show the configuration information of IKEv2 profile: **show ikev2 peer** [*peer-name*] **profile** [*profile-name*]

Show the configuration information of IKEv1 P2 proposal: **show ipsec proposal** [*proposal-name*]

Show the configuration information of IKEv2 P2 proposal: **show ikev2 proposal** [*proposal-name*]

Show the configuration information of manual key VPN tunnel: **show tunnel ipsec manual** [*tunnel-name*]

Show the configuration and switch information of smart link: **show ipsec smart-link-profile** [*profile-name*]

Show the configuration information of IKEv1 tunnel: **show tunnel ipsec auto** [*tunnel-name*]

Show the configuration information of IKEv2 tunnel: **show tunnel ipsec ikev2** [*tunnel-name*]

Show the information of IKEv1 P1 SA: **show isakmp sa** [*peer_ip*] [**worker** *worker-id*]

- *peer_ip* - Shows the information of IKEv1 P1 SA with the specified peer IP address.
- *worker-id* - Shows the information of IKEv1 P1 SA with the specified VPN processor.

Show the information of IKEv2 P1 SA: **show ikev2 ike-sa**

Show the information of IKEv1 P2 SA: **show ipsec sa** [*id* | **active** | **inactive**] [**worker***worker-id*]

- *id* | **active** | **inactive** - Shows the P2 SA information of IKEv1 with the specified phase 2 ID (*id*), or shows the P2 SA information of the active IKEv1 (**active**), or shows the P2 SA information of the inactive IKEv1 (**inactive**).
- **worker***worker-id* - Shows the information of IKEv1 P2 SA with the specified VPN processor.

Show the information of IKEv2 P2 SA: **show ikev2 ipsec-sa** [*sa-id*]

Show the XAUTH address pool information: **show xauth pool** [*pool-name*]

Show the XAUTH client information: **show xauth client** *isakmp-peer-name* [**user** *user-name*]

Show the statistic information of the VPN processor: **show vpnd** [*isakmp-peer-name*] **statistics** [**clear**]

- *isakmp-peer-name* - Shows the statistic information of the VPN processor with the specified ISAKMP gateway name.
- **clear** - Clear the statistic information of the VPN processor.

Show port range of the custom IKE negotiation port pool: **show ike-port-pool**

Examples of Configuring IPsec VPN

This section describes two examples of establishing SA by manual key VPN and IKE VPN respectively, an example of VPN track and redundant backup and an example of XAUTH configuration.

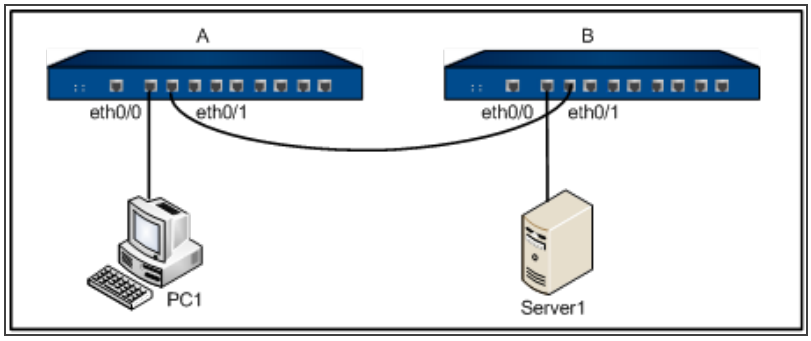
- "Example of Configuring Manual Key VPN" on Page 1478
- "Example of Configuring IKE VPN" on Page 1483
- "Example of Configuring Route-based VPN Track and Redundant Backup" on Page 1490
- "Example of Configuring Policy-based VPN Track and Redundant Backup" on Page 1498
- "Example of Configuring XAUTH" on Page 1506
- "Example of Using IPsec VPN in HA Peer Mode" on Page 1510

Example of Configuring Manual Key VPN

The manual key VPN tunnel requires that all the related SA configurations need to be completed manually. See the example below:

Requirement

There is a tunnel between Hillstone Device A and B. PC1 is a host behind Device A, with the IP address 188.1.1.2 and gateway 188.1.1.1; Server1 is the server behind Device B, with IP address 10.110.8.210 and gateway 10.110.88.220. The goal of this configuration example is to protect the communication between the subnet of PC1 (188.1.1.0/24) and the subnet of Server1 (10.110.88.0/24), using the method of route-based VPN. Use ESP as the security protocol, 3DES as encryption algorithm, SHA1 as hash algorithm and DEFLATE as compression algorithm. The network topology is shown in the following figure.



Configuration Steps

Step 1: Configure interfaces

```
Device A
  hostname(config)# interface ethernet0/0
  hostname(config-if-eth0/0)# zone trust
  hostname(config-if-eth0/0)# ip address 188.1.1.1/24
  hostname(config-if-eth0/0)# exit
  hostname(config)# interface ethernet0/1
  hostname(config-if-eth0/1)# zone untrust
```

```
hostname(config-if-eth0/1)# ip address 192.168.1.2/24
hostname(config-if-eth0/1)# exit
Device B
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.110.88.220/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/0
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 192.168.1.3/24
hostname(config-if-eth0/1)# exit
```

Step 2: Configure routes

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.110.88.0/24 192.168.1.3
hostname(config-vrouter)# exit
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 188.1.1.0/24 192.168.1.2
hostname(config-vrouter)# exit
```

Step 3: Configure a tunnel name VPN1

```
Device A
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.3
```

```
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 1234 outbound 5678
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 00ff outbound 123a
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6001 6002
hostname(config-tunnel-ipsec-manual)# exit
Device B
hostname(config)# tunnel ipsec vpn1 manual
hostname(config-tunnel-ipsec-manual)# interface ethernet0/1
hostname(config-tunnel-ipsec-manual)# protocol esp
hostname(config-tunnel-ipsec-manual)# peer 192.168.1.2
hostname(config-tunnel-ipsec-manual)# hash sha
hostname(config-tunnel-ipsec-manual)# hash-key inbound 5678 outbound 1234
hostname(config-tunnel-ipsec-manual)# encryption 3des
hostname(config-tunnel-ipsec-manual)# encryption-key inbound 123a outbound 00ff
hostname(config-tunnel-ipsec-manual)# compression deflate
hostname(config-tunnel-ipsec-manual)# spi 6002 6001
hostname(config-tunnel-ipsec-manual)# exit
```

Step 4: Configure policy rules

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Device B

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

When the settings above are completed, the security tunnel between Device A and Device B has been successfully established. Then, the data transmission between the subnet 188.1.1.0/24 and subnet 10.110.88.0/24 is encrypted.

Example of Configuring IKE VPN

This section describes an example of IKE VPN configuration.

Requirement

There is a tunnel between Hillstone Device A and B. PC1 is a host behind Device A, with the IP address 10.1.1.1 and gateway 10.1.1.2; Server1 is the server behind Device B, with IP address 192.168.1.1 and gateway 192.168.1.2. The goal of this configuration example is to protect the communication between the subnet of PC1 (10.1.1.0/24) and the subnet of Server1 (192.168.1.0/24), using the method of route-based VPN. Use ESP as the security protocol, 3DES as the encryption algorithm, SHA1 as the hash algorithm and DEFLATE as compression algorithm.

Configuration Steps

Step 1: Configure the interfaces

```
Device A
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
Device B
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# exit
```

Step 2: Configure policy rules

```
Device A
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
```

```
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
Device B
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 3: Configure routes

```
Device A
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 tunnel1
hostname(config-vrouter)# exit
Device B
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Step 4: Configure a P1 proposal

```
Device A
hostname(config)# isakmp proposal p1
```

```
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Device B

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash sha
hostname(config-isakmp-proposal)# encryption 3des
hostname(config-isakmp-proposal)# exit
```

Step 5: Configure an ISAKMP gateway

Device A

```
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.2
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# exit
```

Device B

```
hostname(config)# isakmp peer west
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 1.1.1.1
hostname(config-isakmp-peer)# pre-share hello1
```

```
hostname(config-isakmp-peer)# exit
```

Step 6: Configure a P2 proposal

```
Device A
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
Device B
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# compression deflate
hostname(config-ipsec-proposal)# exit
```

Step 7: Configure a tunnel name VPN

```
Device A
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 10.1.1.0/24 remote 192.168.1.0/24 ser-
vice any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
```

```
hostname(config-if-tun1)# exit
Device B
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.0/24 remote 10.1.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ipsec vpn
hostname(config-if-tun1)# exit
```

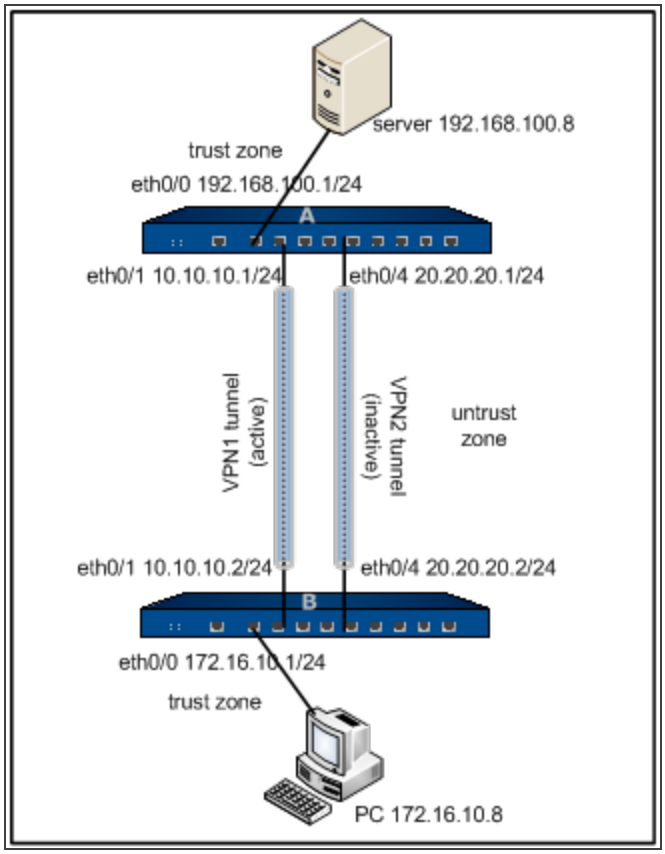
When the settings are completed, the security tunnel between Device A and Device B has been successfully established. The data transmission between the subnet 10.1.1.0/24 and subnet 192.168.1.0/24 is encrypted.

Example of Configuring Route-based VPN Track and Redundant Backup

This section describes a route-based VPN track and redundant backup example.

Requirement

There are two IKE VPN tunnels named VPN1 tunnel and VPN2 tunnel respectively between Hillstone Device A and Device B. The server is behind Device A, with the IP address of 192.168.100.8, and gateway address of 192.168.100.1; PC is behind Device B, with the IP address of 172.16.10.8, and gateway address of 172.16.10.1. The requirement is tracking the VPN status of VPN1 tunnel and VPN2 tunnel. When the main tunnel (VPN1 tunnel) link fails, traffic will be diverted to the backup tunnel (VPN2 tunnel); when the main tunnel recovers, the flow will be switched back to the main tunnel. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure Device A

Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
```

Configure a P1 proposal:

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway:

```
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
```

```
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal:

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure VPN tunnels:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
```

```
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Create tunnel interfaces and bind to the VPN tunnels:

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)#
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone untrust
hostname(config-if-tun2)# ip address 10.2.2.1/24
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel
hostname(config-if-tun2)# exit
```

Configure routes:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)#
hostname(config-vrouter)# ip route 172.16.10.0/24 tunnel2 20
hostname(config-vrouter)# exit
```

Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure Device B

```
Configure interfaces
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
hostname(config-if-eth0/4)# exit
```

Configure a P1 proposal

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway

```
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure VPN tunnels

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
```

```
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 3 threshold 9
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Create tunnel interfaces and bind to the VPN tunnels

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.1.1.2/24
hostname(config-if-tun1)# tunnel ipsec vpn1-tunnel
hostname(config-if-tun1)# exit
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone untrust
hostname(config-if-tun2)# ip address 10.2.2.2/24
hostname(config-if-tun2)# tunnel ipsec vpn2-tunnel
hostname(config-if-tun2)# exit
```

Configure routes

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel1 1
```

```
hostname(config-vrouter)# ip route 192.168.100.0/24 tunnel2 2
hostname(config-vrouter)# exit
```

Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

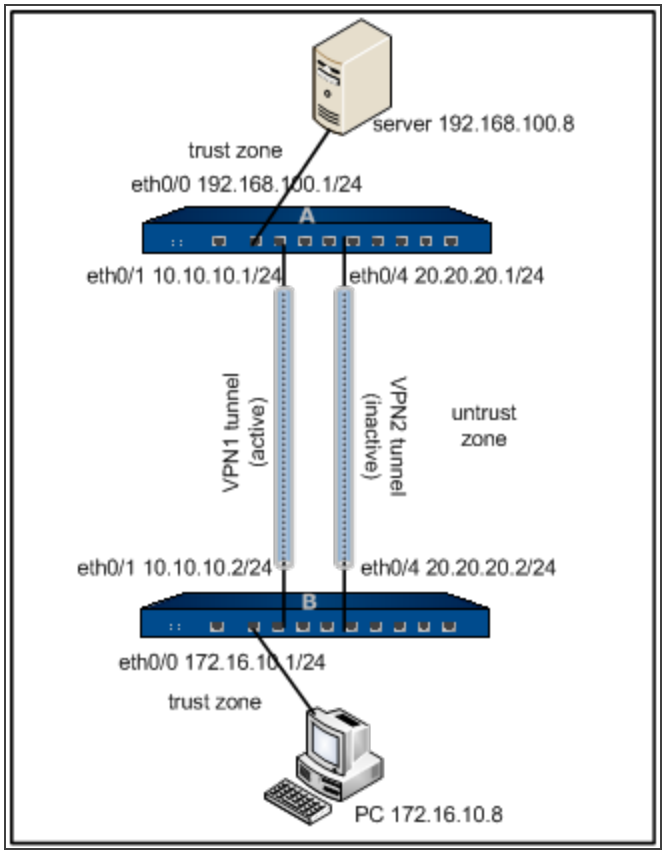
In this example both the VPN devices are Hillstone devices, so you can use the default source and destination addresses for VPN track.

Example of Configuring Policy-based VPN Track and Redundant Backup

This section describes a policy-based VPN track and redundant backup example.

Requirement

There are two IKE VPN tunnels named VPN1 tunnel and VPN2 tunnel respectively between Hillstone Device A and Device B. The server is behind Device A, with the IP address of 192.168.100.8, and gateway address of 192.168.100.1; PC is behind Device B, with the IP address of 172.16.10.8, and gateway address of 172.16.10.1. The requirement is tracking the VPN status of VPN1 tunnel and VPN2 tunnel. When the main tunnel (VPN1 tunnel) link fails, traffic will be diverted to the backup tunnel (VPN2 tunnel); when the main tunnel recovers, the flow will be switched back to the main tunnel. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure Device A

Configure interfaces:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.100.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.1/24
hostname(config-if-eth0/4)# exit
```

Configure the route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 172.16.10.0/24 20.20.20.2
hostname(config-vrouter)# exit
```

Configure a P1 proposal:

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
```

Configure an ISAKMP gateway:

```
hostname(config)# isakmp peer gwa-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.2
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwa-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.2
hostname(config-isakmp-peer)# pre-share i39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
```

Configure a P2 proposal:

```
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure a VPN tunnel:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
```

```
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
```

```
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure Device B

```
Configure interfaces:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 172.16.10.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.10.10.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone untrust
hostname(config-if-eth0/4)# ip address 20.20.20.2/24
```

```
hostname(config-if-eth0/4)# exit
Configure the route:
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.100.0/24 20.20.20.1
hostname(config-vrouter)# exit
Configure a P1 proposal:
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# hash md5
hostname(config-isakmp-proposal)# encryption des
hostname(config-isakmp-proposal)# exit
Configure an ISAKMP gateway:
hostname(config)# isakmp peer gwb-peer-1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 10.10.10.1
hostname(config-isakmp-peer)# pre-shareU8FdHNEEBz6sNn5Mvqx3yWuLRWce
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer gwb-peer-2
hostname(config-isakmp-peer)# interface ethernet0/4
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# peer 20.20.20.1
hostname(config-isakmp-peer)# pre-sharei39jnnNiCSh9rXb77oGA7Fg7BNQy
hostname(config-isakmp-peer)# exit
Configure a P2 proposal:
hostname(config)# ipsec proposal p2
```

```
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash md5
hostname(config-ipsec-proposal)# encryption des
hostname(config-ipsec-proposal)# exit
```

Configure a VPN tunnel:

```
hostname(config)# tunnel ipsec vpn1-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwb-peer-1
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1threshold 5
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2-tunnel auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer gwa-peer-2
hostname(config-tunnel-ipsec-auto)# vpn-track interval 1 threshold 5
hostname(config-tunnel-ipsec-auto)# track-event-notify enable
hostname(config-tunnel-ipsec-auto)#auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Configure policy rules:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 2
```

```
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn1-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-ip 172.16.10.8/24
hostname(config-policy-rule)# dst-ip 192.168.100.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# src-ip 192.168.100.8/24
hostname(config-policy-rule)# dst-ip 172.16.10.8/24
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn2-tunnel
hostname(config-policy-rule)# exit
hostname(config-policy)# rule id 5
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

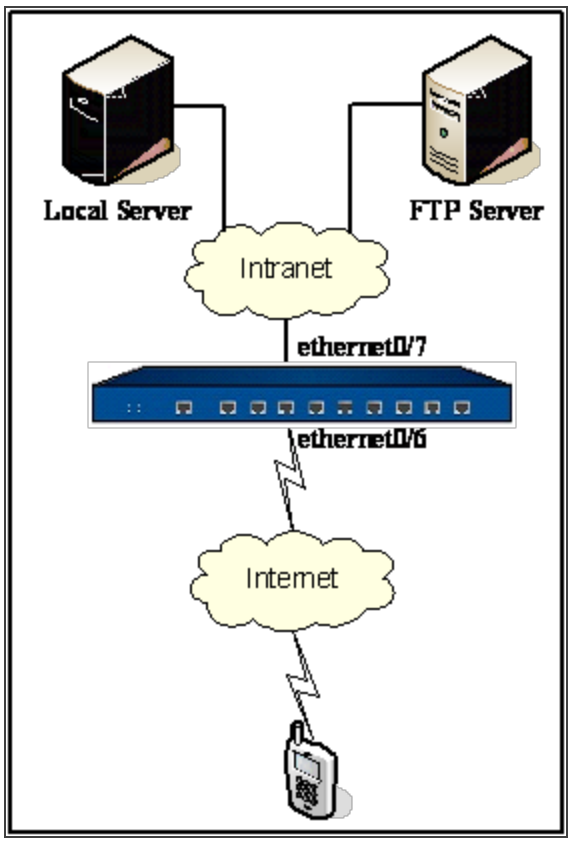
In this example both the VPN devices are Hillstone devices, so you can use the default source and destination addresses for VPN track.

Example of Configuring XAUTH

This section describes a typical XAUTH configuration example.

Requirement

Hillstone device is enabled with XAUTH server, and uses the local AAA server for user authentication. When a user is trying to launch a VPN connection and gain access to internal resources via a mobile phone, the XAUTH server will authenticate the user by a pre-shared key, and permit the authenticated users to access to internal resources. The network topology is shown in the following figure:



Configuration Steps

Step 1: Configure interfaces, zones and policies

```
hostname(config)# interface ethernet0/6
hostname(config-if-eth0/7)# zone trust
```

```
hostname(config-if-eth0/7)# ip address 6.6.6.6 255.255.255.0
hostname(config-if-eth0/7)# manage ping
hostname(config-if-eth0/7)# manage ssh
hostname(config-if-eth0/7)# manage http
hostname(config-if-eth0/7)# exit
hostname(config)# interface ethernet0/7
hostname(config-if-eth0/6)# zone untrust
hostname(config-if-eth0/6)# ip address 7.7.7.7 255.255.255.0
hostname(config-if-eth0/6)# exit
hostname(config)# rule top
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 2: Configure an AAA server

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user xauth
hostname(config-user)# password test
hostname(config-user)# ike-id key-id xauth
hostname(config-user)# end
hostname(config)#
```

Step 3: Configure an XAUTH address pool

```
hostname(config)# xauth pool pool
hostname(config-xauth-pool)# address 9.9.9.9 9.9.9.99 netmask 255.255.255.0
```

```
hostname(config-xauth-pool)# exit
hostname(config)#
```

Step 4: Configure an ISAKMP peer

```
hostname(config)# isakmp peer xauth
hostname(config-isakmp-peer)# mode aggresive
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# psk-sha-aes128-g2
hostname(config-isakmp-peer)# pre-share XhF44BilJO3b/2HFl5lVqXniqeMByq
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# local-id key-id xauth
hostname(config-isakmp-peer)# xauth pool-name pool
hostname(config-isakmp-peer)# xauth server
hostname(config-isakmp-peer)# interfaceethernet0/7
hostname(config-isakmp-peer)# exit
hostname(config)#
```

Step 5: Configure an IKE tunnel and tunnel interface

```
hostname(config)# tunnel ipsec xauth auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer xauth
hostname(config-tunnel-ipsec-auto)# esp-sha-aes128-g0
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# interface tunnel22
hostname(config-if-tun22)# zone trust
hostname(config-if-tun22)# ip address 9.9.9.1 255.255.255.0
hostname(config-if-tun22)# manage telnet
hostname(config-if-tun22)# manage ssh
```

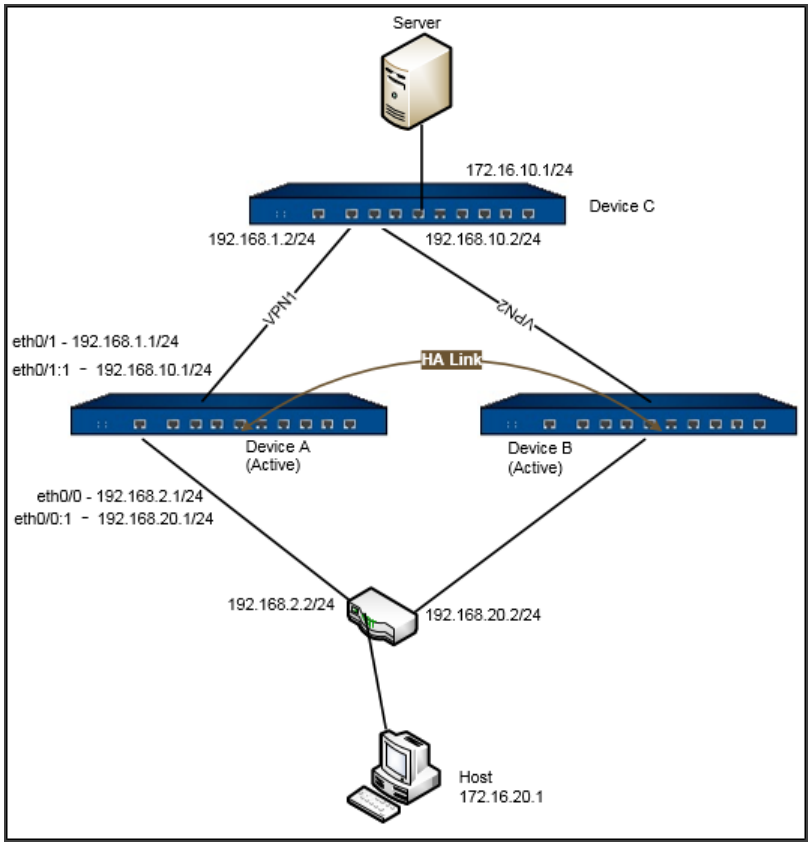
```
hostname(config-if-tun22)# manage ping
hostname(config-if-tun22)# manage http
hostname(config-if-tun22)# manage https
hostname(config-if-tun22)# manage snmp
hostname(config-if-tun22)# tunnel ipsec xauth
hostname(config-if-tun22)# exit
hostname(config)#
```

After the above steps, the mobile phone user can complete the authentication procedure via the VPN client bundled with Android or iOS (username auth, password test, IPsec identifier/group name xauth) and gain access to internal resources.

Example of Using IPsec VPN in HA Peer Mode

The HA peer mode supports IPsec VPN. By using an example, this section introduces how to integrate HA peer mode with IPsec VPN in the asymmetric routing environment. Before configuring the relevant functions, ensure that both Hillstone devices have the same hardware platform, firmware version, and license.

After completing the configurations, both devices are working in the HA peer mode and enable the IPsec VPN function. The traffic from the PC to the server is via the Device A and is secured by the IPsec VPN configured in Device A. The backward traffic from the server to the PC is via the Device B and is secured by the IPsec VPN configured in Device B. If one device or its relevant links are down, the traffic will be forwarded and secured by the other device. The topology is shown as below:



Configuration Steps

Step 1: Configure HA peer mode

Device A

```
hostname(config)# ha link interface eth0/4
hostname(config)# ha link ip 10.10.1.1/24
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
```

Device B

```
hostname(config)# ha link interface eth0/4
hostname(config)# ha link ip 10.10.1.2/24
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# exit
```

Step 2: Configure VFI interface, add router and NAT rules

Device A

```
hostname(config)# interface eth0/1:1
hostname(con-if-eth0/1:1)# zone untrust
hostname(con-if-eth0/1:1)# ip address192.168.10.1/24
hostname(con-if-eth0/1:1)# exit
hostname(config)# interface eth0/0:1
hostname(con-if-eth0/2:1)# zone trust
```

```
hostname(con-if-eth0/2:1)# ip address192.168.20.1/24
hostname(con-if-eth0/2:1)# exit
```

Step 3: Configure IPsec VPN

```
Device A
hostname(M0D1)(config)# isakmp peer peer1
hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1
hostname(M0D1)(config-isakmp-peer)# peer 192.168.1.2
hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(M0D1)(config-isakmp-peer)# pre-share hillstone
hostname(M0D1)(config-isakmp-peer)# exit
hostname(M0D1)(config)# isakmp peer peer2
hostname(M0D1)(config-isakmp-peer)# interface ethernet0/1:1
hostname(M0D1)(config-isakmp-peer)# peer 192.168.10.2
hostname(M0D1)(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(M0D1)(config-isakmp-peer)#  pre-share hillstone
hostname(M0D1)(config-isakmp-peer)# exit
hostname(M0D1)(config)# tunnel ipsec vpn1 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# tunnel ipsec vpn2 auto
hostname(M0D1)(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(M0D1)(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(M0D1)(config-tunnel-ipsec-auto)# exit
hostname(M0D1)(config)# int tunnel1
hostname(M0D1)(config-if-tun1)# zone vpn
```

```
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn1
hostname(M0D1)(config-if-tun1)# exit
hostname(M0D1)(config)# int tunnel1:1
hostname(M0D1)(config-if-tun1)# zone vpn
hostname(M0D1)(config-if-tun1)# tunnel ipsec vpn2
hostname(M0D1)(config-if-tun1)# exit
Device C
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# peer 192.168.1.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share hillstone
hostname(config-isakmp-peer)# exit
hostname(config)# isakmp peer peer2
hostname(config-isakmp-peer)# interface ethernet0/2
hostname(config-isakmp-peer)# peer 192.168.10.1
hostname(config-isakmp-peer)# isakmp-proposal psk-md5-des-g2
hostname(config-isakmp-peer)# pre-share hillstone
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)# tunnel ipsec vpn2 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer2
hostname(config-tunnel-ipsec-auto)# ipsec-proposal esp-md5-des-g2
hostname(config-tunnel-ipsec-auto)# exit
```

```
hostname(config)# int tunnel1
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsecvpn1
hostname(config-if-tun1)# exit
hostname(config)# int tunnel2
hostname(config-if-tun1)# zone vpn
hostname(config-if-tun1)# tunnel ipsec vpn2
hostname(config-if-tun1)# exit
```

Step 4: Configure policy and route for VPN

Device A

```
hostname(M0D1)(config)# ip vrouter trust-vr
hostname(M0D1)(config-vrouter)# ip route192.168.1.2/24 tunnel1
hostname(M0D1)(config-vrouter)# ip route 192.168.10.2/24 tunnel1:1
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24 192.168.2.2
hostname(M0D1)(config-vrouter)# ip route 172.16.20.0/24 192.168.20.2
hostname(M0D1)(config-vrouter)# exit
hostname(M0D1)(config)# rule id 1 from any to any service any permit
```

Device C

```
hostname(config)# ip vrouter trust-vr
hostname(config)# ip route 172.16.20.0/24 tunnel1 20
hostname(config)# ip route 172.16.20.0/24 tunnel2 10
hostname(config)# exit
hostname(config)# rule id 1 from any to any service any permit
```

SSL VPN

Overview

The device provides an SSL based remote access solution. Remote users can access the Intranet resources safely through SSL VPN.

SSL VPN requires an SSL VPN server and an SSL VPN client. SSL VPN server provides the following functions:

- Accepting connections from the client;
- Assigning IP addresses, DNS server addresses, and WIN server addresses to SSL VPN clients;
- Authenticating and authorizing SSL VPN clients;
- Security check of SSL VPN client hosts;
- Decrypting and forwarding encrypted packet from the client.

The SSL VPN client for Hillstone devices is called Hillstone Security Connect. You can download and install it on your PC. When your client has successfully connected to the SSL VPN server, your communication with the server is encrypted and secured.

The default concurrent online client number may vary from hardware platforms. If you want to have a larger client number, consult your local agents to purchase new SSL VPN license.

Configuring SSL VPN Server

This section describes the following configurations about SSL VPN server:

- Configuring an IPv4 Access Address Pool
- Configuring an IPv6 Access Address Pool
- Configuring Resources List

- Configuring a UDP Port
- Configuring an SSL VPN Instance
- Binding the SSL VPN Instance to a Tunnel Interface
- Authentication Using UKey Certificate
- Two-Step Verification
- Host Binding
- Host Check
- Optimal Path Detection
- Force Disconnecting an SSL VPN Client
- Allowing Password Change by Local Users
- Configuring Change Password URL of the Client
- Configuring Forgot Password URL of the Client
- Configuring SSL Cipher Suite
- Exporting and Importing a User-list File
- Control the Access by Using the Radius Server
- Configuring the Allowed Client Types
- General Configuration

Configuring an IPv4 Access Address Pool

Address pool is used to store IPv4 addresses allocated to clients. When a client connects to its server, the server will take an IPv4 address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

access-address-pool *pool-name*

- *pool-name* – Specifies a name for the address pool.

This command creates a new address pool and leads you into the address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete an address pool, in the global configuration mode, use the following command:

no access-address-pool *pool-name*

The following sections explain how to configure address pools, including:

- Configuring an address range and network mask of a pool
- Configuring excluded addresses
- Configuring an IP binding rule
- Configuring a DNS server
- Configuring a WINS server

Configuring an IP Range of the Address Pool

To configure the start ip, end ip and network mask of an address pool, in the IPv4 address pool configuration mode, use the following command:

address *start-ip end-ip* **netmask** *A.B.C.D*

- *start-ip* – Specifies the start IPv4 address.
- *end-ip* – Specifies the end IPv4 address.
- **netmask** *A.B.C.D* – Specifies the network mask for this IPv4 address range.

To delete the IP range setting of an address pool, in the IPv4 address pool configuration mode, use the following command:

no address

Configuring Reserved Addresses

Some addresses in the address pool need to be reserved for other devices, like gateways, FTP servers, etc. These reserved IPv4 addresses are not allowed to allocate to clients.

To configure the start IP and end IP of reserved IP range, in the IPv4 address pool configuration mode, use the following command:

exclude address *start-ip end-ip*

- *start-ip* – Specifies the start IP for reserved IP range.
- *end-ip* – Specifies the end IP for reserved IP range.

To delete the reserved address range, in the IPv4 address pool configuration mode, use the following command:

no exclude

Configuring IP Binding Rules

If an IPv4 client needs static IPv4 address, IP-user binding rule can be applied to meet this requirement. Binding the user of IPv4 client to an IPv4 address in the address pool can guarantee that this IPv4 address is allocated to the client when it reaches the server. In addition, IPv4 address for a client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IPv4 addresses bound to this role.

When an IPv4 server allocates IPv4 addresses, it follows the rules below:

1. Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
2. Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.



Notes: IPv4 addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

Binding an IP to a User

To bind an IP address to a user, in the IPv4 address pool configuration mode, use the following command:

ip-binding user *user-name* **ip** *ip-address*

- **user** *user-name* – Specifies the username.
- **ip** *ip-address* – Specifies an available IPv4 address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the IPv4 address pool configuration mode, use the following command:

no ip-binding user *user-name*

Binding an IP to a Role

To bind an IP address to a role, in the IPv4 address pool configuration mode, use the following command:

ip-binding role *role-name* **ip_range** *start-ip end-ip*

- **role** *role -name* – Specifies the role name.
- **ip_range** *start-ip end-ip* – Specifies the available IP range (start IPv4 address and end IPv4 address) in the address pool.

To cancel a binding between an IP range and a role, in the IPv4 address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IPv4 addresses, the system searches for the first rule which matches the user and applies the IPv4 address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the IPv4 address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role – name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a DNS Server

To specify a DNS server, in the IPv4 address pool configuration mode, use the following command:

dns *address1* [*address2*] [*address3*] [*address4*]

- *address1* – Specifies the IPv4 address of DNS servers. You can specify up to four addresses.

To cancel the DNS setting, in the IPv4 address pool configuration mode, use the following command:

no dns

Configuring a WINS Server

To specify a WINS server, in the IPv4 address pool configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* – Specifies the IPv4 address of WINS server. You can specify up to two WINS servers.

To cancel the WINS server setting, in the IPv4 address pool configuration mode, use the following command:

no wins

Viewing IPv4 Address Pool

To view information about an IPv4 address pool, in any mode, use the following command:

show access-address-pool [*pool-name*]

- *pool-name* – Specifies the name of IPv4 address pool to be shown. If this parameter is not specified, you can view all IPv4 address pools.

Here is an example of viewing IPv4 address pool:

```
hostname(config)# show access-address-pool pool_test1
Name: pool_test1
Address range: 3.3.3.1 - 3.3.3.10 (start IP and end IP)
Exclude range: 3.3.3.1 - 3.3.3.2 (reserved IP addresses)
Netmask: 255.255.255.0 (network mask of the address pool)
Wins server: (WINS server setting)
wins1: 10.1.1.1
Dns server:  (DNS server setting)
dns1: 10.10.209.1
IP Binding User: (IP-user binding)
test 3.3.3.8
IP Binding Role: (IP-role binding)
role1 3.3.3.3 3.3.3.7
```

To view statistical information about an IPv4 address pool, in any mode, use the following command:

show access-address-pool *pool-name* **statistics**

- *pool-name* – Specifies the name of IPv4 address pool whose statistics you want to view.

Here is an example of viewing statistics of an IPv4 address pool:

```
hostname(config)# show access-address-pool pool_test1 statistics
Total Ip Num 10 (total IP count in the address pool)
Exclude Ip Num 2 (reserved IP count)
Fixed Ip Num 6 (bound IP count)
Used Ip Num 2 (assigned IP count)
Fixed Used Ip Num 0 (assigned IP among the bound IP addresses)
Free Ip Num 6 (available IP count in the address pool)
```

Configuring an IPv6 Access Address Pool

IPv6 address pool is used to store IPv6 addresses allocated to clients. When a client connects to its server, the server will take an IPv6 address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

To creat an IPv6 address pool, in the global configuration mode, use the following command:

access-address-pool-ipv6 *pool-name*

- *pool-name* – Specifies a name for the address pool.

This command creates a new address pool and leads you into the IPv6 address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete an IPv6 address pool, in the global configuration mode, use the following command:

no access-address-pool-ipv6*pool-name*

The following sections explain how to configure IPv6 address pool, including:

- Configuring an address range and prefix of a pool
- Configuring excluded addresses
- Configuring an IP binding rule
- Configuring a DNS server

Configuring an IP Range of the Address Pool

To configure the start ip, end ip and network mask of an IPv6 address pool, in the IPv6 address pool configuration mode, use the following command:

address *start-ipv6-address end-ipv6-address* **prefix** *prefix-length*

- *start-ipv6-address* – Specifies the start IPv6 address.
- *end-ipv6-address* – Specifies the end IPv6 address.
- **prefix** *prefix-length* – Specifies the prefix for this IPv6 address range. The range is 111 to 128.

To delete the IP range setting of an address pool, in the IPv6 address pool configuration mode, use the following command:

no address

Configuring Reserved Addresses

Some addresses in the address pool need to be reserved for other devices, like gateways, FTP servers, etc. These reserved IPv6 addresses are not allowed to allocate to clients.

To configure the start IP and end IP of reserved IP range, in the IPv6 address pool configuration mode, use the following command:

exclude address *start-ipv6-address end-ipv6-address*

- *start-ipv6-address* – Specifies the start IP for reserved IP range.
- *end-ipv6-address* – Specifies the end IP for reserved IP range.

To delete the reserved address range, in the IPv6 address pool configuration mode, use the following command:

no exclude

Configuring IP Binding Rules

If an IPv6 client needs static IPv6 address, IP-user binding rule can be applied to meet this requirement. Binding the user of IPv6 client to an IPv6 address in the address pool can guarantee that this IPv6 address is allocated to the client when it reaches the server. In addition, IPv6 address for a client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IPv6 addresses bound to this role.

When an IPv6 server allocates IPv6 addresses, it follows the rules below:

1. Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
2. Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.



Notes: IPv6 addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

Binding an IP to a User

To bind an IP address to a user, in the IPv6 address pool configuration mode, use the following command:

ip-binding user *user-name* **ip** *ipv6-address*

- **user** *user-name* – Specifies the username.
- **ip** *ipv6-address* – Specifies an available IPv6 address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the IPv6 address pool configuration mode, use the following command:

no ip-binding user*user-name*

Binding an IP to a Role

To bind an IP address to a role, in the IPv6 address pool configuration mode, use the following command:

ip-binding role *role-name* **ip-range** *start-ipv6-address end-ipv6-address*

- **role** *role -name* – Specifies the role name.
- **ip-range** *start-ipv6-address end-ipv6-address* – Specifies the available IP range (start IPv6 address and end IPv6 address) in the address pool.

To cancel a binding between an IP range and a role, in the IPv6 address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IPv6 addresses, the system searches for the first rule which matches the user and applies the IPv6 address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the IPv6 address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role –name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a DNS Server

To specify a DNS server, in the IPv6 address pool configuration mode, use the following command:

dns *ipv6-address1* [*ipv6-address2*] [*ipv6-address3*] [*ipv6-address4*]

- *ipv6-address1* – Specifies the IPv6 address of DNS servers. You can specify up to four addresses.

To cancel the DNS setting, in the IPv6 address pool configuration mode, use the following command:

no dns

Viewing IPv6 Address Pool

To view information about an IPv6 address pool, in any mode, use the following command:

show access-address-pool-ipv6 [*pool-name*]

- *pool-name* – Specifies the name of IPv6 address pool to be shown. If this parameter is not specified, you can view all IPv6 address pools.

Here is an example of viewing IPv6 address pool:

```
hostname(config)# show access-address-pool-ipv6
==================================================
Name Address range Prefix length
```

```
-----------------------------------------------------------

1-ipv6-pool 1000:5678:2222~ - 1000:5678:2222~112

2-ipv6-pool 1001:5678:2222~ - 1001:5678:2222~112

3-ipv6-pool 1002:5678:2222~ - 1002:5678:2222~112

4-ipv6-pool 1003:5678:2222~ - 1003:5678:2222~112

5-ipv6-pool 1004:5678:2222~ - 1004:5678:2222~112

6-ipv6-pool 1005:5678:2222~ - 1005:5678:2222~112

============================================================-
=======

hostname(config)# show access-address-pool-ipv6 2-ipv6-pool

Name: 2-ipv6-pool

Address range: 1001:5678:2222:3333:5555:ABCD:EFAB:1000 -
1001:5678:2222:3333:5555:ABCD:EFAB:3000 (start IP and end IP)

Exclude range: 1001:5678:2222:3333:5555:ABCD:EFAB:1000 -
1001:5678:2222:3333:5555:ABCD:EFAB:2000 (reserved IPv6 addresses)

prefix length: 112 (prefix length of the address pool)

Dns server:  (DNS server setting)

dns1: AAAA:BBBB::1

dns2: 3333:2222::1
```

To view statistical information about an IPv6 address pool, in any mode, use the following command:

show access-address-pool-ipv6 *pool-name* **statistics**

- *pool-name* – Specifies the name of IPv6 address pool whose statistics you want to view.

Here is an example of viewing statistics of an IPv6 address pool:

```
hostname(config)# show access-address-pool-ipv6 2-ipv6-pool statistics

Total Ip Num 10 (total IP count in the address pool)

Exclude Ip Num 2 (reserved IP count)
```

Fixed Ip Num 6 (bound IP count)

Used Ip Num 2 (assigned IP count)

Fixed Used Ip Num 0 (assigned IP among the bound IPv6 addresses)

Free Ip Num 6 (available IP count in the address pool)

Configuring Resources List

Resource list refers to resources configured in the system that can be easily accessible by users. Each resource contains multiple resource items. The resource item is presented in the form of resource name followed by resource item name in your default browser page. After the SSL VPN user is authenticated successfully, the authentication server will send the user group information of the user to the SSL VPN server. Then, according to the binding relationship between the user group and resources in the SSL VPN instance, the server will send a resource list which the user can access to the client. After that, the client will analyze and make the default browser that your system comes with pop up a page to display the received resource list information so that the user can access the private network resource directly by clicking the resource item name. The resource list page is poped up only once after the authentication is passed. If a user does not belong to any user group, the browser will not pop up the resource list page after authentication is passed.

To configure a SSL VPN resource, in the global configuration mode, use the following command:

scvpn resource-list *list-name*

- *list-name* – Specifies the resource name. The value range is 1 to 63.

After this command is executed, you will enter SSL VPN resource list configuration mode and you can continue to configure resource items for the new resource. To delete a resource, in the global configuration mode, use the following command:

no resource-list *list-name*



Notes:

- Less than 256 resource lists can be configured.
- SSL VPN client versions that allow you to configure the resource list are as follows: SSL VPN Windows client 1.4.6.1238 or later versions, iOS 2.0.6 or later versions, and Android 4.6 or later versions.

Adding Resource Items

To add resource items for resource, in SSL VPN resource list configuration mode, use the following command:

name *name* **url** *url-string*

- *name* – Specifies the name for resource item. The value range is 1 to 95.
- *url-string* – Specifies the URL for resource item. The value range is 1 to 255.

To delete a resource item, in SSL VPN resource list configuration mode, use the following command:

no name *name*



Notes: The maximum configurable resourse entries of different platforms vary in three levels: 200 entries, 500 entries, and 1000 entries.

Viewing Resource List

To view the configuration information of resource list, in any mode, use the following command:

show scvpn resource-list [*list-name*]

- *list-name* – Specifies the resource name you want to view. The value range is 1 to 63. Information about all resources will be displayed if you keep this parameter unconfigured.

Configuring a UDP Port

To specify the UDP port number of SSL VPN connection, in the global configuration mode, use the following command:

scvpn-udp-port *port-number*

- *port-number* – Specifies the UDP port number. The value range is 1 to 65535. The default value is 4433.

When UDP port number is specified, all SSL VPN connections will communicate on this port.

To restore to the default value, in the global configuration mode, use the following command:

no scvpn-udp-port

Configuring an SSL VPN Instance

To create an SSL VPN instance, in the global configuration mode, use the following command:

tunnel scvpn *instance-name*

- *instance-name* – Specifies a name for the SSL VPN instance.

This command creates an SSL VPN instance and leads you into the SSL VPN instance configuration mode; if the instance exists, you will enter the SSL VPN instance configuration mode directly.

To delete an SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

no tunnel scvpn *instance-name*

This section describes how to configure an SSL VPN instance, including:

- Specifying the service type
- Specifying an access address pool
- Specifying a server interface

- Specifying an SSL protocol version
- Specifying a PKI trust domain
- Specifying an Encryption Trust Domain
- Specifying tunnel cipher suite
- Specifying an AAA server
- Specifying an HTTPS port number
- Configuring the transport protocol
- Configuring an SSL VPN tunnel route
- Configuring anti-replay
- Configuring packet fragmentation
- Configuring idle time
- Configuring forced logoff schedule
- Configuring multi-logon
- Configuring URL redirection
- Clearing cache data of the host that uses the SSL VPN client
- Using SSL VPN in HA peer mode
- Binding L2TP VPN instance
- Binding Resources
- Enabling/Disabling the Browser Login Function

Specifying the Service Type

By default, the service type of SSL VPN instanse is IPv4. To specify the service type of the SSL VPN instance, including IPv4 or IPv6. This command can only be configured when the version is IPv6. In the SSL VPN instance configuration mode, use the following command:

service-type {**ipv4** | **ipv6**}

- **ipv4** | **ipv6** – Specifies the service type of the SSL VPN instance, including IPv4 or IPv6.

Specifying an Access Address Pool

To specify an IPv4 address pool for the IPv4 SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

access-address-pool *pool-name*

- *pool-name* – Specifies the name of IPv4 address pool.

To cancel the IPv4 address pool, in the SSL VPN instance configuration mode, use the following command:

no access-address-pool

To specify an IPv6 address pool for the IPv6 SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

access-address-pool-ipv6 *pool-name*

- *pool-name* – Specifies the name of IPv6 address pool.

To cancel the IPv6 address pool, in the SSL VPN instance configuration mode, use the following command:

no access-address-pool-ipv6

Specifying a Server Interface

The client uses HTTPS protocol to access to the device. To specify the SSL VPN interface of the device, in the SSL VPN instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the interface for the SSL VPN client to connect.

To cancel the SSL VPN interface, in the SSL VPN instance configuration mode, use the following command:

no interface *interface-name*

Specifying an SSL Protocol Version

To specify the SSL protocol version of an SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

ssl-protocol { **tlsv1** | **tlsv1.2** | **tlsv1.3** | **gmssl** | **any**}

- **tlsv1** – Uses TLSv1 protocol.
- **tlsv1.2** – Uses TLSv1.2 protocol. This is the default option.
- **tlsv1.3** – Uses TLSv1.3 protocol.
- **gmssl** – Uses GMSSLv1.0 protocol. After selecting this option, you're recommended to select the trust domain that contains SM2 type key for the PKI trust domain and the encrypted trust domain. The SM4 is preferred for encryption algorithm and the SM3 is preferred for hash algorithm.
- **any** – Uses any of the following protocols: TLSv1, TLSv1.1, TLSv1.2 and TLSv1.3.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no ssl-protocol

If tlsv1.2 or any is specified to the SSL protocol in SSL VPN server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via SSL VPN client, so that the SSL VPN server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate.

We will take the certificate file named oldcert.pfx as an example, the procedure is as follows:

1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format: openssl pkcs12 –in oldcert.pfx –out cert.pem
2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports tlsv1.2 protocol: openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"
3. Import the newly generated .pfx format certificate into your browser or USB Key.

After the above operation, you have to log into SSL VPN server with SSL VPN client whose version is 1.4.6.1239 or later. When configuring an SSL VPN function that uses the GM standard, you need to install the SSL VPN client that supports the GM standard on the PC(The current windows client version that supports GM standard is 1.4.7.1252), and log in with the username/password of GM.

Specifying a PKI Trust Domain

PKI trust domain in SSL VPN is used in HTTPS authentication.

To specify a PKI trust domain for SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of PKI trust domain. The default domain is trust_domain_default.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no trust-domain



Tip: For information on how to create a PKI trust domain, see "PKI" in the "User Authentication"

Specifying an Encryption Trust Domain

To specify the encryption trust domain which is usded for the GMSSL negotiation for the SSL VPN, in the SSL VPN configuration mode, use the following command:

trust-domain-enc *enc-cert*

- *enc-cert* – Specifies the encryption for the GMSSL negotiation, trust domain that system pre-defined.

To delete the configured encryption trust domain, in the SSL VPN configuration mode, use the following command:

no trust-domain-enc

Specifying Tunnel Cipher Suite

Tunnel cipher suite includes encryption algorithm, authentication algorithm and compression algorithm.

To specify cipher suite for the tunnel, in the SSL VPN instance configuration mode, use the following command:

tunnel-cipher encryption {**null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4**} **hash** {**null** | **md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**} [**compression defl**]

- **null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4** – Specifies an encryption algorithm. The default value is AES. Null means no encryption is specified. For more information about encryption algorithms, see Encryption Algorithm.
- **null** | **md5** | **sha** | **sha256** | **sha384** | **sha512**| **sm3** – Specifies an authentication algorithm. The default value is MD5. Null means no authentication is specified. For more information about authentication algorithms, see Hash Algorithm.
- **compression defl** – Specifies the compression algorithm DEFALTE. The default setting is no compression. For more information on compression algorithms, see Compression Algorithm.

To restore to the default algorithm settings, in the SSL VPN instance configuration mode, use the following command:

no tunnel-cipher

Specifying an AAA Server

AAA server in SSL VPN is used for client user authentication.

To specify an AAA server, in the SSL VPN instance configuration mode, use the following command:

aaa-server *aaa-server-name* [**domain** *domain-name*] [**keep-domain-name**]

- aaa-server-name – Specifies the name of AAA server you want to use for authentication.
- **domain** *domain-name* – Specifies the domain for the AAA server so that it can be distinguished from other servers.
- **keep-domain-name** – After specifying this parameter, the AAA server uses the full name of the user, including the username and the domain name, to perform the authentication.



Notes: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication. The OAuth2 server does not support user domain name verification (**keep-domain-name**).

To cancel the AAA server in an SSL VPN, in the SSL VPN instance configuration mode, use the following command:

no aaa-server *aaa-server-name* [**domain** *domain-name*]

Specifying an HTTPS Port Number

HTTPS port is used for the clients to access the device.

To specify an HTTPS port number, in the SSL VPN instance configuration mode, use the following command:

https-port *port-number*

- *port-number* – Specifies a port number of HTTPS protocol in SSL VPN instance. The range is 1 to 65535. The default value is 4433. As Web browser uses port 443 for HTTPS, do not choose 443 as the SSL VPN HTTPS port number. If multiple SSL VPN instances use the same interface, their HTTPS ports should have different port numbers.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no https-port

Configuring the Transport Protocol

The system supports ZTNA data transmission over TCP or UDP. The default protocol is UDP, and the default port is 4433. To configure the transport protocol and port number, in the ZTNA instance configuration mode, use the following command:

transport-service {**tcp** | **udp**} *port-number*

- **tcp** | **udp** - Specifies TCP or UDP for data transmission.
- *port-number* – Specifies the port number for data transmission. The range is 1 to 65535.

To delete the transport protocol and port number, in the ZTNA instance configuration mode, use the following command:

no transport-service {**tcp** | **udp**}

Configuring an SSL VPN Tunnel Route

To reach the destination network segment or destination domain name through SSL VPN tunnel, you need to specify them by configuring the SSL VPN tunnel route.

- The specified destination network segment will be distributed to the VPN client, then the client uses it to generate the route to the specified destination.
- The specified destination domain name will be distributed to the VPN client, and the client will generate the route to the specified destination according to the resolving results from DNS.

Configuring an IPv4 Tunnel Route to the Specified Network Segment

You can only specify the IPv4 SSL VPN tunnel route for the IPv4 SSL VPN instance. To reach the destination network segment through SSL VPN tunnel, in the SSL VPN instance configuration mode, use the following command:

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

To delete a route, in the SSL VPN instance configuration mode, use the following command:

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

Configuring an IPv6 Tunnel Route to the Specified Network Segment

You can only specify the IPv6 SSL VPN tunnel route for the IPv6 SSL VPN instance. To reach the destination network segment through SSL VPN tunnel, in the SSL VPN instance

configuration mode, use the following command:

split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ipv6-address/prefix* – Specifies the IPv6 address and network mask of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

To delete a route, in the SSL VPN instance configuration mode, use the following command:

no split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

Configuring the Domain Route Function

The system will distribute the specified domain name to the client. The client will generate the route to the specified destination according to the resolving results from DNS. To specify the domain name, in the SSL VPN instance configuration mode, use the following command:

domain-route {**disable** | **enable** | **max-entries** *value* | *url*]

- **disable** – Does not distribute the specified domain name to the client. This is the default option.
- **enable** – Distributes the specified domain name to the client.
- **max-entries** *value* – The maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The default value is 1000. The value ranges from 1 to 10000.
- *url* – Specify the URL of the domain name. You can add one each time and you can add up to 64 domain names. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. **com** and **.com** are not supported.

To delete the specified domain name, use the following command in the SSL VPN instance configuration mode:

no domain-route *url*

Notes: The domain route function cannot be used together with the dedicated SSL VPN tunnel function. For more information about how to configure the dedicated SSL VPN tunnel function, see Enabling Dedicated SSL VPN Tunnel.

Enabling Dedicated SSL VPN Tunnel

The system supports the Dedicated SSL VPN Tunnel function. By default, this function is disabled. After you enable this function, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to SSL VPN.

Notes:

- The client versions that support the dedicated SSL VPN tunnel function include: the latest version of the SSL VPN client for Windows, the latest version of the SSL VPN client for macOS, and the latest version of the SSL



VPN client for Linux.

- The dedicated SSL VPN tunnel function cannot be used together with the domain route function. For more information about how to configure the domain route function, see Configuring a Tunnel Route to the Specified Domain Name.
- After you enable the dedicated SSL VPN tunnel function, we recommend that you do not configure a default route in the tunnel routing.

To enable/disable the dedicated SSL VPN tunnel function, in SSL VPN configuration mode, use the following command:

dedicated-tunnel {**enable** | **disable**}

- **enable** - Enable the dedicated SSL VPN tunnel function.
- **disable** -Disable the dedicated SSL VPN tunnel function.

Configuring Anti-replay

Anti-replay is used to prevent hackers from injecting the captured packets repeatedly by rejecting the packets.

To enable anti-replay, in the SSL VPN instance configuration mode, use the following command:

anti-replay {32 | 64 | 128 | 256 | 512}

- **32** – Specifies that the anti-replay window size is 32. This is the default value.
- **64** – Specifies that the anti-replay window size is 64.
- **128** – Specifies that the anti-replay window size is 128.
- **256** – Specifies that the anti-replay window size is 256.
- **512** – Specifies that the anti-replay window size is 512.

Bigger window size suits more in bad network conditions, such as serious packets disorder.

To restore the anti-replay window size to the default value, in the SSL VPN instance configuration mode, use the following command:

no anti-replay

Configuring Packet Fragmentation

You can specify if packet fragmentation is permitted in the device.

To configure packet fragmentation, in the SSL VPN instance configuration mode, use the following command:

df-bit {**copy** | **clear** | **set**}

- **copy** - Copies the DF value from the destination of the packet. This is the default value.
- **clear** - Permits packet fragmentation.
- **set** - Forbids packet fragmentation.

To restore to the default value, in the SSL VPN configuration mode, use the following command:

no df-bit

Configuring Idle Time

Idle time defines the time length a client is allowed to connect to the device without any operation. When a client takes no action for the time period of idle time specified here, it is forced to log out the device.

To specify the idle time, in the SSL VPN instance configuration mode, use the following command:

idle-time *time-value*

- *time-value* – Specifies the idle time value. The value range is 15 to 1500 minutes. The default value is 30.

To restore to the default value, in the SSL VPN instance configuration mode, use the following command:

no idle-time

Configuring Forced Logoff Schedule

When forced logoff schedule is configured for an SSL VPN Instance, the system forces online SSL VPN users to log out based on the periodic schedule or the timeframe. To configure the forced logoff schedule, in the SSL VPN instance configuration mode, use the following command:

kickout-all-user schedule *schedule-name*

- *schedule-name* - Specified the name of the schedule. The system forces users to log out at the start time of the timeframe.



Notes:

- The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect.
- SSL VPN users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.

Configuring Multi-logon

To allow multiple users to log in at multiple places with the same username simultaneously, in the SSL VPN configuration mode, use the following command:

allow-multi-logon

This command enables the function and does not limit the login number. If you want to specify the number of users logging in with the same username simultaneously, in the SSL VPN configuration mode, use the following command:

allow-multi-logon number *number*

- *number* – Specifies the number of users who are allowed to login with one username. The value range is 1 to 99999999.

To disable multi-login, in the SSL VPN instance configuration mode, use the following command:

no allow-multi-logon

Configuring URL Redirection

URL redirection function in SSL VPN server displays a specified URL page to the authenticated client user. By default, this function is disabled.

To enable URL redirection, in the SSL VPN instance configuration mode, use the following command:

redirect-url *url* **title** *name*

- *url* – Specifies the url address of the page shown for the new authenticated client. The value range is 1 to 255 bytes. It can be an HTTP (http://) or an HTTPS (https://) address.
- **title** *name* – Specifies a description for the redirect page. The value range is 1 to 31 bytes.

To cancel URL redirection, in the SSL VPN instance configuration mode, use the following command:

no redirect-url

URL Format

You should follow the format of redirected URL pages defined by StoneOS. The format may vary from URL types. Here are some format requirements for HTTP URL:

- For pages of UTF-8 encoding, type URL + username=$USER&password=$PWD, for example, type the address http://www.-abc.com/oa/login.do?username=$USER&password=$PWD.
- For pages of GB2312 encoding, type URL + username=$GBUSER&password=$PWD, for example, type the address http://www.-abc.com/oa/login.do?username=$GBUSER&password=$PWD.
- For other pages, type http://www.abc.com.



Notes: For configuration example of URL redirection feature, see Example of Configuring URL Redirect.

Clearing Cache Data of the Host that Uses the SSL VPN Client

For the security of the private data in the host that uses the SSL VPN client, you can clear the cache data including the cache data in the Web temporary and other temporary files. To enable this function, use the following command in the SSL VPN instance configuration mode:

host-cache-clear enable

To disable this function, use the following command in the SSL VPN instance configuration mode:

host-cache-clear disable

Using SSL VPN in HA Peer Mode

In the network environment using HA peer mode, configure SSL VPN in both Hillstone devices. When one device or its relevant links are down, the SSL VPN client can re-connect to the other device. You need to configure the reconnection address table. The SSL VPN client will re-connect to the SSL VPN server according to the priority of the reconnection address. If the SSL VPN client fails to re-connect to the server, it will try every address in the reconnection address table until it can connect to the server. You can at most specify four reconnection address. The priority is based on the order you specified. The first one you configured has the high priority and the last one you configured has the low priority. To configure the reconnection address table, use the following command in the SSL VPN instance configuration mode:

cluster { **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]] [{ **ip** *A.B.C.D* | **domain** *url* } [**port** *port-number*]]

- **ip** *A.B.C.D* | **domain** *url* – Enter the IP address or the domain name of the SSL VPN server.
- **port** *port-number* – Enter the port number that the SSL VPN server used. The default port is 4433.

Use the **no cluster** command to clear the above settings.

When using this new function, note the following matters:

- If you select the **Auto Reconnect** option in the SSL VPN client and use the client-auto-connect count command to set the reconnection times as unlimited, the SSL VPN client will only re-connect to the originally configured server, and will not re-connect to the server specified in the reconnection address table. If you set the reconnection times as X, the SSL VPN client will re-connect to the server in the table after X times of failed attempts to the originally configured server.
- If you does not select the **Auto Reconnect** option in the SSL VPN client, the SSL VPN client will directly re-connect to the server you specified in the reconnection address table
- When using the firmware that supports the using of SSL VPN in HA peer mode, the SSL VPN whose version is lower than 1.4.4.1207 can connect to the SSL VPN server if the server has no reconnection address table configured. StoneOS will inform the users to update the SSL VPN client. If the server has configured the reconnection address table, the SSL VPN whose version is lower than 1.4.4.1207 cannot connect to SSL VPN server. You need to uninstall the client and login to the SSL VPN Web Login page to download the new version of the SSL VPN client. Then install the new version. The new version is compatible with the firmware that does not support this new function.

Binding L2TP VPN Instance

When using the old version of SSL VPN client (Hillstone byod client (HBC)) for iOS to connect the SSL VPN server, you need to bind a L2TP VPN instance to the SSL VPN instance and the bound L2TP VPN needs to reference an IPSec tunnel. To configure the binding settings, use the following command in the SSL VPN instance configuration mode:

client-bind-lns *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP VPN instance you want to bind. This L2TP VPN instance needs to reference an IPSec tunnel. To cancel the binding settings, use the following command: **no client-bind-lns**

The L2TP VPN instance and the IPSec tunnel mentioned above must meet the following requirements:

- The authentication method of the IPSec tunnel must be pre-shared key authentication.
- The secret string of the L2TP instance (specified by the secret secret-string command) must be the same as pre-shared key of the IPSec tunnel.
- The AAA servers used by the L2TP instance and the SSL VPN instance must be the same.
- The address pool of the L2TP instance must be configured correctly. The device will allocate the corresponding IP addresses using the address pool of the L2TP instance.

Binding Resources

Only after binding rules between resources and user groups/roles has been configured, can the SSL VPN client make the default browser pop up a page to display the received resource list information after the authentication is passed. A user group/role can be bound with multiple resources, and a resource can also be bound with multiple user groups/roles. Only 256 binding entries can be configured in an SSL VPN instance.

To configure a binding rule, use the following command in the SSL VPN instance configuration mode:

bind resource-list *list-name* {**user-group** *aaa-server-name group-name* | **role** *role-name*}

- *list-name* – Specifies the resource name. The value range is 1 to 63.
- *aaa-server-name* – Specifies the AAA server name which the user group belongs to. Currently, only the local authentication server and the RADIUS server are available.
- *group-name* – Specifies the user group name.
- **role** *role-name* - Specifies the role name.

To cancel the binding settings, in the SSL VPN instance configuration mode, use the following command:

no bind resource-list *list-name* {**user-group** *aaa-server-name group-name* | **role** *role-name*}

Enabling/Disabling the Browser Download Function

With the browser download function, you're allowed to download the SSL VPN client via the browser WebUI. By default, the function is enabled. When this function is disabled, you can only download the SSL VPN client from www.hillstonenet.com.cn

To enable the function , in the SSL VPN instance configuration mode, use the following command:

client-download-page enable

To disable the function , in the SSL VPN instance configuration mode, use the following command:

client-download-page disable

Binding SSL VPN Instance to a Tunnel Interface

Only when an SSL VPN instance binds to a tunnel interface can it take effect.

To bind an SSL VPN instance to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel scvpn *instance-name*

- *instance-name* – Specifies the name of the SSL VPN instance you want to bind.

To cancel the binding of an SSL VPN instance, in the tunnel interface configuration mode, use the following command:

no tunnel scvpn *instance-name*

Authentication with USB Key Certificate

The client is allowed to use a USB flash disk that stores a certificate to authenticate. A USB disk which supports Windows SDK (Certificate Store Functions) and has a legal UKey certificate can pass the authentication and connect to the server.

The USB Key certificate authentication supports the following authentication methods:

- Username/Password + USB Key Certificate: SSL VPN users should have a USB Key that stores the correct digital certificate, and enter the correct user name, password and PIN code when logging in before they can pass the authentication.
- USB Key Certificate Only: SSL VPN users should have a USB Key that stores the correct digital certificate, and enter the correct PIN code when logging in to pass the authentication.



Notes: When using the authentication method of USB Key Certificate Only:

- The function of Allowing Password Change by Local User is not supported.
- The function of SMS Authentication is not supported.
- The SSL VPN client will not reconnect to the SSL VPN server automatically if the USB Key is removed.

The following sections describe how to configure USB Key certificate authentication, including:

- Enabling USB Key certificate authentication
- Importing a CA certificate to a trust domain
- Configuring a trust domain

Enabling USB Key Certificate Authentication

By default, this function is disabled. To enable the USB Key certificate authentication, in the SSL VPN instance configuration mode, use the following command:

client-cert-authentication [**usbkey-only**]

- **usbkey-only** – Specifies the USB Key authentication as USB Key only. If this parameter is not specified, the authentication of Username/Password + USB Key will be used.

To disable the function, in the SSL VPN instance configuration mode, use the following command:

no client-cert-authentication [**usbkey-only**]

Importing a USB Key Certificate to a Trust Domain

CA certificates can be imported through various methods, including downloading from an FTP or TFTP server and from USB disk. To import a certificate, in the execution mode, use the following command:

import pki *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name***password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- *trust-domain-name* – Specifies the name of PKI trust domain.
- **ftp server ip-address** [**user** *user-name* **password** *password*] – Specifies the IP address of FTP server, username and password to log in. If the server supports anonymous login, skip the username and password.
- **tftp server** *ip-address* – Specifies the IP address of TFTP server.
- **usb0 | usb1** – Specifies the port to which the USB disk is plugged.
- *file-name* – Specifies the file name of CA certificate which must be in the root directory of the USB disk.

Specifying a Trust Domain for the CA Certificate

USB Key certificate authentication requires a trust domain for the CA certificate. When the certificate provided from client matches one of the trust domain certificates, it passes authentication.

To specify a trust domain, in the SSL VPN instance configuration mode, use the following command:

client-auth-trust-domain *trust-domain*

- *trust-domain* – Specifies a configured PKI trust domain for the CA certificate. Repeat this command to add more trust domains. The system supports up to 10 domains.

To cancel a PKI trust domain for a certificate, in the SSL VPN instance configuration mode, use the following command:

no client-auth-trust-domain *trust-domain*



Tip: For information on how to create PKI trust domain, see "PKI" in the "User Authentication"

Two-Step Verification

Two-Step Verification means that when an SSL VPN user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS Authentication, Token Authentication or Email Authentication after the username and password is entered. The user must enter the random verification code received in order to log into SSL VPN and access intranet resources.

Enabling/Disabling Two-Step Verification

The two-step verification function is disabled by default. Enabling or disabling the two-step verification function, in the SSL VPN instance configuration mode, use the following command:

- Enable: **two-step verification enable**
- Disable: **two-step verification disable**

Specifying the Type of Two-Step Verification

To specify the type of the two-step verification, in the SSL VPN instance configuration mode, use the following command:

two-step verification type {**token** | **sms modem** | **sms service-provider** | **email**}

- **token**- Specifies to use the token authentication for two-step verification.
- **sms modem**- Specifies to send a short message through an SMS modem for two-step verification.

- **sms service-provider**- Specifies to send a short message through an SMS gateway for two-step verification.
- **email**- Specifies to use Email authentication for two-step verification.

Token Authentication

The system supports for authentication through the token password when logging in, and user-defined prompt information for token authentication.

Configuring Prompt Message

To configure the prompt message of the token authentication, in the SSL VPN instance configuration mode, use the following command:

token-auth prompt-message *message*

- **prompt-message** *message*- Specifies the prompt message. The range is 1 to 255 characters.

SMS Authentication

SMS authentication means that when an SSL VPN user logs in by providing a username and password, the Hillstone device, through an SMS modem or an SMS gateway, sends a dynamically generated random password to the mobile phone number of the user in SMS after the username and password is entered. The user must enter the random password received in the mobile phone in order to log into SSL VPN and access intranet resources. This section describes how to configure the global parameters for the SMS authentication function.



Notes: Not all platforms support SMS authentication.

Modem Authentication

Hillstone device adopts an external GSM modem. Before configuring the SMS authentication function, you need to prepare an SIM card and a GSM modem, and then connect the modem to the device properly. To connect the modem to the device, first, you should insert the SIM card

into the GSM modem properly; then, connect the modem to the USB port of the device via a USB cable.

The following models of SMS modem are recommended:

Model	Type	Interface
4G MODEM M1806-NC5	LTE(FDD) LTE(TDD) WCDMA TD-SCOMA GSM/GPRS/EDGE CDMA2000	USB interface
GSM MODEM M1206B	GSM	USB interface

The following sections introduce how to configure SMS authentication, including:

- Configuring a mobile phone number for SMS authentication
- Configuring expiration time of SMS auth-code
- Configuring the SMS Verification Code Length
- Configuring the SMS Verification Content
- Configuring a maximum SMS number
- Sending a test message

Configuring a Mobile Phone Number for SMS Authentication

SSL VPN local users and AD users, when assigned with a mobile phone number by the administrator, can use SMS password sent by the system to authenticate.

To configure the phone number for a local user, in the user configuration mode, use the following command:

phone *phone-number*

- *phone-number* – Specifies the mobile phone number.

To cancel a number, in the user configuration mode, use the following command:

no phone

For an AD user, configure the mobile phone number in the mobile propriety of AD server.

Configuring Expiration Time of SMS Auth-code

Each SMS authentication code has a period of validity. If the user neither types the auth-code within the period nor applies for a new code, SSL VPN server will disconnect the connection.

To configure the SMS auth-code validity period, in the SSL VPN instance configuration mode, use the following command:

sms-auth expiration *expiration*

- *expiration* – Specifies the validity period. The range is 1 to 10 minutes. The default value is 10.

To restore the validity period to the default value, in the SSL VPN instance configuration mode, use the following command:

no sms-auth expiration

Configuring the SMS Verification Code Length

To specify the length of the SMS verification code, in the SSL VPN instance configuration mode, use the following command:

sms-auth verification-code-length *length*

- *length* – Specifies the length of the SMS verification code. The range is 4 to 8 characters. The default value is 8.

In the SSL VPN instance configuration mode, use the following command to restore the default value.

no sms-auth verification-code-length

Configuring the SMS Verification Content

To specify the SMS verification content, in the SSL VPN instance configuration mode, use the following command:

sms-auth message-content *content*

- *content* – Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.

In the SSL VPN instance configuration mode, use the following command to restore the default content.

no sms-auth message-content

Configuring a Maximum SMS Number

You can specify the maximum number of SMS messages sent by the SMS modem per hour or per day. If the modem is required to send more messages than the maximum number, it will reject and record a log.

To configure the maximum SMS number, in the global configuration mode, use the following command:

sms modem {**num-per-hour** | **num-per-day**} *number*

- {**num-per-hour** | **num-per-day**} *number* – Specifies the maximum number of SMS messages per hour or per day. The value range is 1 to 1000.

If you do not limit the maximum number of SMS messages sent by the SMS modem per hour or per day, in the global configuration mode, use the following command:

no sms modem {**num-per-hour** | **num-per-day**}

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number.

To send a test message, in any mode, use the following command:

exec sms send test-message to *phone-number*

- *phone-number* – Specifies the phone number which receives the test message.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

Viewing SMS Modem Settings

To view the configuration information of an SMS modem, in any mode, use the following command:

show sms modem

SMS Gateway Authentication

Hillstone device, through SMS gateway or other proxy server, can send a short message to users in SMS after the username and password is entered. Before configuring the function, you need to ask the supplier to provide the necessary information, such as the gateway address, device ID which sends the short messages.

SMS gateway authentication configuration includes:

1. Create a Service Provider(SP) instance.
2. Bind the SP instance to a configured SSL VPN tunnel, and enable the SMS gateway authentication function.

Specifying the Default Protocol Type of SMS gateway

The types of SMS gateway protocol supported by the device include SGIP, UMS, ACC, ALIYUNSMS, XUANWU, CAS, BEIKE and HTTP(S) and ChinaMobileMusic. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. HTTP(S) indicates HTTP/HTTPS protocol, ChinaMobileMusic indicates China Mobile Music SMS Platform. To specify the default protocol type of SMS gateway, in the global configuration mode, use the following command:

sms service-provider default-protocol {**sgip** | **ums** | **acc** | **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)** | **chinamobilemusic** }

- **sgip** | **ums** | **acc** | **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)** | **chinamobilemusic** - Specifies the default protocol type of SMS gateway that the SP instance is running. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. **http(s)** indicates HTTP/HTTPS protocol. **chinamobilemusic** indicates China Mobile Music SMS Platform.

In the global configuration mode, use the command **no sms service-provider default-protocol**to cancel the specified default protocol type.

Creating an SP Instance

To create an SP instance, use the following command in the global configuration mode:

sms service-provider *sp-name* [**protocol** {**sgip** | **ums** | **acc**| **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)** | **chinamobilemusic**}]

- *sp-name* - Specifies the SP instance name. The value range is 1 to 31.
- **protocol** {**sgip** | **ums** | **acc**| **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)** | **chinamobilemusic**- Specifies the protocol of SMS gateway that the SP instance is running. System only supports SGIP of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Telecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. HTTP(S) indicates HTTP/HTTPS protocol. **chinamobilemusic** indicates China Mobile Music SMS Platform.

This command creates an SP instance and leads you into the SP instance configuration mode; if the instance exists, you will enter the SP instance configuration mode directly. The system supports at most eight SP instances now.

In the global configuration mode, use the following command to delete the specified SP instance:

no sms service-provider *sp-name*

In the SP instance configuration mode, you can configure as follows:

- Specifying the VRouter
- Specifying the Request Method
- Specifying the Charset
- Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol
- Specifying the URL
- Specifying Source Mobile Number
- Configuring Platform ID
- Configuring Platform Password
- Configuring Platform Subsystem ID
- Configuring Template ID
- Specifying the Success Code
- Specifying the Attributes
- Configuring the protocol subtype
- Specifying the Gateway Address and Port Number
- Specifying the Number to Send Auth-message
- Specifying the Device ID

- Specifying the Username and Password
- Specifying the Template Parameter
- Specifying a Maximum SMS Number
- Enabling/Disabling the Sending Sign Code Function
- Sending a test message
- Specifying the Company Code
- Specifying the AccessKeyId
- Specifying the AccessKeySecret
- Specifying Instance of SMS Gateway
- Enabling/Disabling SMS Gateway Authentication
- Specifying the Sender Name or Sign Name
- Specifying the Template Code
- Specifying the Request Type
- Specifying the Organization Code
- Specifying the SMS Service Type
- Specifying the Trading Code
- Specifying the Channel

Specifying the VRouter

The system supports multi-VR, and the default VR is trust-vr. To specify the VRouter which SP belongs to, use the following command:

vrouter {**trust-vr** | *vr-name*}

- **trust-vr** - Specifies the VR as trust-vr.
- *vr-name* – Specifies a created VR.

In SP instance configuration mode, use the following command to restore the default VR:

no vrouter {**trust-vr** | *vr-name*}

Specifying the Request Method

When the HTTP (S) protocol type is specified for the SP instance, you can specify the request method of HTTP(S). The default request method is POST. To specify the request method, in the SP instance configuration mode, use the following command:

request-type [**get** | **post**]

- **get** – Specifies the request method of HTTP(S) as GET.
- **post** – Specifies the request method of HTTP(S) as POST.

To restore the default request type, use the command **norequest-type**.

Specifying the Content Type of the HTTP(S) Packets

When the HTTP(S) protocol type is specified for the SP instance, you can specify the content type of HTTP POST request packets. The default content type is URL-ENCODE. To specify the content type of HTTP POST request packets, in the SP instance configuration mode, use the following command:

content-type { **url-encode** | **json**}

- **url-encode**- Indicates that the content type of HTTP POST request packets is application/x-www-from-urlencode.
- **json** - Indicates that the content type of HTTP POST request packets is application/json.

To restore to the default content type of HTTP POST request packets, use the command **nocontent-type**.

Specifying the Charset

When the HTTP (S) protocol type is specified for the SP instance, you can specify the charset of HTTP(S). The default charset is UTF-8. To specify the charset, in the SP instance configuration mode, use the following command:

charset [**utf-8** | **gbk**]

- **utf-8** – Specifies to use UTF-8 to encode the content of the authentication message.
- **gbk** – Specifies to use GBK to encode the content of the authentication message.

To restore the default charset, use the command **nocharset** .

Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol

To specify the protocol of UMS, ACC , ALIYUNSMS, CAS or BEIKE, in the SP instance configuration mode, use the following command:

protocol {**http** | **https**}

- **http** | **https** – Specifies the protocol type as HTTP or HTTPS. The default protocol of UMS, CAS and BEIKE is HTTPS. The default protocol of ACC and ALIYUNSMS is HTTP.

In the SP instance configuration mode, use the following command to restore the default protocol type:

no protocol

Specifying the URL

When the HTTP (S) or the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the URL of HTTP(S). You need to enter a complete access path. The system requests to communicate with the SMS gateway based on the specified URL address. To specify the URL address, in the SP instance configuration mode, use the following command:

url *url string*

- *url string* – Specifies the URL address of the SMS gateway, such as "http(s)://1.1.1.1". The range is 1 to 255 characters.

To delete the specified URL address, use the command **no url**.

Specifying Source Mobile Number

When the SP instance uses the ChinaMobileMusic protocol type, you can specify the mobile number used to send verification code messages. To configure the source mobile number, run the following command in SP instance configuration mode:

source-addr *phone-number*

- *phone-number* - Specifies the mobile number used to send verification code messages. The value can be an 8-digit to 21-digit number.

In SP instance configuration mode, run the **no source-addr** command to delete the specified source mobile number.

Configuring Platform ID

When the SP instance uses the ChinaMobileMusic protocol type, you can configure the ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. To do this, run the following command in SP instance configuration mode:

device-id *id*

- *id* - Enter the ID of China Mobile Music SMS Platform, which is a 4-digit number.

In SP instance configuration mode, run the **no device-id** command to delete the specified platform ID.

Configuring Platform Password

When the SP instance uses the ChinaMobileMusic protocol type, you can configure the password used to log in to China Mobile Music SMS Platform. The password is provided by China Mobile Music SMS Platform. To do this, run the following command in SP instance configuration mode:

device-pwd *password*

- *password* - Enter the password used to log in to China Mobile Music SMS Platform, which is 1 to 64 characters.

In SP instance configuration mode, run the **no device-pwd** command to delete the specified platform password.

Configuring Platform Subsystem ID

When the SP instance uses the ChinaMobileMusic protocol type, you can configure the subsystem ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. To do this, run the following command in SP instance configuration mode:

access-platform-id *id*

- *id* - Enter the subsystem ID of China Mobile Music SMS Platform, which is a 3-digit number or 7-digit number.

In SP instance configuration mode, run the **no access-platform-id** command to delete the specified platform subsystem ID.

Configuring Template ID

When the SP instance uses the ChinaMobileMusic protocol type, you can configure the template ID of verification code messages, which is provided by China Mobile Music SMS Platform. To do this, run the following command in SP instance configuration mode:

templet-id *id*

- *id* - Enter the template ID, which is a 1-digit to 21-digit number.

In SP instance configuration mode, run the **no templet-id** command to delete the specified template ID.

Specifying the Success Code

When the HTTP (S) protocol type is specified for the SP instance, you can specify the success code of HTTP(S). Success code is used to determine whether the SMS gateway successfully sent an authentication message. The SMS gateway sends an authentication message to the mobile phone, and when completed, it will send a message containing the status code to the system. If

the message contains the specified success code, the system will judge that the authentication message has been sent successfully. For example, if an SMS gateway sent an authentication message successfully, the status code returned is "OK: 325689", and if failed, the status number returned is "ERROR: eUser". In this instance, you can specify the success code as "OK". When the system receives a message sent by the SMS gateway, it determines whether the message contains "OK". If the message contains the specified success code, it means that the SMS gateway has sent message successfully. To specify the success code, in the SP instance configuration mode, use the following command:

success-code *string*

- *string* – Specifies the success code. The range is 1 to 50 characters. Different SMS gateways return different status code. Refer to the status code in the SMS gateway manual.

To delete the specified success code, use the command **no success-code**.

Specifying the Attributes

When the HTTP (S) protocol type is specified for the SP instance, you can configure attributes to communicate with the SMS gateway. Attributes including the parameter name of the mobile number field, the parameter name of the message content field, the password filed, and the username filed, etc. You can configure up to 32 attributes. The parameter name of the mobile number field and the parameter name of the message content field are default attributes and must be specified. The password field and other custom fields about user are optional.



Notes:

- Node name and array object can be configured only when the method is POST, content type is JSON, and parameter type is HTTP DATA.
- For the attribute fields with the same node name, the array object configurations need to be consistent.

To specify the parameter name of the mobile number field and the parameter name of the message content field, in SP instance configuration mode, use the following command:

default-attribute {**phone-attr-name***phone-attr-name* | **msg-content-attr-name***msg-content-name*} [**node***node-name*] [**add-to-array**]

- **phone-attr-name** *phone-attr-name* − Specifies the parameter name of the mobile number field, such as phone. This is the default attribute and the range is 1 to 20 characters.
- **msg-content-attr-name** *msg-content-name* − Specifies the parameter name of the message content field, such as msg. This is the default attribute and the range is 1 to 20 characters.
- **node** *node-name* - Specifies the node name of the mobile number field or message content field, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names.
- **add-to-array**- Sets the mobile number field or message content field to array object. After you specify this parameter, the parameter values are stored in array.

The system will obtain the parameter values of the mobile number field and the parameter values of the message content field when SMS gateway and the system is communicating.

When the SMS gateway and the system communicate, the SMS gateway can obtain the parameter values of the mobile number field and the parameter values of the message content field from the system. To delete the parameter name of the specified mobile number field and the parameter name of the message content field, use the command **no default-attribute** {**phone-attr-name** | **msg-content-attr-name**}.

To specify the parameters of password to log in SMS gateway, which is an optional attribute, in SP instance configuration mode, use the following command:

password-attribute {*password-name password-value*} [**node***node-name*] [**add-to-array**]

- *password-name* − Specifies the parameter name of the password, such as password. The range is 1 to 20 characters.

- *password-value* – Specifies the parameter value of the password, such as 123456. The range is 1 to 255 characters.
- **node***node-name* - Specifies the node name of the password field, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names.
- **add-to-array**- Sets the password field to array object. After you specify this parameter, the password field value is stored in array.

To delete the specified parameters of password, use the command **no password-attribute**.

To specify the custom parameter of user to log in SMS gateway, which is optional, in SP instance configuration mode, use the following command:

user-attribute {*parameter-name value*} [**add-to-header** | **node** *node-name*] [**add-to-array**]

- *parameter-name* – Specifies the parameter name of the custom parameter, such as username. The range is 1 to 20 characters.
- *value* – Specifies the value of the custom parameter, such as user1. The range is 1 to 255 characters.
- **add-to-header** – Specifies to add the custom parameter of the user to the HTTP header. If not specified, the parameter will be used as the data content of HTTP (HTTP DATA).
- **node***node-name* - Specifies the node name of the custom parameter, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names.
- **add-to-array** - Sets the custom parameter of the user to array object. After you specify this parameter, the custom parameter value is stored in array.

To delete the specified custom parameter of user, use the command **nouser-attribute** {*parameter-name*} [**add-to-header**. If **add-to-header** is specified when you configure the user attribute, you need to specify **add-to-header** when you delete the user attribute.

Configuring the Protocol Subtype

When the SP instance uses the HTTP(s) protocol type, you can configure the MAS, EMAY, or ZGC protocol subtype to connect the Hillstone device to the mobile cloud MAS SMS platform, EMAY SMS platform, or ZGC SMS platform. To configure the MAS or EMAY protocol subtype, run the following command in SP instance configuration mode:

subtype { **mas** | **emay** | **zgc**}

In SP instance configuration mode, run the **no subtype** command to delete the MAS, EMAY, or ZGC protocol subtype configuration.

When you specify the MAS protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- mobiles: In SP instance configuration mode, run the **default-attribute phone-attr-name mobiles** command to set the name of the mobile number field to mobiles. This attribute is required.
- content: In SP instance configuration mode, run the **default-attribute msg-content-attr-name content** command to set the name of the SMS content field to content. This attribute is required.
- secretKey: In SP instance configuration mode, run the **password-attribute secretKey** *password-value* command to set the name of the password used to log in to the SMS gateway to secretKey. The *password-value* can be 1 to 255 characters in length. This attribute is required.
- apId: In SP instance configuration mode, run the **user-attribute apId** *value* command to set the username used to log in to the SMS gateway to apId. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.

- ecName: In SP configuration mode, run the **user-attribute ecName** *value* command to set the name of the enterprise name field to ecName. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.
- sign: In SP instance configuration mode, run the **user-attribute sign** *value* command to set the name of the signature code field to sign. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is required.
- addSerial: In SP instance configuration mode, run the **user-attribute addSerial** *value* command to set the name of the extension code field to addSerial. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is optional.



Notes:

- When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the chartset needs to be "UTF-8".
- When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON".

Specifying the Gateway Address and Port Number

To specify the gateway address and port number, in the SP instance configuration mode, use the following command:

gateway {**host** *hostname* | **ip** *ip-address*} [**port** *port-number*]

- **host** *hostname* - Specifies the hostname of the gateway, the range is 1 to 31.
- **ip** *ip-address* - Specifies the IP address of the gateway.

- **port** *port-number* - Specifies the port number of the gateway. If this parameter is not specified, the system will use 8801 as the port number of the gateway by default. When the protocol type is specified as "SGIP", the default port number is 8801; When the protocol type is specified as "UMS", the default port number is 9600. When the protocol type is specified as "XUANWU" or "CAS", the default port number is 8080.

Execute this command for many times and the latest configuration takes effect.

In the SP instance configuration mode, use the following command to delete the gateway address and port number:

no gateway {**host** *hostname* | **ip** *ip-address*}

Specifying the Number to Send Auth-message

After enabling the SMS Authentication function, the system will send an Auth-message to the mobile phone number. In the SP instance configuration mode, use the following command to set number:

source-number *phone-number*

- *phone-number* – Specifies the user's phone number, the range is 1 to 21.

In the SP instance configuration mode, use the following command to cancel the specification of user’s phone number:

no source-number

Specifying the Device ID

Before configuring the SMS gateway, you have to ask your supplier to provide the device ID of SP, which sends the SMS messges. In the SP instance configuration mode, use the following command to specify device ID:

device-code *code-number*

- *code-number* - Specifies the device ID. The range is 1 to 4294967295.

In the SP instance configuration mode, use the following command to cancel the device ID specification:

no device-code

Specifying the Username and Password

To specify the username and password, in the SP instance configuration mode, use the following common:

user *username* **password** *password*

- *username* – Specifies the username to log in SMS gateway. The range is 1 to 64. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
- *password* – Specifies the password for the user. The range is 1 to 64. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.

In SP instance configuration mode, use the following command to cancel the specificantion of username and password:

no user *username* **password** *password*

Specifying the Template Parameter

To specify the template parameter of BEIKE SMS gateway, in the SP instance configuration mode, use the following command:

template *value*

- *value* – Specifies the template parameter of BEIKE SMS gateway. The length is 1 to 64 characters.

In SP instance configuration mode, use the following command to delete the template parameter of BEIKE SMS gateway:

no template

Specifying a Maximum SMS Number

You can specify the maximum number of SMS messages sent by the SMS gateway per hour or per day. To configure the maximum SMS number, in the SP instance configuration mode, use the following command:

{**num-per-hour** | **num-per-day**} *number*

- *number* – Specifies the maximum number of SMS messages per hour or per day. The value range is 0 to 65535.

In the SP instance configuration mode, use the following command to cancel the maximum number:

no {**num-per-hour** | **num-per-day**}

Enabling/Disabling the Sending Sign Code Function

When this function is enabled, the ACC SMS gateway will add a sign code field when sending a request to the ACC server, which will prevent the content of the SMS from being tampered with. In the SP instance configuration mode, use the following command to enable the sending sign code function:

sign enable

In the SP instance configuration mode, use the following command to disable the sending sign code function:

no sign enable

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number. To send a test message, in any mode, use the following command:

exec sms sp *sp-name tunnel-name* **sendtest-message to** *phone-number*[**test-msg-content** *content*]

- *phone-number* – Specifies the phone number.
- *tunnel-name* – Specifies the tunnel name which bound the SP instance.

- *content* – Specifies the content of the test message. The default value is "This is a test message, please don't feedback!". The range is 1 to 64 characters.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

Specifying the Company Code

When the SP instance uses the UMS protocol type, users can specify the enterprise code registered on the UMS platform, in the SP instance configuration mode, use the following command:

spcode *spcode-number*

- *spcode-number* - Specifies the company code. The range is 1 to 31 digits.

In the SP instance configuration mode, use the following command to cancel the company code:

no spcode

Specifying the AccessKeyId

If the protocol of SMS gateway that the SP instance is running is ALIYUNSMS, users must specify the AccessKeyId which will be used as the username for authentication between the device and the SMS gateway of Alibaba Cloud . To specify the AccessKeyId, in the SP instance configuration mode, use the following command:

accesskeyid *word*

- *word* - Specifies the AccessKeyId. The range is 1 to 64 characters. This parameter should be the same with the template AccessKeyId applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the **no accesskeyid** command to cancel the specified AccessKeyId.

Specifying the AccessKeySecret

If the protocol of SMS gateway that the SP instance is running is ALIYUNSMS, users must specify the AccessKeySecret which will be used as the password for authentication between the

device and the SMS gateway of Alibaba Cloud. To specify the AccessKeySecret, in the SP instance configuration mode, use the following command:

accesskeysecret *word*

- *word* - Specifies the AccessKeySecret. The range is 1 to 63 characters. This parameter should be the same with the template AccessKeySecret applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the **no accesskeysecret** command to cancel the specified AccessKeySecret.

Specifying Instance of SMS Gateway

The SP instance needs to be bound to the SSL VPN tunnel to take effect. To specify the SMS gateway instance, in the SSL VPN instance configuration mode, use the following command:

sms-auth enable servicer-provider *sp-name*

- *sp-name* – Specifies the name of the SP instance, which must be the created SP instance. The value range is 1 to 31 characters.

Enabling/Disabling SMS Gateway Authentication

The SP instance should be bound to SSL VPN tunnel so that it can take effect. By default, the SMS gateway authentication is disabled. In the SSL VPN instance configuration mode, use the following command to enable the SMS gateway authentication function:

sms-auth enable *sp-name*

- *sp-name* – Specifies the SP instance name, which should be a created SP. The range is 1 to 31.

In the SSL VPN instance configuration mode, use the following command to disable the function:

sms-auth disable *sp-name*

Specifying the Sender Name or Sign Name

If the protocol of the SP instance bound to SSL VPN tunnel is SGIP, USM or ACC, users can specify a message sender name to display in the message content. If the protocol of the SP instance bound to SSL VPN tunnel is ALIYUNSMS, users must specify the sign name applied in the SMS of Alibaba Cloud to display in the message content. To specify the sender name or sign name, in the SSL VPN instance configuration mode, use the following command:

sms-auth sms-sender-name *sender-name*

- *sender-name* – Specifies the sender name. The range is 1 to 63 characters. The sign name should be the same with the sign name applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the following command to cancel the specified sender name or sign name:

no sms-auth sms-sender-name



Notes: Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.

Specifying the Template Code

If the protocol of the SP instance bound to SSL VPN tunnel is ALIYUNSMS, users must specify the code of the SMS template applied in the SMS of Alibaba Cloud. To specify the template code, in the SSL VPN instance configuration mode, use the following command:

sms-auth sms-msg-templatecode *word*

- *word* – Specifies the template code. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the following command to cancel the specified template code:

no sms-auth sms-msg-templatecode

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number. To send a test message, in any mode, use the following command:

exec sms sp sp-name *tunnel-name* **send test-message to** *phone-number*

- *sp-name* – Specifies the SP name.
- *phone-number* – Specifies the phone number.
- *tunnel-name* – Specifies the tunnel name which bound the SP instance.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

Specifying the Request Type

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the request type. To specify the request type, in the SP instance configuration mode, use the following common:

post_type *post_type*

- *post_type* – Specifies the request type. The range is 1-6.

In the SP instance configuration mode, use the following command to cancel the request type:

no post_type

Specifying the Organization Code

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the organization code. To specify the organization code, in the SP instance configuration mode, use the following common:

orgcode *orgcode*

- *orgcode* – Specifies the organization code. The range is 1-31.

In the SP instance configuration mode, use the following command to cancel the organization code:

no orgcode

Specifying the SMS Service Type

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the SMS service type. To specify the SMS service type, in the SP instance configuration mode, use the following common:

smstype *smstype*

- *smstype* – Specifies the SMS service type. The range is 1-31.

In the SP instance configuration mode, use the following command to cancel the SMS service type:

no smstype

Specifying the Trading Code

If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the trading code. To specify the trading code, in the SP instance configuration mode, use the following common:

trading_code *trading-code*

- *trading-code* – Specifies the trading code. The range is 1-7.

In the SP instance configuration mode, use the following command to cancel the trading code:

no trading_code

Specifying the Channel

If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the channel. To specify the channel, in the SP instance configuration mode, use the following common:

channel *channel-value*

- *channel-value* – Specifies the channel. The range is a-z.

In the SP instance configuration mode, use the following command to cancel the channel:

no channel

Viewing SMS Gateway Settings

To view the SMS gateway configurations, use the following command in any mode:

show sms service-provider [*sp-name*]

- *sp-name* – Specifies the SP instance name. If not specified, the system will show all the SP instance configurations that have already created.

Viewing SMS Statistic Information

To view the statistic information that indicates the SMS message is failed or succeed, use the following command in any mode:

show tunnel scvpn *scvpn-name* **smsp-statistice** [**clear**]

- *scvpn-name* – Specifies the SSL VPN instance name that exists.
- **clear** – Clear all the statistic information.

Email Authentication

Email Authentication means that when an SSL VPN user logs in by providing a "username/password" or a "username/password+Digital Certificate", Hillstone device, through a mail server, can automatically send a Email containing random verification code to the user after the username and password is entered. The user must enter the random verification code received in order to log into SSL VPN and access intranet resources.

Configurations of Email authentication on SSL VPN server include:

- Configuring the Email Address
- Specifying the Email Server

- Configuring the Verification Code Length
- Configuring the Lifetime of Email Verification Code
- Configuring the Sender Name
- Configuring the Email Verification Content

Configuring the Email Address

Users can receive the verification code via Email address configured on a local server or a Radius server.

When receiving the verification code via Email address configured on a local server, to configure the Email address, in the user configuration mode, use the following command:

email *email-address*

- *email-address* - Specifies the Email address used to receive the verification code. The range is 1 to 127 characters.

In the user configuration mode, use the **no email** command to cancel the specified Email address.

When receiving the verification code via Email address configured on a Radius server, users need to configure the Email address on the Radius server. Take FreeRadius as an example:

```
"test1" Cleartext-Password: ="123456"
Login-LAT-Group="radiusgroup1",
Hillstone-user-type=16,
Hillstone-user-vsys-id=0,
Hillstone-user-login-type=63,
Hillstone-user-admin-privilege=4294967295,
Hillstone-user-email=user-test@hillstonenet.com ( Add the
attribute value of Hillstone-user-email in "etc/-
freeradius/users".)
```

Specifying the Email Server

To specify the existing Email server which the Email address that used to send the verification code is configured on, in the SSL VPN instance configuration mode, use the following command:

email-auth smtp-server *smtp-server-name*

- *smtp-server--name* - Specifies the existing Email server which the Email address that used to send the verification code is configured on,. The range is 1 to 31 characters.

In the SSL VPN instance configuration mode, use the **no email-auth smtp-server** command to cancel the specified Email server.

Configuring the Verification Code Length

To specify the length of the Email verification code, in the SSL VPN instance configuration mode, use the following command:

email-auth verification-code-length *length*

- *length* - Specifies the length of the Email verification code. The range is 4 to 8 characters. The default value is 8.

In the SSL VPN instance configuration mode, use the **no email-auth verification-code-length** command to restore the default value.

Configuring the Lifetime of Email Verification Code

Each Email verification code has a period of validity. If the user neither types the code within the period nor applies for a new code, SSL VPN server will disconnect the connection.

To the lifetime of the Email verification code, in the SSL VPN instance configuration mode, use the following command:

email-auth expiration *value*

- *value* – Specifies the lifetime of the Email verification code. The range is 1 to 10 minutes. The default value is 10.

In the SSL VPN instance configuration mode, use the **no sms-auth expiration** command to restore the default value.

Configuring the Sender Name

To specify a verification code sender name to display in the Email content, in the SSL VPN instance configuration mode, use the following command:

email-auth sender-name *name*

- *name* - Specifies a verification code sender name to display in the Email content. The range is 1 to 63 characters. The default value is "hillstone". In order to prevent the mail from being identified as spam, it's recommended that users to configure the sender name.

In the SSL VPN instance configuration mode, use the **no email-auth sender-name** command to restore the default value.

Configuring the Email Verification Content

To specify the Email verification content, in the SSL VPN instance configuration mode, use the following command:

email-auth message-content *content*

- *content* - Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".

In the SSL VPN instance configuration mode, use the **no email-auth message-content** command to restore the default content.

Host Binding

Host binding is used to authenticate the hosts of SSL VPN clients. When you use the SSL VPN client to log into the server, the client collects information about the PC running it, including mainboard SN, hardware SN, CPU ID and BIOS SN, and uses MD5 algorithm to generate a 32-bit string, which is the host ID. Then, the client sends the host ID with username and password to the SSL VPN server for authentication. The SSL VPN server authenticates the user by looking up the candidate list and binding list.

The candidate list and binding list are described as below:

- Candidate list: A table recording username and host ID as well as their mapping relationship.
- Binding list: A table of authorized host IDs and their usernames. You can add a pair of host ID and its username to the table or allow login user to be added automatically. When a client logs in, the SSL VPN server checks if the binding list has the host ID and matched username, if so, the user passes authentication; if not, the SSL VPN communication will be disconnected.

Note: For hosts deployed on virtual platforms, the host ID might not be unique. Therefore, the host binding function might not work properly.

Enabling Host Binding

By default, host binding is disabled. To enable host binding, in the SSL VPN instance configuration mode, use the following command:

user-host-verify [**allow-multi-host**] [**allow-shared-host**] [**auto-approved-first-bind**]

- **user-host-verify** – Enables host binding. By default, a user is allowed to log into the server using one single computer.
- **allow-multi-host** – Allows one user to log in using multiple hosts.
- **allow-shared-host** – Allows multiple users to log in using one host.

- **auto-approved-first-bind** – Specifies that the server automatically adds the username and host ID to the binding list when the user logged in for the first time.

To disable host check, in the SSL VPN instance configuration mode, use the following command:

no user-host-verify

Approving a Candidate

Approving a pair of host ID and user in the candidate list means to add it to the binding list. To approve a candidate, in any mode, use the following command:

exec scvpn *instance-name* **approve-binding user** *user-name* **host** *host-id*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the username in the candidate list.
- **host** *host-id* – Specifies the host ID of the user.

Configuring a Super User

A super user can log into the server using any host. To change a user in candidate or binding list to a super user, in any mode, use the following command:

exec scvpn *instance-name* **no-host-binding-check user** *user-name*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user who will be changed to a super user. The length is 1 to 95 characters.

To cancel a super user, in any mode, use the following command:

exec scvpn *instance-name* **host-binding-check user** *user-name*

Configuring a Shared Host

If a host is considered as a shared host, users logging into the server from this host are not limited by host binding authentication. To configure a host in candidate or binding list as a shared host, in any mode, use the following command:

exec scvpn *instance-name* **no-user-binding-check host** *host-id*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **host** *host-id* – Specifies the ID of the host which will be changed to a shared host. The host must be in the candidate list or binding list.

To cancel a shared host, in any mode, use the following command:

exec scvpn *instance-name* **user-binding-check host** *host-id*

Increasing/Decreasing Pre-approved Hosts

Even when multi-host login is allowed for a user, by default, the system only records the first login host-user pair into its binding list; other login pairs are in the candidate list. However, the host-user binding pair number in the binding list can be changed.

To increase the pre-approved host-user binding pair number, in any mode, use the following commands:

exec scvpn *instance-name* **increase-host-binding user** *user-name number*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user.
- *number* – Specifies the number of pre-approved host-user binding pairs to be added to the binding list for the user. The number ranges from 1 to 32. The total number of pre-approved host-user binding pairs in a binding list ranges from 0 to 100.

exec scvpn *instance-name* **decrease-host-binding user** *user-name number*

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user.
- *number* – Specifies the number of pre-approved host-user binding pairs to be decreased in the binding list for the user. The number ranges from 1 to 32. The total number of pre-approved host-user binding pairs in a binding list ranges from 0 to 100.

Clearing a Binding List

To clear a binding list or an entry in the table, in any mode, use the following command:

exec scvpn *instance-name* **clear-binding** [{**user** *user-name* [**host** *host-id*] | **host** *host-id* }]

- **scvpn** *instance-name* – Specifies the name of SSL VPN instance.
- **user** *user-name* – Specifies the name of user. If the next parameter is not defined, all hosts bound to this user will be cleared.
- **host** *host-id* – Specifies the host ID of the host which will be cleared.

Exporting/Importing a Binding List

The binding list can be exported to (and imported from) an FTP server, TFTP server or USB disk.

To export a binding list, in the execution mode, use the following command:

export scvpn user-host-binding to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – Specifies that the table is exported to an FTP server. Type the IP address of FTP server. Type username and password if needed; if the server supports anonymous login, skip user name and password.
- **tftp server** *ip-address* – Specifies that binding list is exported to a TFTP server. Type the IP address of the TFTP server.
- **usb0 | usb1** – Exports the binding list to the root directory of the USB disk.
- *file-name* – Specifies a name for the file of exported binding list.

To import a binding list, in the execution mode, use the following command:

import scvpn user-host-binding from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} [*file-name*]

- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – Specifies that the table is imported from an FTP server. Type the IP address of FTP server. Type username and password if needed; if the server supports anonymous login, skip user name and password.
- **tftp server** *ip-address* – Specifies that binding list is imported from a TFTP server. Type the IP address of the TFTP server.
- **usb0 | usb1** – Imports the binding list from the root directory of the USB disk.
- *file-name* – Specifies the file name of imported binding list.

Host Check

The host check function checks the security status of the hosts running SSL VPN clients, and according to the checking result, the SSL VPN server will determine the security level for each host and assign corresponding resource access permission based on their security level. The checked factors are operating system, IE version, and the installation of some specific software.

Checked Factors

The factors to be checked by the SSL VPN server are displayed in the list below:

Factor	Description
Operating system	• Operating system, e.g., Windows 2000, Windows 2003, Windows XP, Windows Vista, etc. • Service pack version, e.g., Service Pack 1 • Windows patch, e.g., KB958215, etc.
	• Whether the Windows Security Center and Automatic Update is enabled. • Whether the installation of AV software is compulsory, and whether the real-time monitor and the auto update of signature database are

Factor	Description
	enabled • Whether the installation of anti-spyware is compulsory, and whether the real-time monitor and the online update of signature database are enabled • Whether the personal firewall is installed, and whether the real-time protection is enabled
Other configurations	Whether the IE version and security level reach the specified requirements
	Whether the specified processes are running
	Whether the specified services are installed
	Whether the specified services are running
	Whether the specified registry key values exist
	Whether the specified files exist in the system

Role Based Access Control and Host Check Procedure

Role Based Access Control (RBAC) means that the permission of the user is not determined by his user name, but his role. The resources can be accessed by a user after the login is determined by his corresponding role. So role is the bridge connecting the user and permission.

The SSL VPN host check function supports RBAC. And the concepts of primary role and guest role are introduced in the host check procedure. The primary role determines which host check profile (contains the host check contents and the security level,can be configured via WebUI) will be applied to the user and what access permission can the user have if he passes the host check. And the guest role determines the access permission for the users who failed in the host check. For more information about role and host check, see the Table 7: Relationship between Host Check Rule and Check Results.

The host check procedure is:

1. The SSL VPN client sends request for connection and passes the authentication.
2. The SSL VPN server sends host check profile to the client.
3. The client checks the host security status according to the host check profile. If it failed in the host check, the system will notify the check result.
4. The client sends the check result back to the server.
5. If the host check succeeds, the server will assign access permissions based on the primary role defined in the host check profiles; if the host check fails, the server will disconnect the client and issue a prompt, or assign access permissions based on the guest role defined in the host check profile.

The host check function also supports dynamic access permission control. On one side, when the client's security status changes, the server will send a new host check profile to the client to make it re-check; on the other side, the client can perform the security check periodically, e.g., if the AV software is disabled and it is detected by the host check function, the assigned role to the client may changed, and so does the access permission.

Configuring a Host Check Profile

Host check profile defines the checking contents and security level. You can use WebUI or CLI to create a host check profile, but the detailed settings of that profile can only be done in the WebUI.

To create a host check profile, in the global configuration mode, use the following command:

scvpn host-check-profile *hostcheck-profile-name*

- *hostcheck-profile-name* – Specifies a name for the host check profile.

To delete a host check profile, in the global configuration mode, use the following command: **no scvpn host-check-profile** *hostcheck-profile-name*.

Configuring a Host Check Profile via WebUI

To create a host check profile via WebUI, take the following steps:

1. On the Navigation pane, click **Configure** > **Network** > **SSL VPN** to visit the SSL VPN page.
2. On the Task tab in the right auxiliary pane, click **Host Check** to visit the Host Check page.
3. Click **New**.
4. On the **Basic** and **Advanced** tabs, configure the following options.

   Options on the **Basic** tab:

   - **Name:** Specifies the name of the host check profile.
   - **OS version:** Specifies whether to check the OS version on the client host. Click one of the following options:
     - **No check** - Do not check the OS version.
     - **Must match** - The OS version running on the client host must be the same as the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
     - **At least** - The OS version running on the client host should not be lower than the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
   - **Patch X:** Specifies the patch that must be installed on the client host. Type the patch name into the box. Up to five patches can be specified.
   - **Lowest IE version:** Specifies the lowest IE version in the Internet zone on the client host. The IE version running on the client host should not be lower than the version specified here.
   - **Lowest IE security level:** Specifies the lowest IE security level on the client host. The IE security level on the host should not be lower than the level specified here.

Options on the **Advanced** tab:

- **Security center:** Checks whether the security center is enabled on the client host.
- **Auto update:** Checks whether the Windows auto update function is enabled.
- **Anti-Virus software:** Checks if the client host has installed anti-virus software and others, including:
    - **Installed** - The client host must have the AV software installed.
    - **Monitor** - The client host must enable the real-time monitor of the AV software.
    - **Virus signature DB update** - The client host must enable the signature database online update function.
- **Anti-Spyware software:** Checks if the client host has installed anti-spyware and others, including:
    - **Installed** - The client host must have the anti-spyware installed.
    - **Monitor** - The client host must enable the real-time monitor of the anti-spyware.
    - **Signature DB update** - The client host must enable the signature database online update function.
- **Firewall:** Checks if the client host has installed firewall and others, including:
    - **Installed** - The client host must have the personal firewall installed.
    - **Monitor** - The client host must enable the real-time monitor function of the personal firewall.

- **Registry key value: Key X:** Checks whether the key value exists. Up to five key values can be configured. The check types are:
  - **No check** - Do not check the key value.
  - **Exist** - The client host must have the key value. Type the value into the box.
  - **No exist** - The client does not have the key value. Type the value into the box.
- **File path name: File X:** Checks whether the file exists. Up to five files can be configured. The check types are:
  - **No check** - Do not check the file.
  - **Exist** - The client host must have the file. Type the file name into the box.
  - **No check** - The client does not have the file. Type the file name into the box.
- **Running process name: Process X:** Checks whether the process is running. Up to five processes can be configured. The check types are:
  - **No check** - Do not check the process.
  - **Exist** - The client host must have the process running. Type the process name into the box.
  - **No exist** - The client cannot have the process running. Type the process name into the box.
- **Installed service name:** Checks whether the service is installed. Up to five services can be configured. The check types are:
  - **No check** - Do not check the service.
  - **Exist** - The client host must have the service installed. Type the service name into the box.

- **No exist** - The client host cannot have the service installed. Type the service name into the box.

- **Running service name:** Checks whether the service is running. Up to five services can be configured. The check types are:

  - **No check** - Do not check the service.

  - **Exist** - The client host must have the service running. Type the service name into the box.

  - **No exist** - The client host cannot have the service running. Type the service name into the box.

5. Click **OK** to save the settings.

Referencing a Host Check Profile to a Rule

To make the configured host check profile take effect, you must bind the profiles to the host check rules. And then the host check function will work in the system.

To configure a host check rule, in the SSL VPN instance configuration mode, use the following command:

host-check [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name* |**redirect-url** *url*] [**periodic-check** *period-time*]

- **role** *role-name* – Specifies a configured role in AAA server as the primary role for the user. If this parameter is defined, the host check profile works for this role; if not, the profile is the default profile and serves all users.

- **profile** *profile-name* – Specifies the name of the bound host check profile.

- **guest-role** *guestrole-name*|**redirect-url** *url*- Specifies the exception handling method.

  - **guest-role** *guestrole-name* – Specifies the guest role. If the client host fails in host check, this parameter enables the user to own the privileges of this guest role; if this

parameter is not defined, the client will be disconnected.

- **redirect-url** *url*- Specifies the redirect URL. If the client host fails in host check, this parameter enables the browser jump to the specified URL , and guide the user to download the software required for host security detection and disconnect the client; if this parameter is not defined, the client will be disconnected.

- **periodic-check** *period-time* − Specifies the auto-check period of the user. The value range is 5 to 1440 minutes. The default value is 30.

Repeat this command to add more host check rules. If a user matches multiple host check rules, the server uses the first matched rule; in addition, if a user binds to multiple roles with matched host check rules, the server uses the first matched rule.

Repeat this command to add more host check rules. If a user matches multiple host check rules, the server uses the first matched rule; in addition, if a user binds to multiple roles with matched host check rules, the server uses the first matched rule.

To cancel the host check rule setting, in the SSL VPN instance configuration mode, use the following command:**no host-check** [**role** *role-name*] **profile** *profile-name* [**guest-role** *guestrole-name*|**redirect-url** *url*] [**periodic-check** *period-time*].

The table below lists the relationship between the policy rule and host check result.

Rule Setting	Check Result	
	Successful	Failed
Primary role: configured Profile: configured Guest role: configured Redirect URL: not configured	Obtain privileges of primary role	Obtain privileges of guest role
Primary role: configured Profile: configured Guest role: not configured Redirect URL: configured	Obtain privileges of primary role	The browser jump to the specified URL , and guide the user to download the software required for host

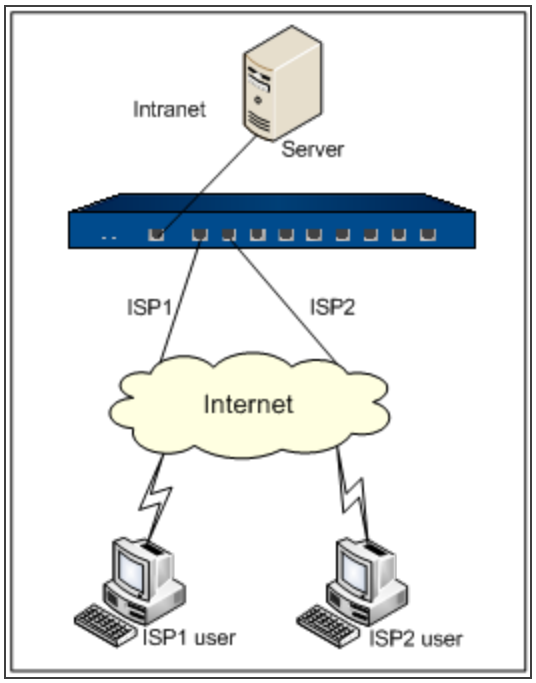
Rule Setting	Check Result	
	Successful	Failed
		security detection and disconnect the client
Primary role: configured Profile: configured Guest role: not configured Redirect URL: not configured	Obtain privileges of primary role	Be disconnected
Primary role: not configured Profile: configured Guest role: configured Redirect URL: not configured	In connection	Obtain privileges of guest role
Primary role: not configured Profile: configured Guest role: not configured Redirect URL: configured	In connection	The browser jump to the specified URL , and guide the user to download the software required for host security detection and disconnect the client
Primary role: not configured Profile: configured Guest role: not configured Redirect URL: not configured	In connection	Be disconnected

Selecting an Optimal Path

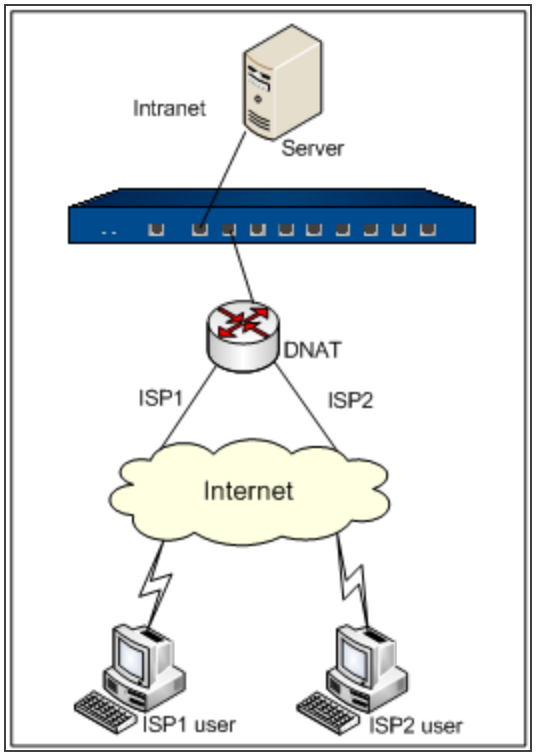
VPN networks with multiple ISPs (Internet Service Provider) can be greatly influenced by the defects of narrow bandwidth and long delay in communication among different ISPs. To solve the

issue, the Hillstone device provides optimal path check feature which enables the device to automatically select the fastest path for the client to connect to SSL VPN server.

There are two designs of network implementation for you to use optimal path selection feature.



As shown in the figure above, SSL VPN client visits the egress interface of the server. Firstly, the SSL VPN server needs to apply for different ISP services and enable interfaces for each of the ISP services as the tunnel egress interfaces. When the SSL VPN clients with different ISP accesses try to visit headquarters, the optimal path selection feature judges the ISP of the requiring client, arranges the SSL VPN interfaces in the sequence of relevancy to the ISP, and then provides the sequence of SSL VPN egress interface to the client for it to choose; if optimal path detection on the client is enabled, the client selects a preferential link path by sending UDP probe packets.



As shown in the figure above, SSL VPN client accesses to SSL VPN server by the way of DNAT device which translates the client address to SSL VPN server egress interface. The DNAT device accesses Internet using multiple ISP links. You need to add the DNAT device's egress interface to an address entry in the SSL VPN server address pool. If optimal path detection on the SSL VPN server is enabled, the server judges the ISP type of client's access address and assigns DNAT's egress interface addresses to the client according to the priority of address so that the client can select its optimal path; if optimal path detection on the client is enabled, the client sends UDP probe packets to choose an optimal path.

To specify an interface as SSL VPN tunnel egress interface, in the SSL VPN instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of server interface.

Repeat this command to specify more interfaces (up to two) as the tunnel egress interface.

To cancel the specified tunnel interface, in the SSL VPN instance configuration mode, use the following command:

no interface *interface-name*

To configure the optimal path selection, in the SSL VPN instance configuration mode, use the following command:

link-select [**server-detect**] [*A.B.C.D* [**https-port** *port-number*]] [**A.B.C.D** [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]] [*A.B.C.D* [**https-port** *port-number*]]

- **server-detect** – Enables the optimal link detection of the device. When this parameter is not configured, optimal link detection is enabled. By default, the client selects link spontaneously.
- *A.B.C.D* – Specifies the Internet interface IP address of DNAT device. The system allows up to four IP addresses.
- **https-port** *port-number* – Specifies the HTTPS port number of the DNAT Internet interface. The value range is 1 to 65535. The default value is 4433. To avoid collision with WebUI HTTPS port number, you are not recommended to use port 443.

To cancel optimal link selection, in the SSL VPN instance configuration mode, use the command **no link-select**.

SSL VPN optimal link selection also provides multi-link redundancy, which enables the server to switch links when one link disconnects so as to guarantee the connection stability between server and client (traffic flow may be interrupted during switching).

Kicking out an SSL VPN Client

The SSL VPN server can force to disconnect with a client.

To kick out an SSL VPN client, in the configuration mode, use the following command:

exec scvpn *instance-name* {**kickout** *user-name* | **kickout-all-user**}

- *instance-name* – Specifies the name of SSL VPN instance.
- *user-name* – Specifies the name of client to be kicked out of the server.
- **kickout-all-user** – Specifies all online users to be kicked out of the server.

Configuring Change Password URL of the Client

The system supports to redirect to the specified page to modify the password through the configured URL through the client .

To configuring change password URL, in the SSL VPN instance configuration mode, use the following command:

change-password-url*url*

url – Specifies the URL address that needs to be redirected to modify the password. The ranges is 1 to 255 characters.

To cancel the configuration,use the following command:

no change-password-url

Configuring Forgot Password URL of the Client

The system supports tsupports to redirect to the specified page through the configured URL to reset the password.

To configuring forgot password URL, in the SSL VPN instance configuration mode, use the following command:

forgot-password-url*url*

url – Specifies the URL address that needs to be redirected to reset the password. The ranges is 1 to 255 characters.

To cancel the configuration,use the following command:

no forgot-password-url

Exporting and Importing a User-list File

To avoid userinfo setting disoperation, you can export/import the user-list file from/to the SSL VPN server. The system supports the import of user-list files in BOM-UTF-8 .txt format and in BOM-UTF-8 .csv format. When the user-list file is imported, the system will carry out validity test and complexity check of the user password. If the results turn out to be successful, the

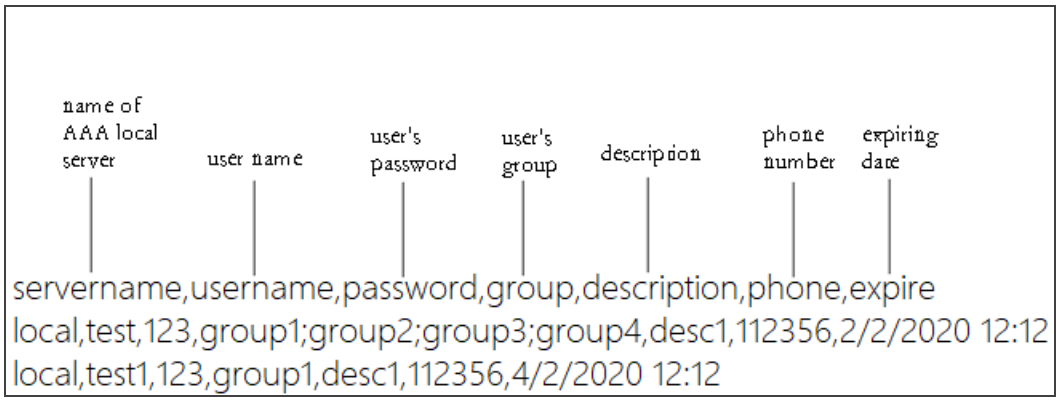
importing is successful; if the results turn out to be unsuccessful, the importing is unsuccessful. The system exports the user-list file in .csv format, of which the content is the real-time information of the user list in the system.

The user-list in .csv file is illustrated in the figure below.

servername	username	password	group	description	phone	expire
local	test	testadfdgfadg	group1;group2;group3;group4	desc1	112356	2/2/2020 12:12
local	test1	testadfdgfadg	group	desc1	112356	2/2/2020 12:12
local	test2		group	desc1	112356	2/2/2020 12:12
local	test3	testadfdgfadg		desc1	112356	2/2/2020 12:12
local	test5	testadfdgfadg	group		112356	2/2/2020 12:12
local	test6	testadfdgfadg	group	desc1		17/1/2020 12:12
local	test7	testadfdgfadg	group	desc1	112356	
local	test8	testadfdgfadg	group	desc1	112356	1/1/2020 12:12

name of local AAA server | user name | user's password | user's group | description | phone number | expiring date

The user-list in text file is illustrated in the figure below.



Notes: Before importing the user-list file, please read carefully the annotations in the above figures and fill in the user information according to the format.

Exporting a User-list File

To export a user-list file, in the execution configuration mode, use the following command:

export aaa user to {**tftp server** *ip-address* | **ftp server** *ip-address* [**user** *user-name*]} *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* – Specifies the username of the FTP server.
- *file-name* – Specifies the file name of the exported user-list file.

Importing a User-list File

To import a user-list file, in the execution configuration mode, use the following command:

import aaa user from {**tftp server** *ip-address* | **ftp server ip-address** [**user** *user-name*]} *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* – Specifies the username of the FTP server.
- *file-name* – Specifies the file name of the imported user-list file.

The principles of importing user-list files are:

- If a user in the imported user-list file already exists in the system, its user information in the imported file will cover the original information in the system.
- If a user in the imported user-list file is new to the system, it and its user information will be added to the system automatically.



Notes:

- When password file is imported, it takes effect immediately.
- The command line will show the number of imported users.
- In the imported user-list file, the "username" field should not contain slash/-comma/double quotation marks/question mark/@; the "group" field should not contain comma/double quotation marks/question mark.

- In the imported user-list file, the date in the "expire" field should be in the format of DD/MM/YYYY HH:SS.
- If the user-list is imported in the format of text file, special notice should be given to the following points:
  - Every parameter in the file should be separated by half-width commas
  - If a parameter does not exist, use a half-width comma to replace it, etc. "123123,,local".
  - The sequence of the parameters in the first row is fixed and case-insensitive, etc. "Servername,userName,pAssWord".
  - The file should not contain blank lines or gibberish lines, or it is not able be imported successfully.
  - If the length of a parameter is less or more than its length range, it is not able be imported successfully.
    The length range of "username": 1-63 characters
    The length range of "password": 1-31 characters
    The length range of "phone": 6-15characters
    The length range of "email": 1-127 characters
    The length range of "description": 0-127 characters

Control the Access by Using the Radius Server

When you use the Radius authentication mode, you can set the access scope for the authenticated users. For the authenticated users, the system obtains the information that regulates the access scope of the users from the Radius server. Based on obtained information, the system will dynamically create policy that is from the source address to the regulated access scope. For the users that

do not pass the authentication, the system refuses to allow them to access the network. When users logged off or were kicked out by administrators, or when the logging time of a user has timeout, the corresponding policy will be deleted automatically.

To view the regulated access scope, use the following command in any mode:

show auth-user username *user-name*

- *user-name* – Specifies the username of the user that you want to view.

Configuring Radius Server

To control the access by using the Radius server, you must define the following attributes in the dictionary file:

Attribute Name	Type	Value
Hillstone-user-policy-dst-ip-begin	ipaddr	The start IP address of the access scope. Only IPv4 address is supported.
Hillstone-user-policy-dst-ip-end	ipaddr	The end IP address of the access scope. Only IPv4 address is supported.

After adding the attributes, specifying the values for the desired users, restarting the Radius server, the system will then set the access scope for the users that are successfully authenticated through the SSL VPN client. If you do not set the access scope for the users, they will not be limited.

Configuring the Allowed Client Types

By default, you are allowed to access the system with five types of SSL VPN clients, which are SSL VPN client for Windows, SSL VPN client for Android, SSL VPN client for iOS, SSL VPN client for macOS, SSL VPN client for Linux, and SSL VPN client for ChineseOS. You can configure to access the system only via the specified types of SSL VPN clients as needed.

To configure client type with which you are allowed to access the system, in the SSL VPN instance configuration mode, use the following command:

allowed-client-type {**Android** | **iOS** | **Linux** | **macOS** | **Windows** | **ChineseOS**}

- **Android** | **iOS** | **Linux** | **macOS** | **Windows** - Specifies the allowed type of SSL VPN client. The type can be SSL VPN client for Windows (**Windows**), SSL VPN client for Android (**Android**), SSL VPN client for iOS (**iOS**), SSL VPN client for macOS (**macOS**), SSL VPN client for Linux (**Linux**), and SSL VPN client for ChineseOS (**ChineseOS**).

To allow more types, execute the above command multiple times.

In the SSL VPN instance configuration mode, use the command **no allowed-client-type** {**Android** | **iOS** | **Linux** | **macOS** | **Windows** | **ChineseOS**} to forbid the specified type of SSL VPN client to access the system.

General Configuration

The following configurations are shared by ZTNA and SSL VPN. The configurations take effect on both ZTNA and SSL VPN.

- Configuring SSL Cipher Suite
- Allowing Password Change by Local Users
- Customizing Client Download Source
- Customizing the Background Picture of Client Download Page
- Configuring Upgrade URL for Windows Type Client
- Customizing the Page Title

Configuring SSL Cipher Suite

To configure the SSL cipher suite, in the global configuration mode, use the following command:

secure-connect ssl-cipher-list *string*

- string - Specifies the SSL cipher suite list. The default is "ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2:!RC4".

To restore to the default SSL cipher suite list, in the global configuration mode, use the following command:

no secure-connect ssl-cipher-list

Allowing Password Change by Local Users

By default, the local user is not allowed to change its password, but you can configure the device to enable password changing right for local users if they pass SSL VPN or ZTNA authentication.

To enable/disable the right for local users to change the login password, in the password control mode, use the following command:

- Enable: **allow-pwd-change**
- Disable: **no allow-pwd-change**



Tip: Secure Connect client of version 1.2.0.1106 and later allows the local users to change password. Therefore, it's advised to use the latest Secure Connect client.

When the server allows the client user to change password, the user can change login password after passing SSL VPN or ZTNA authentication by the following steps:

1. Right-click the client icon in notification area of the task bar on the right-bottom corner and a menu appears.



2. Click **Changing Password** and type current password and new password into the corresponding boxes.



3. Click **OK** to save the changes.

Customizing Client Download Source

End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.

By default, the client download source on the device is the same with that on Hillstone Networks Official Website. In the application scenario where you want end users to download and use specific Secure Connect clients, such as a client of the specified version or a customized client, you can import the client into the system to overwrite the default download source on the device. You can import Windows, macOS and Linux type clients.

To import the client file from a server, in the execution configuration mode, use the following command:

import secure-connect client {**windows** | **linux** | **macos**} **from** { {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies that the client file is imported from an FTP/FTPS/SFTP server. Type the IP address of the FTP/FTPS/SFTP server, virtual router name, username and password (skip if the server can be logged in anonymously).
- **tftp server** *ip-address* - Specifies that the client file is imported from a TFTP server and specifies the TFTP server address.
- **usb0** | **usb1** - Specifies that the client file is imported from the USB disk plugged to USB0 or USB1 port.
- *file-name* – Specifies the client file. The system will check the imported file. It is recommended to import a client file downloaded from Hillstone Networks Official Website and keep the file name unchanged. Otherwise, the import might fail.

You can delete the imported client file. After deletion, the download source will be restored to the default source. In the execution configuration mode, use the following command to delete the imported client file:

exec secure-connect client {**windows** | **linux** | **macos**} **delete**

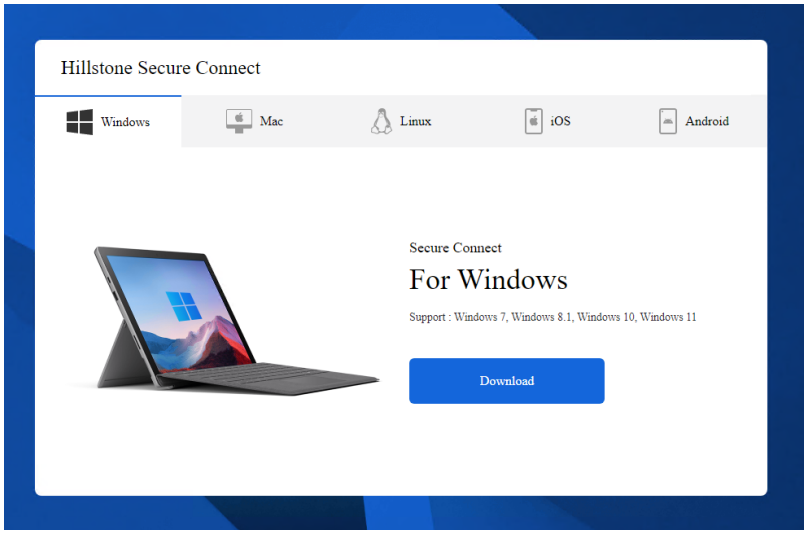
Viewing Secure Connect Client Information

In any mode, use the following command to view the information of Secure Connect clients saved in the system:

show secure-connect client-info [**windows** | **linux** | **macos**]

Customizing the Background Picture of Client Download Page

You can customize the title and background of the download address on the device. The default download page is shown as below:



To import the background picture from a server, in the execution configuration mode, use the following command:

import customize secure-connect download-webpage-background-picture from { {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies that the background picture is imported from an FTP/FTPS/SFTP server. Type the IP address of the FTP/FTPS/SFTP server, virtual router name, username and password (skip if the server can be logged in anonymously).
- **tftp server** *ip-address* - Specifies that background picture is imported from a TFTP server and specifies the TFTP server address.
- **usb0** | **usb1** - Specifies that the background picture is imported from the USB disk plugged to USB0 or USB1 port.
- *file-name* – Specifies the picture name and picture format. The picture must be in PNG format, the resolution is recommended at 1920x *1080x, and the picture size must be less than 2MB.

To restore to the default background picture, in any mode, use the following command:

exec customize secure-connect download-webpage-background-picture default

Configuring Upgrade URL for Windows/Linux/macOS Type Client

The Windows/Linux/macOS type client checks and downloads the new version by using the configured upgrade URL. The system has a default URL that links to the official upgrade server and this URL cannot be deleted. To configure the upgrade URL, use the following command in the global configuration mode:

secure-connect update-url *url*

- *url* – To use the intranet server to check and download the new version, enter the URL of the intranet server. You need to deploy the new version in this intranet server.

To use the default URL that links to the official upgrade server, use the following command in the global configuration mode:

no secure-connect update-url

To view the default URL that links to the official upgrade server, use the following command in any mode:

show secure-connect update-url



Notes:

- When the client version is 1.4.4.1199 or below and the StoneOS version is 5.5R1 or above, it is recommended to uninstall the previous client and login the Web page to re-install it.
- If you want the end users to download the Windows type client carried in the system image, configure this command **secure-connect update-url localhost**.
- After you import a Windows/Linux/macOS type client file using the **import secure-connect client** command, the **secure-connect update-url** configuration will not take effect.

Customizing the Page Title

By default, the title of client download page is "Hilllstone Secure Connect". To customize the title of client download page, in the global configuration mode, use the following command:

secure-connect download-web-page-title *title*

- *title* - Specifies the title of client download page. The length is 1 to 63 characters.

To delete the customized title of client download page, use the following command in the global configuration mode. After the customized title is deleted, no title will be displayed on the client download page.

no secure-connect download-web-page-title

To view the customized title of client download page, use the following command in any mode:

show secure-connect download-web-page-title

Viewing SSL VPN Settings

Use the following commands to view information about SSL VPN.

- Show SSL VPN instance:

  show tunnel scvpn [*scvpn-instance-name]*

- Show online users of the specified SSL VPN instance:

  show scvpn client *scvpn-instance-name* [**user** *user-name*]

- Show online users of all SSL VPN instances:

  show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

- Show user-host binding list:

  show scvpn user-host-binding *scvpn-instance-name* {**host** [*host-id*] | **user** [*user-name*]}

- Show the license capacity of SSL VPN authorized user:

  show secure-connect user capacity

- Show client upgrade URL:

  show secure-connect update-url

- Show client information:

  show secure-connect client-info

- Show the customized client download page title:

  show secure-connect download-web-page-title

Hillstone Secure Connect Client for Windows

The SSL VPN/ZTNA client for Windows is Hillstone Secure Connect. It can run in the following operating systems:

- Windows7/Windows8.1/Windows10/Windows11
- Windows server 2008 R2/Windows server 2012/Windows server 2012 R2/Windows server 2016/Windows server 2019/Windows server 2022

The encrypted data can be transmitted between the client and the device after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC on which the client is running.
- Show the connecting status, statistics, interface information, and route information.
- Show log messages.
- Upgrade the client software.
- Resolve the resource list information received from the server.
- Collect and report endpoint device status information.

System supports IPv4 and IPv6 Secure Connect Windows clients.

This section mainly describes how to download, install, start, uninstall the Secure Connect Windows client, and gives instructions on how to use its GUI and menu. The device side supports the following authentication methods:

- Username/Password
- Username/Password + Digital Certificate (including USB Key certificate and file certificate)
- Digital Certificate (including USB Key certificate and file certificate) only

System supports IPv4 and IPv6 Secure Connect Windows clients.

Downloading and Installing the Client

Take either of the following methods to download and install the Secure Connect Windows client:

- Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.

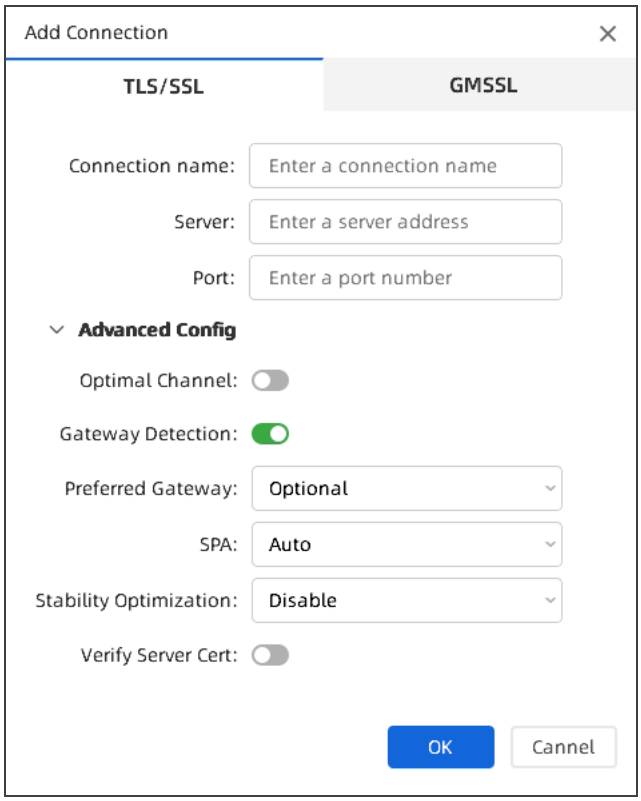
A virtual network adapter will be installed on your PC together with the Secure Connect Windows client. It is used to transmit encrypted data between the device and the client.

Starting Up and Connecting

After the Secure Connect Windows client is installed successfully, take the following steps to start and log in the client:

1. Double-click the shortcut of Hillstone Secure Connect on your desktop, or from the Start menu, choose **All Programs > Hillstone Secure Connect > Hillstone Secure Connect**. The client main page is displayed.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
SMSSL	Select this tab to use the SMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Auth type	Select the authentication type. "User name/Password", "User name/Password + Digital certificate" and "Only

Option	Description
	Digital certificate" are supported. For digital certificate authentication, software certificates and USB-Key certificates are supported.
User name	Enter the name of the login user. When Auth type is specified as "User name/Password" or "User name/Password + Digital certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is enabled, you do not need to enter the user's password at the next-time connection.
Digital certificate	When the authentication type is "User name/Password + Digital certificate" or "Only Digital certificate", click this option to enter the dialog box for selecting a certificate. The selected certificate will be sent to the device for authentication.
TLS certificate	Options in the "TLS certificate" dialog box are described as follows: • Use system default certificates: Click this radio button to allow the device to use the Hillstone UKey certificate as the system default certificate. This is the default setting.

Option	Description
	• Use USB-Key certificates: Click this radio button and select a USB-Key certificate from the current certificate list. The USB Key should be inserted into the USB interface of the PC in advance. You can use the USB Key deployment tool named SelectUSBKey to set the third-party certificate as the default certificate. For more information, refer to Third-Party USB Key. • Use software certificates: Click this radio button and select a software certificate from the current certificate list. The software certificate should be imported into the PC in advance. • Current certificate list: Display the existing certificate in the system. Click **Refresh** icon to update the list.
SMSSL certificate	Options in the "SMSSL certificate" dialog box are described as follows: • Device: Select the current USB Token device name in the drop-down list. The USB Token device should be inserted into the USB interface of the PC in advance. • Application: The application is a structure that contains a container, a device authentication key, and a file. Select the specified application name in the

Option	Description
	drop-down list. • Container: The container is the unique storage space in the USB Token device to save the key. It is used to store the encryption key pair, the encryption certificate corresponding to the encryption key pair, the signature key pair, and the signature certificate corresponding to the signature key pair. Select the name of the specified container in the drop-down list. • Signature certificate: Display the name of the SM2 signature certificate in the specified container. • Encryption certificate: Display the name of the SM2 encryption certificate in the specified container.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/Password + Digital certificate" or "Only Digital certificate".
Remember PIN	After this option is enabled, you do not need to enter the PIN at the next-time connection.
Optimal channel	Set whether to enable optimal path detection function. For more information about optimal path detection, see Selecting an Optimal Path. It is disabled by default.
Gateway detection	Set whether to enable the gateway detection function,

Option	Description
	which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet

Option	Description
	authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. This function applies in the SSL VPN access scenario. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.



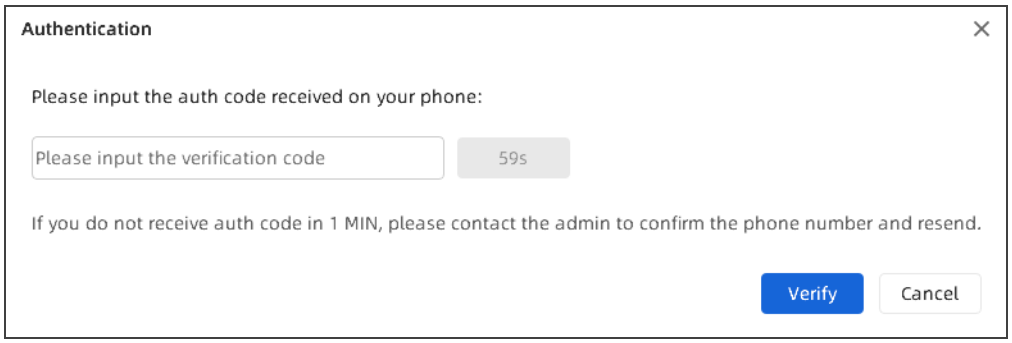
Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical

password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.

5. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog (as shown below) and click **Verify**. If you have not received the authentication code within one minute, you can re-apply by clicking **Resend**.



6. If token authentication is enabled on the device side, the token Authentication dialog will appear. You need to pass the token authentication.

   - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.

- You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

7. If Email authentication is enabled on the device side, the Email Authentication dialog will appear. You need to pass the Email authentication.

    - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.

    - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

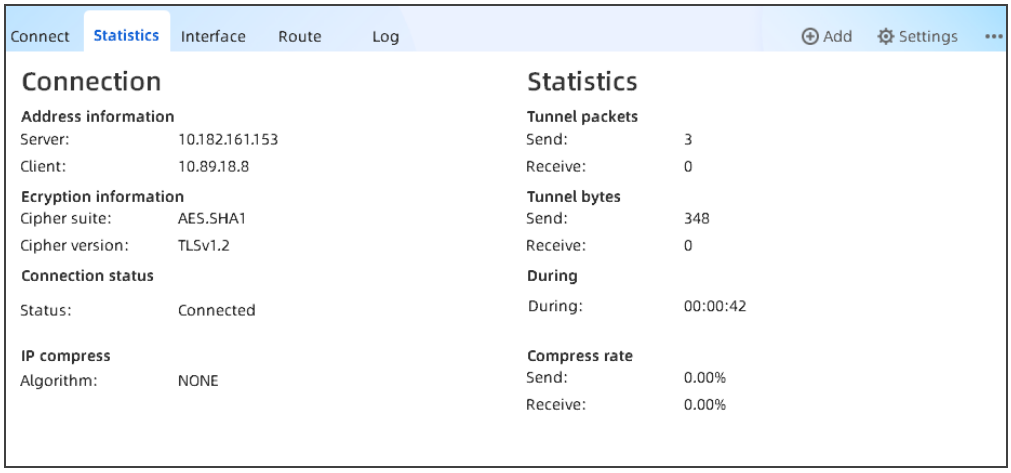
Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the icon () will be displayed in the notification area. And the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.



Address information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packets	
Send	The number of sent packets through the encryption tunnel.
Receive	The number of received packets through the encryption tunnel.
Tunnel Bytes	
Send	Bytes sent through the SSL VPN/ZTNA. tunnel.

Address information: Shows the IP addresses	
Receive	Bytes received through the SSL VPN/ZTNA. tunnel.
During	
During	Time period during which the client is online.
Compress rate	
Send	Length ratio of sent data after compression.
Receive	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.



Option	Description
Interface name	The name of the interface used to send encrypted data.
Interface type	The type of the interface used to send encrypted data.
Interface status	The status of the interface used to send encrypted data.
IP address type	The IP address type of the interface used to send encrypted data.
IP address	The IP address (allocated by the device) of the interface used to send

Option	Description
	encrypted data.
Subnet mask	The subnet mask of the interface used to send encrypted data.
Default Gateway	The default gateway address of the interface used to send encrypted data.
DNS Server address	The address of the DNS server used by the client.
WINS address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Third-party USB Key

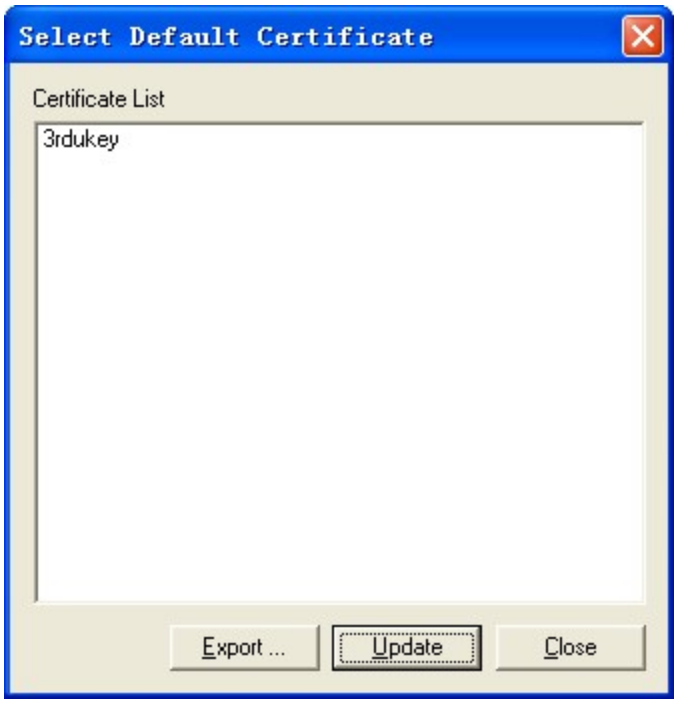
Hillstone UKey certificate is the default certificate for the USB Key authentication. When authenticating with Hillstone UKey certificate, the client will select the Hillstone UKey certificate automatically and send it to the server, and the server will perform the authentication with the default certificate. This authentication process is transparent to the authenticated clients, i.e., the client need not to choose the certificate. If the third-party USB Key is used, you can set the third-party

certificate as the default certificate to simplify the authentication process by using the tool named SelectUSBKey.

To set the third-party certificate to the default certificate, first you have to export the CSP Name of the USB Key in form of a registry file, and then add the exported file content to the registry of the client PC.

To export the CSP Name of the USB Key, take the following steps:

1. Install the driver of the third-party USB Key.
2. Insert the third-party USB Key.
3. Double click SelectUSBKey.exe, and the Select Default Certificate dialog is shown as below:



Export: Exports the CSP Name of the USB Key in form of a registry file.

Update: Refreshes the certificate list.

Close: Closes the dialog.

4. Select the certificate you want from the certificate list, and then click **Export**.

After exporting the CSP Name of the USB Key, double click the exported file, and then add the content to the registry of the client PC. When authenticating with the third-party certificate, the client will automatically select the third-party USB Key certificate and send it to the server.

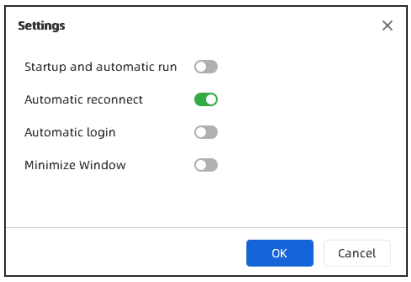
Client Menu

Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application resources, the portal page displays a message indicating that no Web resources are available to the user.
- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.



- **Startup and automatic run**: Enable this option to automatically run the client when the PC is starting.
- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the specified user to login automatically when the client is starting. Select the auto login user from the drop-down list.
- **Minimize window**: Enable this option to allow the client window to be minized.

Uninstalling the Client

To uninstall the client on your PC, from the Start menu, click **All Programs > Hillstone Secure Connect > Uninstall**.

Hillstone Secure Connect Client for Linux

The SSL VPN/ZTNA client for Linux is Hillstone Secure Connect. It can run in the following operation systems:

- CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5
- Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04
- Ubuntu Kylin 18.04/20.04

The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC in which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint status information.

Take CentOS 7.6 as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other three Linux systems can refer to 64-bit Ubuntu Kylin16.04 desktop.

Downloading and Installing the Client

To download and install the Secure Connect Linux client, take the following steps:

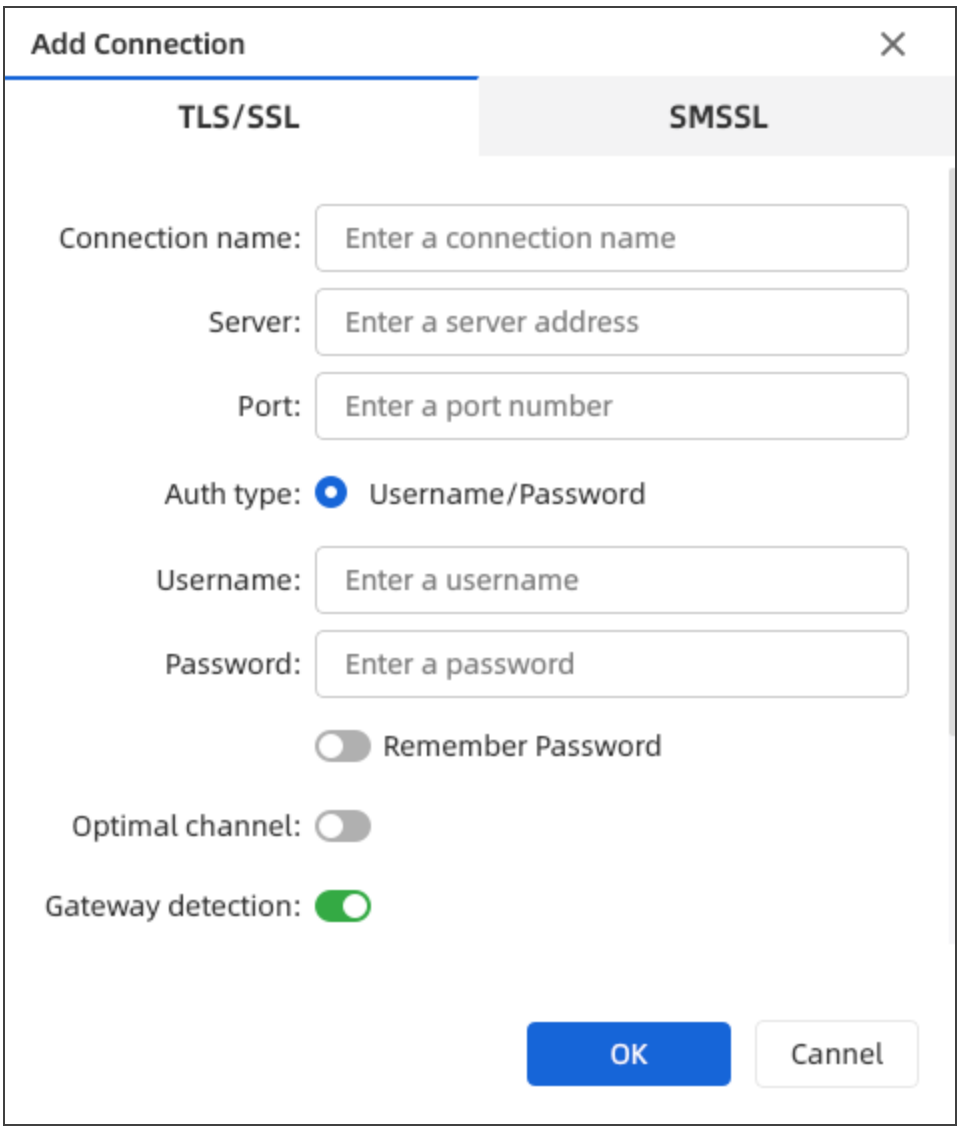
1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, right-click the client icon and select **Properties** to go to the properties page. In the properties page, click **Permissions** tab and check **Allow executing files as program**, then close it.
3. Double-click the client icon and follow the setup wizard to complete the installation.

Starting Up and Connecting

After the Secure Connect Linux client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on your desktop. The client main page is displayed.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
SMSSL	Select this tab to use the SMSSL protocol.

Option	Description
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is enabled, you do not need to enter the user's password at the next-time connection.
Optimal channel	Set whether to enable optimal path detection function. For more information about optimal path detection, see Selecting an Optimal Path. It is disabled by default.
Gateway detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all

Option	Description
	gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified.

Option	Description
	• Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. This function applies in the SSL VPN access scenario. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.



Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.

5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

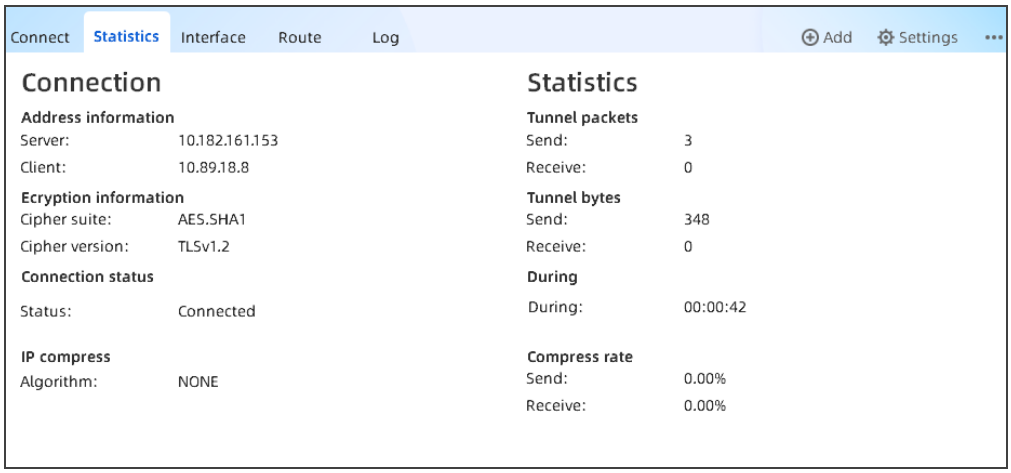
After the client connects to the SSL VPN/ZTNA server, the encrypted data can be transmitted between the client and the server now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.



Address information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.

Address information: Shows the IP addresses	
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packets	
Send	The number of sent packets through the encryption tunnel.
Receive	The number of received packets through the encryption tunnel.
Tunnel Bytes	
Send	Bytes sent through the SSL VPN/ZTNA. tunnel.
Receive	Bytes received through the SSL VPN/ZTNA. tunnel.
During	
During	Time period during which the client is online.
Compress rate	
Send	Length ratio of sent data after compression.
Receive	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.



Option	Description
Interface name	The name of the interface used to send encrypted data.
Interface type	The type of the interface used to send encrypted data.
Interface status	The status of the interface used to send encrypted data.
IP address type	The IP address type of the interface used to send encrypted data.
IP address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet mask	The subnet mask of the interface used to send encrypted data.
Default Gateway	The default gateway address of the interface used to send encrypted data.
DNS Server address	The address of the DNS server used by the client.
WINS address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Client Menu

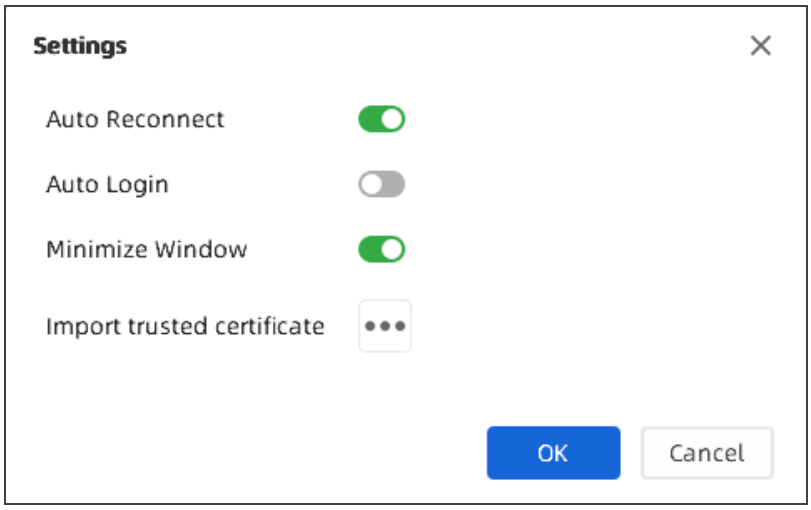
Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application resources, the portal page displays a message indicating that no Web resources are available to the user.

- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.



- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the specified user to login automatically when the client is starting. Select the auto login user from the drop-down list.
- **Minimize window**: Enable this option to allow the client window to be minimized.

Hillstone Secure Connect Client for Android

The SSL VPN/ZTNA client for Android is Hillstone Secure Connect. It can run in Android Android 8.x/Android 9.x/Android 10.x/Android 11.x/Android 12.x/Android 13.x/HongmengOS 2.0. The functions of Secure Connect Android client contain the following items:

- Obtain the interface information of the Android OS.
- Display the connection status with the device, traffic statistics, interface information, and routing information.
- Display the log information of the application.
- Collect and report endpoint status information.

Downloading and Installing the Client

To download and install the Secure Connect Android client, take the following steps:

1. Visit https://www.hillstonenet.com/more/services/product-downloads/ to download the installation file of the client, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. Use the Android device to scan the QR code of the Secure Connect Android client.
3. Open the URL and download the Hillstone-Secure-Connect-Versione_Number.apk file.
4. After downloading successfully, find this file in the Android device.
5. Click it and the installation starts.
6. Read the permission requirement.
7. Click **Install**.

After installing the client successfully, the icon of the Secure Connect Android client appears in the desktop as shown below.

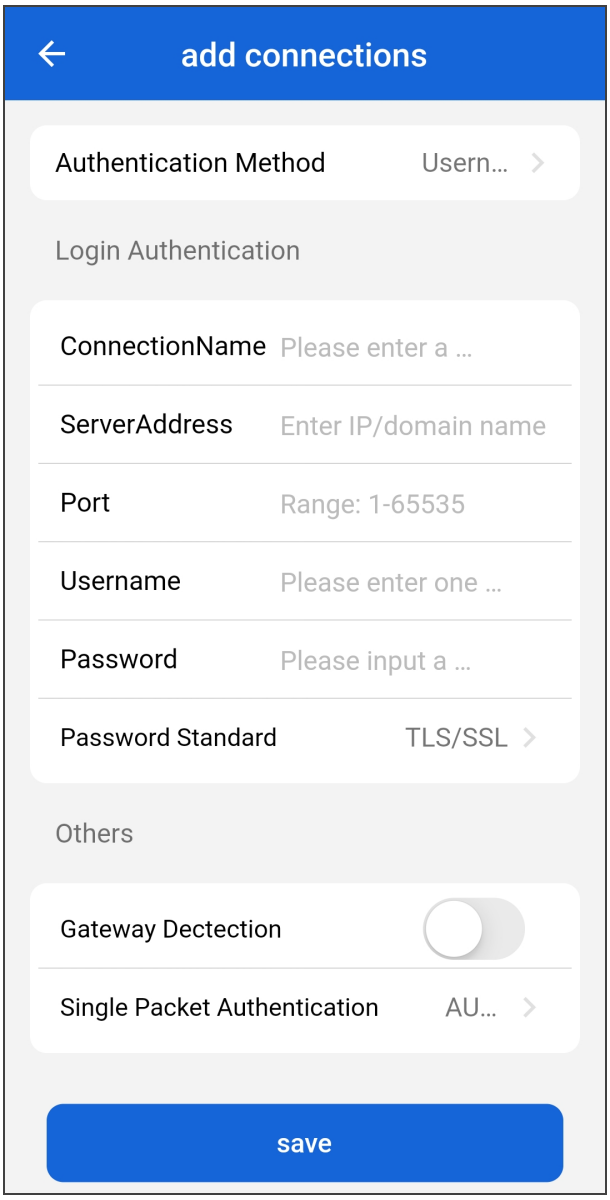


Starting Up and Connecting

After the Secure Connect Android client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.

2. In the "Home" tab, click "+" and enter the "Add Connection" page.



Enter the connection information.

Option	Description
Authentication Method	Select the authentication method. "User name/-password", "User name/password + Digital Certificate" and "Digital Certificate" are supported.
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user. When authentication method is specified as "User name/password" or "User name/password + Digital Certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/password + Digital certificate" or "Digital certificate".
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Select Cer-	Select the digital certificate that has been imported into the Android device in advance.

Option	Description
tificate	
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also

Option	Description
	need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number.



Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous pass-

word. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS authentication, token authentication or email authentication is enabled, you need to enter the corresponding authentication code to complete the authentication.

After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit a login entry, click the icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.

Option	Description
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface State	The status of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
Network Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gateway	The default gateway address of the interface used to send encrypted data.
DNS Address	The address of the DNS server used by the client.

Hillstone Secure Connect Client for iOS

The SSL VPN/ZTNA client for iOS is Hillstone Secure Client. It supports iOS 12.x/iOS 13.x/iOS 14.x/iOS 15.x/iOS 16.x versions. The Secure Connect iOS client mainly has the following functions:

- Simplify the tunnel creation process between the iOS device and the Hillstone device
- Display the connection status between the iOS device and the Hillstone device
- Display the log information
- Collect and report endpoint device status information.

Downloading and Installing the Client

You can take either of the following methods to download and install the Secure Connect iOS client:

- Search Hillstone Secure Client(beta) in the App Store.
- Visit https://www.hillstonenet.com/more/services/product-downloads/, locate the QR code for iOS client, use the iOS device to scan the code and then jump to App Store for downloading and installation.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance

Starting Up and Connecting

After the client is installed successfully, for the first time login, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.

2. In the "Home" tab, click "+" and enter the "Add Connection" page.

   Enter the connection information.

Option	Description
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a

Option	Description
	connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should

Option	Description
	be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number.



Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS, token or email authentication is enabled, type the corresponding code to complete the authentication.
6. After login, the iOS device will start the VPN configuration deployment automatically. In the **Would Like to Add VPN Configurations** page, click **Allow**.

7. Enter your passcode. The passcode is the one for unlocking your iOS screen. With the correct passcode entered, the iOS device starts to install the profile.
8. After the installation is complete, start **Settings** of the iOS device and navigate to **VPN**.
9. Select the configured connection name and click the **Connect** button.
10. After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Notes: For subsequent logins, you do not need to perform the VPN configuration deployment steps. You can log in the client and start the connection directly.

Editing and Deleting Login Entry

To edit a login entry, click the icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.

Option	Description
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface State	The status of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
Network Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gateway	The default gateway address of the interface used to send encrypted data.
DNS Address	The address of the DNS server used by the client.

Hillstone Secure Connect Client for macOS

The SSL VPN/ZTNA client for macOS is Hillstone Secure Connect. It can run in macOS 10.13/macOS 10.14/macOS 10.15/macOS 11.0/macOS 12.0/macOS 13.0 versions. The

encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Establish the encrypted connection with the SSL VPN/ZTNA server.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint device status information.

Downloading and Installing the Client

To download and install the Secure Connect macOS client, take the following steps:

1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, double-click it. In the pop-up, drag the Secure Connect macOS client to the **Applications** folder to perform the installation.

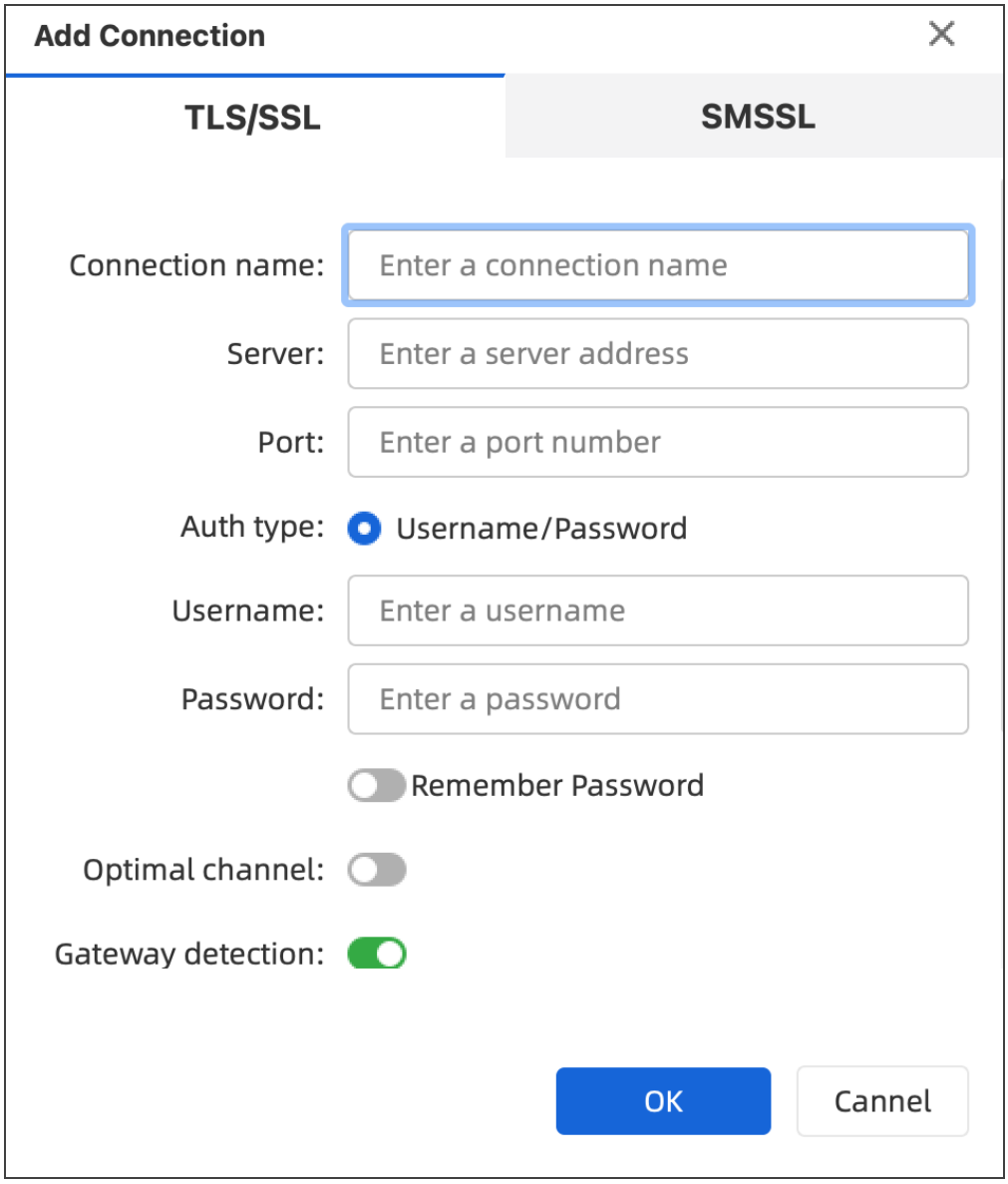


Notes: To open the installation file, you must have the administrator permission and select **Anywhere in System Preferences > Security & Privacy > General > Allow apps downloaded from**.

Starting Up and Connecting

After the Secure Connect macOS client is installed successfully, take the following steps to start and log in the client:

1. Select **Launchpad > Hillstone Secure Connect**. The client starts.
2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
SMSSL	Select this tab to use the SMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Auth type	The authentication type is username/password.
User name	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Optimal channel	Set whether to enable optimal path detection function. It is disabled by default.
Gateway detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gate-

Option	Description
	way and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients.

Option	Description
	• Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. This function applies in the SSL VPN access scenario. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.



Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous step to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.
5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

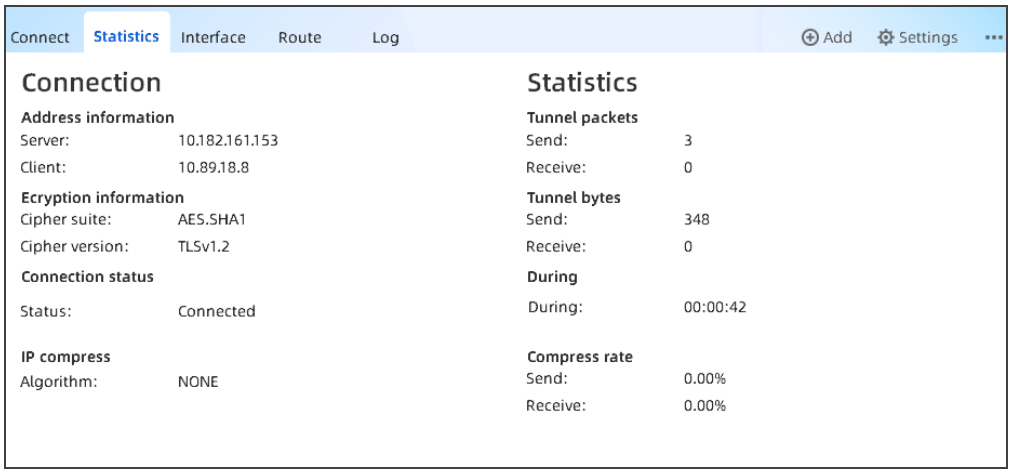
Finishing the above steps, the client will connect to the server automatically.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.



Address information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL

Address information: Shows the IP addresses	
	VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packets	
Send	The number of sent packets through the encryption tunnel.
Receive	The number of received packets through the encryption tunnel.
Tunnel Bytes	
Send	Bytes sent through the SSL VPN/ZTNA. tunnel.
Receive	Bytes received through the SSL VPN/ZTNA. tunnel.
During	
During	Time period during which the client is online.
Compress rate	
Send	Length ratio of sent data after compression.
Receive	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.



Option	Description
Interface name	The name of the interface used to send encrypted data.
Interface type	The type of the interface used to send encrypted data.
Interface status	The status of the interface used to send encrypted data.
IP address type	The IP address type of the interface used to send encrypted data.
IP address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet mask	The subnet mask of the interface used to send encrypted data.
Default Gateway	The default gateway address of the interface used to send encrypted data.
DNS Server address	The address of the DNS server used by the client.
WINS address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Client Menu

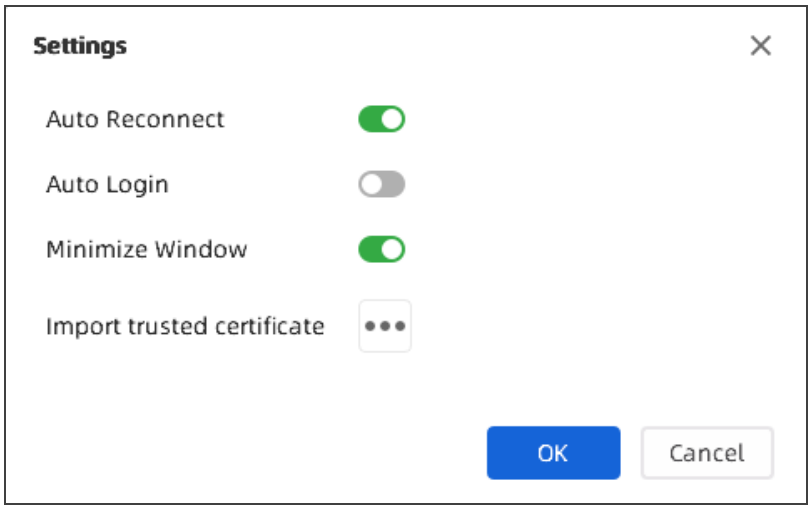
Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application resources, the portal page displays a message indicating that no Web resources are available to the user.

- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.



- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the specified user to login automatically when the client is starting. Select the auto login user from the drop-down list.
- **Minimize window**: Enable this option to allow the client window to be minimized.

Uninstalling the Client

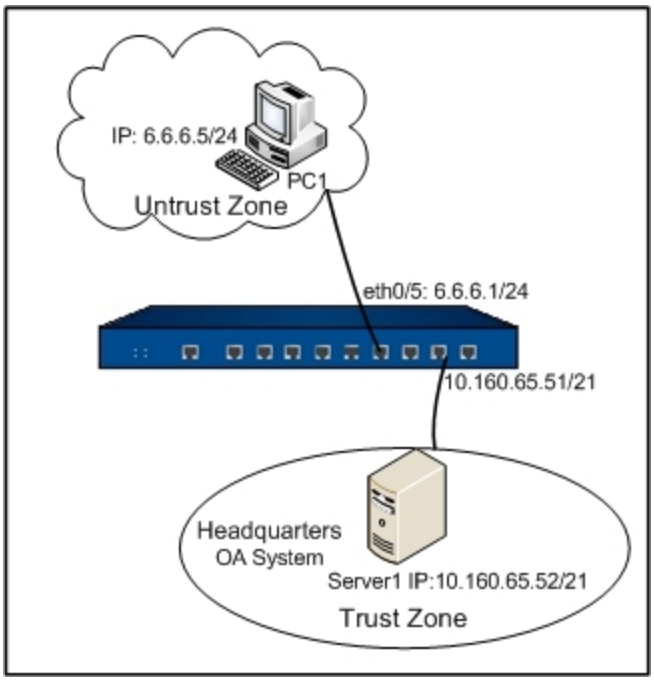
To uninstall the client, right-click the client icon and select Move to Trash from the drop-down-list.

Example of Configuring URL Redirect

This section describes a URL redirect configuration example.

An enterprise uses Hillstone device as the SSL VPN server in its OA system. The goal is to log into both the SSL VPN and OA system at one time.

This requirement can be met by the URL redirect function. The topology is shown as below:



Configuration Steps

Step 1: Create a local user

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user test
hostname(config-user)# password test
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure an address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address 20.1.1.1 20.1.1.255 netmask 255.255.255.0
```

```
hostname(config-address-pool)# dns 20.1.1.1
hostname(config-address-pool)# wins 20.1.1.2
hostname(config-address-pool)# exit
hostname(config)#
```

Step 3: Configure URL redirect in an SSL VPN instance. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# access-address-pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# redirect-url http://192.10.5.201/oa/login.-
do?username=$USER&password=$PWD title-en OA title-zh
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# split-tunnel-route 192.10.5.0/24
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 4: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool must be in the same network segment)

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure a policy from VPN zone to trust zone

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 6: In the web browser of PC1, visit **https://6.6.6.1:4433**, and in the login page, type test and test into the Username and Password boxes respectively. After the authentication, download and install Secure Connect.

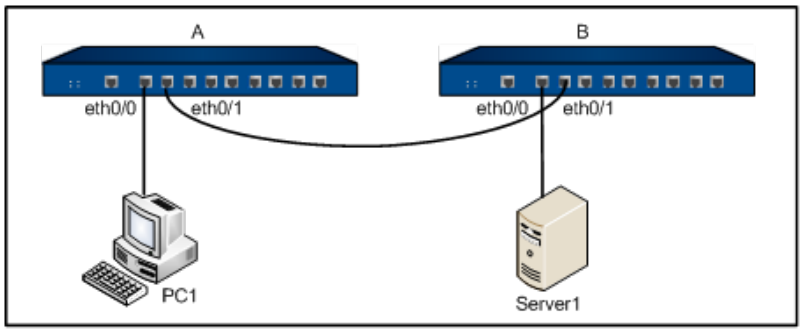
Step 7: After logging in with Secure Connect, the page will be redirected to the OA system authentication page

Examples of Configuring SSL VPN

This section describes several SSL VPN examples with the username/password authentication method.

Requirement

Server1 (10.160.65.52/21) in the Intranet is protected by a Hillstone device. PC1 (6.6.6.5/24) in Internet wants to visit the resources on Server1 (10.160.65.52/21).



- **Requirement 1**: The goal is to control the access by encrypting the data by SSL VPN with the username/password authentication method.
- **Requirement 2**: The goal is to control the access by encrypting the data by SSL VPN with the USB Key authentication method. As long as the UKey of the client supports standard Windows SDK (Certificate Store Functions) and the stored certificate is valid, the client can log in. Hillstone UKey is used as the example.

Example 1

Step 1: Create a local user

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#exit
```

Step 2: Configure an address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address 20.1.1.1 20.1.1.100 netmask 255.255.255.0
hostname(config-address-pool)# dns 20.1.1.1
hostname(config-address-pool)# wins 20.1.1.2
```

```
hostname(config-address-pool)# exit
hostname(config)#
```

Step 3: Configure an SSL VPN instance. By default, the system adds the split-tunnel-route 0.0.0.0/0 route entry. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# access-address-pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/5
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.160.64.0/21
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 4: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# zone VPN
hostname(config-zone-VPN)#
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address 20.1.1.101/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure a policy from VPN zone to trust zone

```
hostname(config)# policy-global
hostname(config-policy)# rule
```

```
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 6: Type **https://6.6.6.1:4433** in the Web browser to visit the login page. Enter username user1 and password 123456. When you log in successfully, download the SSL VPN client Hillstone Secure Connect

Step 7: After logging in, PC1 can access resources in the trust zone through SSL VPN

Example 2

On the basis of Example 1, add USB Key authentication feature. This feature requires that user's UKey should support standard Windows SDK (Certificate Store Functions) with a legal certificate in it. This example uses the Hillstone UKey.

Preparations

Before using the USB Key, make the following preparations:

- Prepare the certificate and the corresponding CA certificate;
- Prepare the Hillstone UKey and the CD provided by Hillstone;
- Import the certificate to the UKey using Hillstone UKey manager.

Configuration Steps

Step 1: Configure an SSL VPN server

```
#Create a PKI trust domain named stone and specify that the certificate is obtained by the method of terminal
hostname(config)# pki trust-domain stone
hostname(config-trust-domain)# enrollment terminal
hostname(config-trust-domain)# exit
hostname(config)#
#Enable USB Key certificate authentication of SSL VPN instance SSL1 and specify a CA trust domain
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# client-cert-auth
hostname(config-tunnel-scvpn)# client-auth-trust-domain stone
hostname(config-tunnel-scvpn)# exit
hostname(config)#
#Import the CA certificate file to the CA trust domain
hostname(config)# exit
hostname# import pki stone cacert from tftp server 192.168.1.2 certnew.cer
```

Step 2: Operations on the clients

1. Install Hillstone UKey driver on the client PC.
2. Insert the UKey.
3. In the SSL VPN client Login dialog, fill each option as below and click Login:
    - Server: 6.6.6.1
    - Port: 4433
    - Username: user1

- Password: hillstone
- PIN: 1111 (the default value)

Example of Configuring Host Check

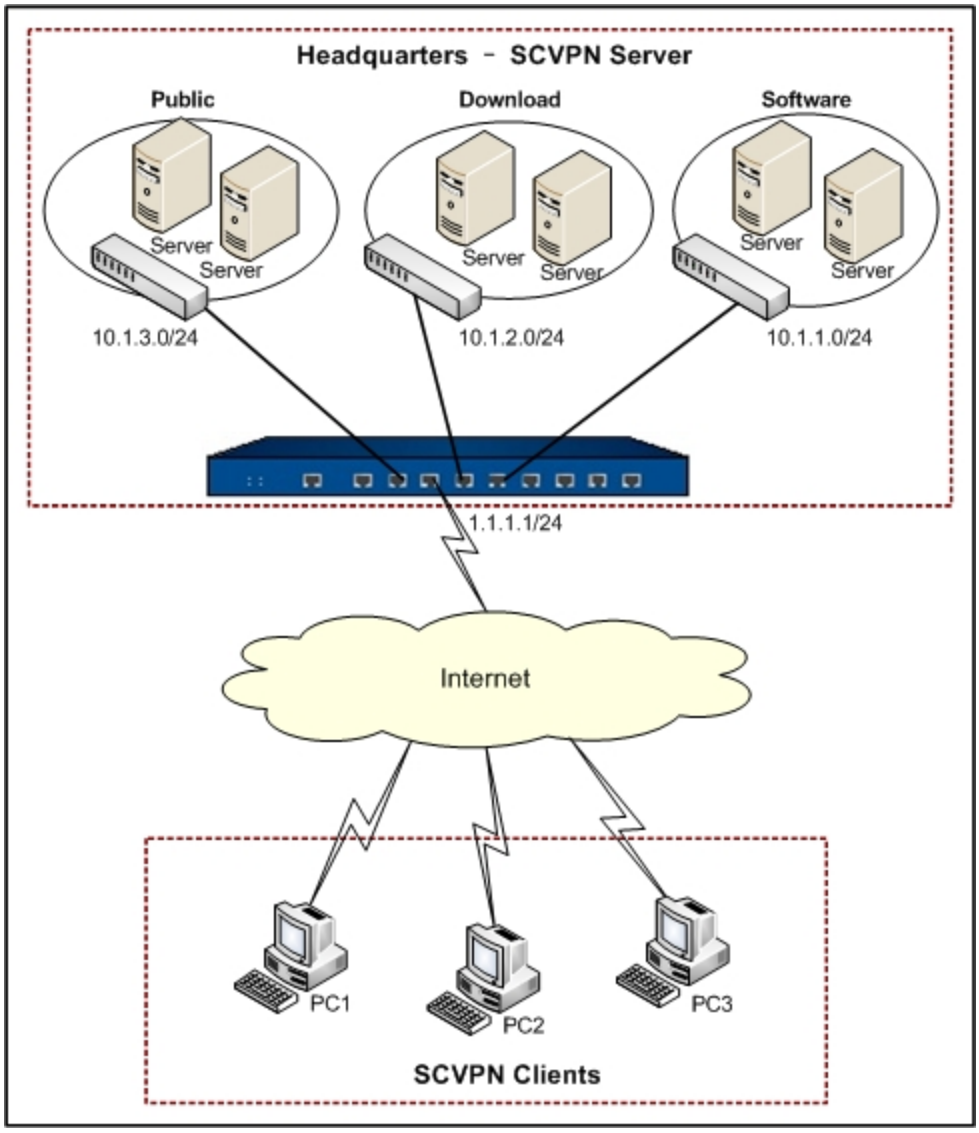
This section describes an SSL VPN host check configuration example.

Requirements

The Hillstone device works as the SSL VPN server for an enterprise. The goal is to meet the following requirements:

- The client can access headquarters resources with SSL VPN.
- Resources in the software network segment (10.1.1.0/24) can be accessed by role sw only; resources in the downloading network segment (10.1.2.0/24) can be accessed by role dl; and resources in public network segment (10.1.3.0/24) can be accessed by all users.
- Perform host security check to the clients and control the resources access based on the check results.

The topology is shown as below:



Configuration Steps

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user pc1
hostname(config-user)# password xxxfcvg236
hostname(config-user)# exit
hostname(config-aaa-server)# user pc2
```

```
hostname(config-user)# password xcabuv112
hostname(config-user)# exit
hostname(config-aaa-server)# user pc3
hostname(config-user)# password xacfomg763
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure a role mapping rule

```
hostname(config)# role sw
hostname(config)# role dl
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user pc1 role sw
hostname(config-role-mapping)# match user pc1 role dl
hostname(config-role-mapping)# match user pc2 role dl
hostname(config-role-mapping)# exit
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# role-mapping-rule rule1
hostname(config)#
```

Step 3: Configure an interface on the SSL VPN server

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure the host check profiles

```
hostname(config)# scvpn host-check-profile dl-security-check
```

```
hostname(config-profile_scvpn)# exit
hostname(config)# scvpn host-check-profile sw-security-check
hostname(config-profile_scvpn)# exit
hostname(config)#
```

To configure a host check profile on WebUI interface, take the following steps:

1. On the Navigation pane, click **Configure > Network > SSL VPN** to visit the SSL VPN page.
2. On the **Task** tab in the right auxiliary pane, click **Host Check** to visit the Host Check page.
3. Click **New**. In the Host Checking Configuration dialog, configure the options as below:

   Basic

   - **Name**: dl-security-check
   - **OS version**: At least, Win2003, None
   - **Patch 1**: KB958215
   - **Lowest IP version**: IE6.0
   - **Lowest IP security level**: High

   Advanced

   - **Security center**: Must
   - **Anti-Virus software**: Installed, Monitor, Virus signature DB update
   - **Anti-Spyware software**: Installed, Monitor, Signature DB update
   - **Firewall**: Installed, Monitor
4. Click **OK** to save the settings and return to the SSL VPN page.

5. Repeat Step 3-4 to create the profile named sw-security-check. The profile contents are:

   Basic

   - **Name**: sw-security-check
   - **OS version**: Must match, WinXP, SP3
   - **Patch 1**: KB921883
   - **Lowest IP version**: IE7.0
   - **Lowest IP security level**: High

   Advanced

   - **Security center**: Must
   - **Auto update**: Must
   - **Anti-Virus software**: Installed, Monitor, Virus signature DB update
   - **Anti-Spyware software:** Installed, Monitor, Signature DB update
   - **Firewall**: Installed, Monitor
   - **File path name**: File 1: Exist, C:\Program Files\McAfee\VirusScan\Enterprise.exe

6. Click **OK** to save settings.

Step 5: Configure an address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address11.1.1.10 11.1.1.100 netmask 255.255.255.0
hostname(config-address-pool)# dns 10.1.1.1
hostname(config-address-pool)# wins wins
hostname(config-address-pool)# exit
hostname(config)#
```

Step 6: Configure an SSL VPN instance. To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# access-address-pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 metric 10
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.2.0/24 metric 5
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.3.0/24 metric 3
hostname(config-tunnel-scvpn)# host-check role sw profile sw-security-check guest-role dl
hostname(config-tunnel-scvpn)# host-check profile dl-security-check periodic-check 50
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 7: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# ip address11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 8: Configure a policy rule

```
hostname(config)# address sw
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# address dl
hostname(config-addr)# ip 10.1.2.0/24
hostname(config-addr)# exit
hostname(config)# address public
hostname(config-addr)# ip 10.1.3.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr sw
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role sw
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dl
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role dl
```

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr public
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

After finishing the above configurations, when the client connects the server, the server will check the host based on the configured host check profile, and assign the corresponding access right according to the check result. The following list shows the relationship between the host check rule and the access right.

User	Host check rule	Check result and access right	
		Successful	Failed
PC1	Role: sw Profile: sw-security-check Guest role: dl Periodic: 30 minutes CLI: **host-check role sw profile sw-security-check guest-role dl**	Permit to access resources in the software network segment, and the host check will performed every 30 minutes automatically.	Permit to access resources in the download network segment, and the host check will be performed every 30 minutes automatically.
PC2	Role: Null (the access right of the default role dl will be	Permit to access resources in the soft-	Disconnect

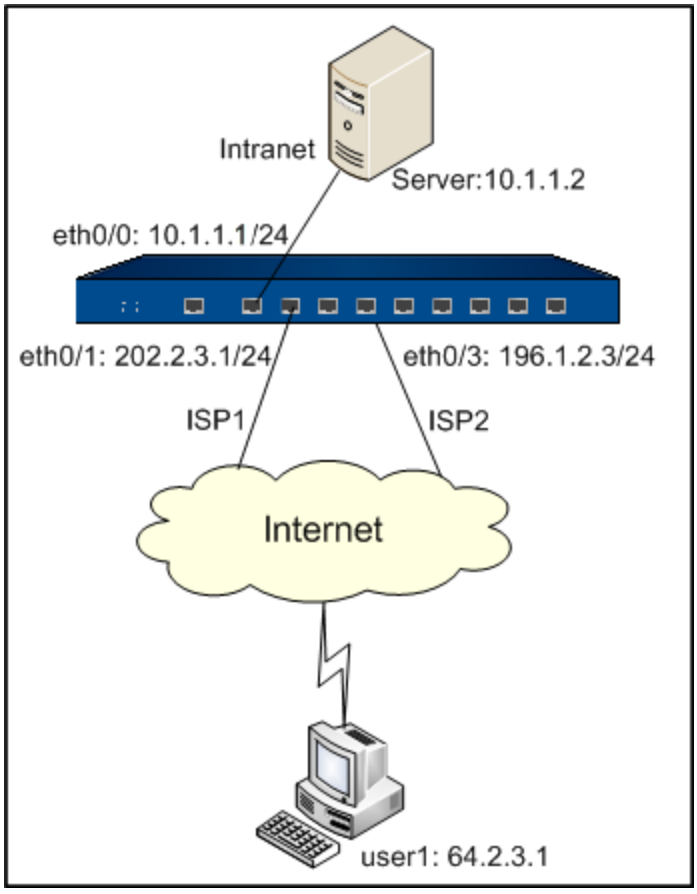
User	Host check rule	Check result and access right	
		Successful	Failed
	assigned) Profile: dl-security-check Guest role: Null Periodic: 50 minutes CLI: **host-check profile dl-security-check periodic-check 50**	ware network segment, and the host check will performed every 30 minutes automatically.	
PC3	Role: Null Profile: dl-security-check Guest role: Null Periodic: 50 minutes CLI: **host-check profile dl-security-check periodic-check 50**	Permit to access resources in the public network segment, and the host check will be performed every 50 minutes automatically.	Disconnect

Example of Configuring Optimal Path

This section provides an example of configuring SSL VPN optimal path.

Requirement 1

A company uses a Hillstone device as the SSL VPN server which has two accesses to the Internet, ISP1 (ethernet0/1, IP: 202.2.3.1/24) and ISP2 (ethernet0/3, IP: 196.1.2.3/24). The goal is that the PC (IP: 64.2.3.1) can access the headquarters server (IP: 10.1.1.2) using optimal path detection feature.



You have two configuration methods to meet this requirement, which are:

- Using the server to choose an optimal path
- Using the client to choose an optimal path

Using SSL VPN Server to Choose an Optimal Path

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the server interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.0/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.2.3.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 196.1.2.3/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Configure an address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address 11.1.1.10 11.1.1.100 netmask 255.255.255.0
hostname(config-address-pool)# dns 10.1.1.1
hostname(config-address-pool)# wins 10.1.1.2
hostname(config-address-pool)# exit
hostname(config)#
```

Step 4: Configure an SSL VPN instance (with optimal path detection). To limit the access range of the remote user, use the no split-tunnel-route 0.0.0.0/0 command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# access-address-pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
```

```
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# interface ethernet0/3
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route 10.1.1.0/24 metric 10
hostname(config-tunnel-scvpn)# link-select server-detect
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 5: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6: Configure a policy rule

```
hostname(config)# address dst
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
```

```
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configure an ISP

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24
hostname(config-isp)# subnet 64.2.3.0/24
hostname(config-isp)# exit
hostname(config)#
```

When the client PC initiates a connection request to SSL VPN server using ISP2, the server identifies that the IP addresses of SSL VPN egress interface ethernet0/1 and client PC both belong to ISP1, so it assigns an IP of egress interface with higher priority to the client and the PC can access the headquarters server using ISP1.

Using SSL VPN Client to Choose an Optimal Path

Configuration steps of using client to choose optimal path have slight differences with steps of using the server in choosing optimal path, and the different steps are:

Step 4: Configure an SSL VPN instance (with optimal path detection feature)

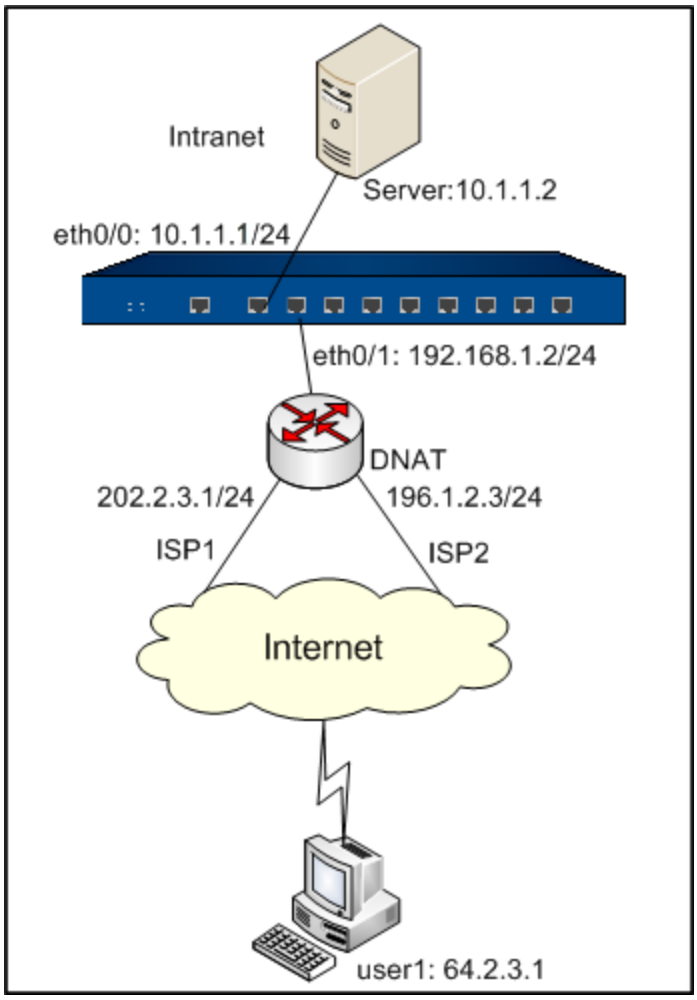
```
hostname(config)# tunnel scvpn ssl1
……
hostname(config-tunnel-scvpn)# link-select
.....
```

Step 7: Skip this step

When the PC initiates connection requests to the headquarters using ISP2 link, the server will assign the IP addresses of both ethernet0/1 and ethernet 0/3 to the client and the client judges the optimal path by sending UDP probe packets.

Requirement 2

A company uses a Hillstone device as the SSL VPN server in its headquarters and uses a DNAT device with two Internet accesses (ISP1: 202.2.3.1/24 and ISP2: 196.1.2.3/24). The goal for the client PC (64.2.3.1) is to access to the headquarters server (IP: 10.1.1.2) using optimal path detection feature.



You have two configuration methods to meet this requirement, which are:

- Using SSL VPN server to choose an optimal path
- Using SSL VPN client to choose an optimal path

Using SSL VPN Server to Choose an Optimal Path

Step 1: Create a local user

```
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# password drgrhrgerg231
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the server interface

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 10.1.1.0/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 192.168.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 3: Configure an address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address 11.1.1.10 11.1.1.100 netmask 255.255.255.0
hostname(config-address-pool)# dns 10.1.1.1
hostname(config-address-pool)#wins 10.1.1.2
hostname(config-address-pool)# exit
hostname(config)#
```

Step 4: Configure an SSL VPN instance (with optimal path detection). To limit the access range of the remote user, use the **no split-tunnel-route 0.0.0.0/0** command

```
hostname(config)# tunnel scvpn ssl1
hostname(config-tunnel-scvpn)# pool pool1
hostname(config-tunnel-scvpn)# aaa-server local
hostname(config-tunnel-scvpn)# interface ethernet0/1
hostname(config-tunnel-scvpn)# https-port 4433
hostname(config-tunnel-scvpn)# split-tunnel-route10.1.1.0/24 metric 10
hostname(config-tunnel-scvpn)# link-select server-detect 202.2.3.1 https-port 2234
196.1.2.3 https-port 3367
hostname(config-tunnel-scvpn)# exit
hostname(config)#
```

Step 5: Create a tunnel interface and bind the SSL VPN instance to it (the tunnel interface and SSL VPN address pool should be in the same IP address segment)

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 11.1.1.1/24
hostname(config-if-tun1)# tunnel scvpn ssl1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6: Configure a policy rule (a rule from dmz zone to trust zone)

```
hostname(config)# address dst
hostname(config-addr)# ip 10.1.1.0/24
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone dmz
```

```
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configure an ISP

```
hostname(config)# isp-network isp1
hostname(config-isp)# subnet 202.2.3.0/24
hostname(config-isp)# subnet 64.2.3.0/24
hostname(config-isp)# exit
hostname(config)#
```

When the client PC initiates a connection request to SSL VPN server using ISP2, the DNAT device translates the client address (196.1.2.3:3367) to SSL VPN server's egress interface address (192.168.1.2:4433). Then, the server identifies that the IP addresses of client PC and DNAT Internet interface (202.2.3.1/24) belong to ISP1, so it assigns the IP of DNAT's Internet interface which has higher priority to the client and the PC can access the headquarters server using ISP1.

Using SSL VPN Client to Choose an Optimal Path

Configuration steps of using client to choose optimal path have slight differences with steps of using the server in choosing optimal path, and the different steps are:

Step 4: Configure an SSL VPN instance (with optimal path detection feature)

```
hostname(config)# tunnel scvpn ssl1
……
hostname(config-tunnel-scvpn)# link-select 202.2.3.1 https-port 2234 196.1.2.3 https-
```

```
port 3367
……
```

Step 7: Skip this step

When the PC initiates connection requests to the headquarters using ISP2 link, the DNAT device translates client address (196.1.2.3:3367) to SSL VPN server’s egress interface address (192.168.1.2: 4433). The SSL VPN server will assign the IP address of DNAT device’s Internet interface to the client, and the client judges the optimal path by sending UDP probe packets.

Dial-up VPN

Overview

Dial-up VPN means the center device has only one VPN tunnel established to allow multiple remote clients accessing to it through this VPN tunnel. The remote clients should be configured with same IKE VPN settings with the center device for data protection. Meanwhile, the center device uses pre-shared key or certificate to authenticate the clients and establishes VPN tunnel to communicate with the clients.

Applying Dial-up VPN

There are two methods of applying a configured VPN tunnel to the security device to achieve secure traffic transmissions: one is to use policy-based VPN, the other is to use route-based VPN.

- Policy-based VPN: When you use policy-based VPN, the VPN tunnel is introduced into a policy rule so that traffic which conforms to the rule can be transferred through the VPN tunnel. Policy-based VPN supports accessing from branch to center, but does not support accessing from center to branch or hub-and-spoke.
- Route-based VPN: When you use route-based VPN, the VPN tunnel binds to a tunnel interface and the next hop of static route is the tunnel interface.

Configuring the Center Device

This section introduces the following configurations of dial-up VPN center device:

- Configuring P1 proposal
- Configuring an ISAKMP gateway
- Configuring P2 proposal
- Configuring a tunnel
- Configuring a dial-up user

Configuring P1 Proposal

P1 proposal is an IKE security proposal applied to ISAKMP gateway in the SA Phase 1. Configuring an IKE proposal includes settings of authentication, encryption algorithm, DH group and SA lifetime.

Creating a P1 Proposal

To create a P1 proposal (IKE security proposal), in the global configuration mode, use the following command:

isakmp proposal *p1-name*

- *p1-name* – Type a name for the new P1 proposal. This command leads you into the P1 proposal configuration mode in which you can configure the proposal.

To delete the specified P1 proposal, use the command **no isakmp proposal** *p1-name*.

Specifying an Authentication Method

Authentication defined here refers to IKE identity authentication which is used to confirm the identities of the two communicating peers. Authentication can be performed in two ways: pre-shared key authentication and digital certificate authentication. For pre-shared key authentication, community is used to generate a private key as the input.

To specify the authentication method of IKE security proposal, in the P1 proposal configuration mode, use the following command:

authentication {**pre-share** | **rsa-sig** | **dsa-sig** | **gm-de** }

- **pre-share** – Specifies that the pre-shared key is used for authentication. This is the default method.
- **rsa-sig** – Specifies that RSA digital certificate is used for authentication.
- **dsa-sig** – Specifies the DAS digital certificate is used for authentication.

- **gm-de** – Uses the envelope authentication mode. When the authentication mode is selected, only encryption algorithm SM1 and SM4 are supported and verification algorithm SHA or SM3 are supported.

To restore to the default authentication method, use the command **no authentication**.

Specifying an Encryption Algorithm

The following five encryption algorithms are supported: 3DES, DES, 128-bit AES, 192-bit AES and 256-bit AES.

To specify the encryption algorithm of IKE security proposal, in the P1 proposal configuration mode, use the following command:

encryption {**3des** | **des** | **aes** | **aes-192** | **aes-256**}

- 3des – Specifies to use 3DES encryption algorithm. The private key length is 192 bits. This is the default encryption method.
- des – Specifies to use DES encryption algorithm. The private key length is 64 bits.
- aes – Specifies to use AES encryption algorithm. The private key length is 128 bits.
- aes-192 – Specifies to use 192-bit AES encryption algorithm. The private key length is 192 bits.
- aes-256 – Specifies to use 256-bit AES encryption algorithm. The private key length is 256 bits.

To restore to the default encryption algorithm, use the command **no encryption**.

Specifying a Hash Algorithm

The following authentication algorithms are supported: MD5, SHA-1 and SHA-2 (including SHA-256, SHA-384 and SHA-512).

To specify a Hash algorithm for IKE security proposal, in the P1 proposal configuration mode, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512**}

- **md5** – Specifies to use MD5 for authentication. The hash value length is 128 bits.
- **sha** – Specifies to use SHA-1 for authentication. The hash value length is 160 bits. This is the default value.
- **sha256** – Specifies to use SHA-256 for authentication. The hash value length is 256 bits.
- **sha384** – Specifies to use SHA-384 for authentication. The hash value length is 384 bits.
- **sha512** – Specifies to use SHA-512 for authentication. The hash value length is 512 bits.

To restore to the default algorithm method, use the command **no hash**.

Selecting a DH Group

Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. The longer the key element is, the more secure the generated key will be, and the more difficult it will be to decrypt it. The selection of DH group is important, because the DH Group is only determined in the Phase 1 SA negotiation, and the Phase 2 negotiation will not re-select a DH group. The two phases use the same DH group; therefore the selection of DH group will have an impact on the keys generated for all sessions. During negotiation, the two ISAKMP gateways should select the same DH group, i.e., the length of key element should be equal. If the DH groups do not match, the negotiation will fail.

To select a DH group, in the P1 proposal configuration mode, use the following command:

group {1 | 2 | 5 | 14 | 15 |16 | 19 | 20 | 21 | 24}

- **1** - Selects DH Group1. The key length is 768 bits (MODP Group).
- **2** - Selects DH Group2. The key length is 1024 bits (MODP Group). This is the default value.
- **5** - Selects DH Group5. The key length is 1536 bits (MODP Group).
- **14** - Selects DH Group14. The key length is 2048 bits (MODP Group).

- **15** - Selects DH Group15. The key length is 3072 bits (MODP Group).
- **16** - Selects DH Group16. The key length is 4096 bits (MODP Group).
- **19** - Selects DH Group19. The key length is 256 bits (ECP Group).
- **20** - Selects DH Group20. The key length is 384 bits (ECP Group).
- **21** - Selects DH Group21. The key length is 521 bits (ECP Group).
- **24** - Selects DH Group24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore the DH group to the default, in the P1 proposal configuration mode, use the command **no group**.

Specifying a SA Lifetime

Phase 1 SA negotiation has a default lifetime. When ISAKMP SA lifetime is due, it sends an SA P1 deleting message to the peer, and then initiates a new SA negotiation.

To specify a SA lifetime, in the P1 proposal configuration mode, use the following command:

lifetime *time-value*

- *time-value* – Specifies the lifetime of SA Phase 1. The value range is 300 to 86400 seconds. The default value is 86400.

To restore to the default lifetime, use the command **no lifetime**.

Configuring an ISAKMP Gateway

This section introduces configurations about ISAKMP gateway.

Creating an ISAKMP Gateway

To create an ISAKMP gateway, in the global configuration mode, use the following command:

isakmp peer *peer-name*

- *peer-name* – Specifies a name for the ISAKMP gateway.

This command leads you into ISAKMP gateway configuration mode in which you can configure the parameters of the gateway.

To delete the specified ISAKMP gateway, in the global configuration mode, use the command **no isakmp peer** *peer-name*.

Specifying an AAA Server for ISAKMP Gateway

AAA server defined here is used to authenticate the peer device.

To specify an AAA server for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

aaa-server *server-name*

- *server-name* – Specifies the name of AAA server. All types of AAA server can be ISAKMP gateway, including local, Radius, AD, LDAP and TACACS+ server.

To delete the specified AAA server, in the ISAKMP gateway configuration mode, use the following command:

no aaa-server

Binding an Interface to the ISAKMP Gateway

To bind an interface to the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the bound interface.

To cancel the binding of interface, use the command **no interface**.

Configuring an IKE Negotiation Mode

There are two IKE negotiation modes: Main and Aggressive. The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in

the situation that the IP address of the center device is static while the IP address of client device is dynamic.

To configure an IKE negotiation mode, in the ISAKMP gateway configuration mode, use the following command:

mode {main | aggressive}

- **main** – The main mode can provide ID protection and it is the default mode.
- **aggressive** – Specifies to use the aggressive mode.

To cancel the IKE negotiation mode, use the command **no mode**.

Specifying a Peer Type

To specify a type for the peer device, in the ISAKMP gateway configuration mode, use the following command:

type usergroup

To cancel the specified type of a peer device, in the ISAKMP gateway configuration mode, use the following command:

no type

Specifying P1 Proposal

To specify P1 proposal for the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

isakmp-proposal p1-proposal1[p1-proposal2] [p1-proposal3] [p1-proposal4]

- **p1-proposal1** – Specifies the name of P1 proposal. You are allowed to specify up to four P1 proposals for an ISAKMP gateway's peer.

To cancel the specified P1 proposal, use the command **no isakmp-proposal**.

Configuring a Pre-shared Key

If you decide to use pre-shared key to authenticate, to specify a pre-shared key for ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

pre-share *string*

- *string* – Specifies the content of pre-shared key.

To cancel the specified pre-shared key, use the command **no pre-share**.

Configuring a PKI Trust Domain

If digital certificate is used to authenticate, you need to specify a PKI trust domain for the certificate. To specify a PKI trust domain, in the ISAKMP gateway configuration mode, use the following command:

trust-domain *string*

- *string* – Specifies the PKI trust domain.

To cancel the specified PKI trust domain, use the command **no trust-domain**.



Tip: For more information about PKI trust domain, see "PKI" in the "User Authentication"

Configuring a Local ID

To specify the type of local identifier (FQDN and Asn1dn are supported), in the ISAKMP gateway configuration mode, use the following command:

local-id {**fqdn** *string* | **asn1dn** [*string*] | **u-fqdn** *string* }

- **fqdn** *string* – Specifies to use FQDN type ID. *string* is the identifier.
- **asn1dn** [*string*] – Specifies to use Asn1dn type ID, which can only be used in authentication with certificate. *string* is the identifier which can me omitted because the system can get the identifier from certificate.
- **u-fqdn** *string* – Specifies to use U-FQDN type ID (email address type, like user-1@hillstonenet.com).

To cancel the local ID setting, use the command no local-id.

Specifying a Connection Type

To specify the connection type of the ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

connection-type {**bidirectional** | **initiator-only** | **responder-only**}

- **bidirectional** – Specifies that the ISAKMP gateway serves as both initiation and responder. This is the default value.
- **initiator-only** – Specifies that the ISAKMP gateway serves only as the initiator.
- **responder-only** – Specifies that the ISAKMP gateway serves only as the responder.

As dial-up VPN cannot be initiator, this parameter can only be set to **bidirectional** or **responder-only**.

To restore to the default value, use the command **no connection-type**.

Enabling NAT Traversal

If an NAT device exists in an IPsec or IKE VPN tunnel and it translates VPN data, NAT traversal function must be enabled. This function is disabled by default.

To enable NAT traversal, in the ISAKMP configuration mode, use the following command:

nat-traversal

To disable NAT traversal, use the command **no nat-traversal**.

Configuring DPD

DPD (Dead Peer Detection) is used to detect the status of peer device. When this function is enabled, the responder initiates a DPD request if it cannot receive packets from the peer for a long time. This function is disabled by default.

To enable DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd

To configure DPD, in the ISAKMP gateway configuration mode, use the following command:

dpd [**interval** *seconds*] [**retry** *times*]

- **interval** *seconds* – Specifies the interval of sending DPD requests. The value range is 1 to 10 seconds. The default value is 10.
- **retry** *times* – Specifies the times of sending DPD request to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.

Specifying Description

To add description for an ISAKMP gateway, in the ISAKMP gateway configuration mode, use the following command:

description *string*

- *string* – Specifies description content for the ISAKMP gateway.

To delete the description, use the command **no description**.

Configuring P2 Proposal

Phase 2 proposal is used during SA Phase 2 negotiation. This section describes how to configure P2 proposal, including protocol type, encryption algorithm, hash algorithm and lifetime.

Creating P2 Proposal

To create P2 proposal (IPsec proposal), in the global configuration mode, use the following command:

ipsec proposal *p2-name*

- *p2-name* – Specifies a name for the P2 proposal. This command leads you into P2 proposal configuration mode where you make all relative configurations.

To delete the specified IPsec proposal, use the command **no ipsec proposal** *p2-name*.

Specifying a Protocol Type

P2 proposal can use AH or ESP protocol type.

To specify a P2 proposal type, in the P2 proposal configuration mode, use the following command:

protocol {esp | ah}

- **esp** – Specifies to use ESP protocol, which is the default value.
- **ah** – Specifies to use AH protocol.

To restore to the default setting, use the command **no protocol**.

Specifying an Encryption Algorithm

P2 proposal can use one to four encryption algorithms.

To specify an encryption algorithm for P2 proposal, in the P2 proposal configuration mode, use the following command:

encryption {3des | des | aes | aes-192 | aes-256 | null} [3des | des | aes | aes-192 | aes-256 | null] [3des | des | aes | aes-192 | aes-256 | null]……

- **3des** - Specifies to use 3DES encryption algorithm. The key size is 192 bits and it is the default algorithm in the system.
- **des** - Specifies to use DES. The key size is 64 bits.
- **aes** - Specifies to use AES. The key size is 128 bits.
- **aes-192** - Specifies to use 192bit AES. The key size is 192 bits.
- **aes-256** - Specifies to use 256bit AES. The key size is 256 bits.
- **null** - No encryption.

To restore to the default setting, use the command **no encryption**.

Specifying a Hash Algorithm

P2 proposal can use one to three hash algorithms.

To specify a hash for P2, in the P2 proposal configuration type, use the following command:

hash {**md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3** | **null**} [**md5** | **sha** | **sha256** | **sha384** | **sha512** | **null**] [**md5** | **sha** | **sha256** | **sha384** | **sha512** |**null**]

- **md5** - Specifies to use MD5 for authentication. The hash value is 128 bits.
- **sha** - Specifies to use SHA-1 for authentication. The hash value is 160 bits. This is the default value.
- **sha256** - Specifies to use SHA-256 for authentication. The hash value is 256 bits.
- **sha384** - Specifies to use SHA-384 for authentication. The hash value is 384 bits.
- **sha512** - Specifies to use SHA-512 for authentication. The hash value is 512 bits.
- **null** - No hash algorithm.

To restore to the default setting, use the command **no hash**.

Configuring PFS

PFS (Perfect Forward Secrecy) is used to ensure that the compromise of one private key in the private key set will not result in the decryption of the entire set of private keys. When PFS is enabled, a private key can be used once and the reference for generating it can only be used once. In this way, when one private key is compromised and revealed, it will not affect the whole encrypted communication.

To enable PFS, in the P2 proposal configuration mode, use the following command:

group {**nopfs** | **1** | **2** | **5** | **14** | **15** |**16**| **19** | **20** | **21** | **24**}

- **nopfs** - Disables PFS. This is the default setting.
- **1** - Selects DH Group1. The key length is 768 bits (MODP Group).

- **2** - Selects DH Group2. The key length is 1024 bits (MODP Group). This is the default value.
- **5** - Selects DH Group5. The key length is 1536 bits (MODP Group).
- **14** - Selects DH Group14. The key length is 2048 bits (MODP Group).
- **15** - Selects DH Group15. The key length is 3072 bits (MODP Group).
- **16** - Selects DH Group16. The key length is 4096 bits (MODP Group).
- **19** - Selects DH Group19. The key length is 256 bits (ECP Group).
- **20** - Selects DH Group20. The key length is 384 bits (ECP Group).
- **21** - Selects DH Group21. The key length is 521 bits (ECP Group).
- **24** - Selects DH Group24. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

To restore to the default setting, use the command **no group**.

Specifying a Lifetime/Lifesize

Lifetime of P2 proposal can be measured by time or by traffic volume. When SA reaches the specified traffic flow amount or runs out of time, this SA expires and new negotiation should be initiated.

To specify a lifetime of P2 proposal, in the P2 proposal configuration mode, use the following commands:

lifetime *seconds*

- *seconds* – Specifies to use time period to measure lifetime. The default value is 28800 seconds.

lifesize *kilobytes*

- *kilobytes* – Specifies to use traffic volume to measure lifetime. The default value is 0 byte, which means no limit on lifesize.

To restore to the default settings, use the following commands:

no lifetime

no lifesize

Configuring a Tunnel

This section describes how to configure an IPsec tunnel, including specifying a protocol type, ISAKMP gateway, IKE proposal, ID, fragmentation and anti-replay.

Creating an IKE Tunnel

To create an IKE tunnel, in the global configuration mode, use the following command:

tunnel ipsec *tunnel-name* **auto**

- *tunnel-name* - Type a name for the new IKE tunnel.

This command leads you into the IKE tunnel configuration mode where you configure all IKE tunnel related configurations.

To delete the specified IKE tunnel, in the global configuration mode, use the command **no tunnel ipsec** *tunnel-name* **auto**.

Specifying an IPsec Mode

To specify the operation mode (tunnel mode) for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

mode tunnel

To restore to the default mode, use the command **no mode**.

Specifying an ISAKMP Gateway

To specify an ISAKMP gateway, in the IKE tunnel configuration mode, use the following command:

isakmp-peer *peer-name*

- *peer-name* – Specifies the name of ISAKMP gateway.

To cancel the specified ISAKMP gateway, use the command **no isakmp-peer**.

Specifying P2 Proposal

To specify P2 proposal for the IKE tunnel, in the IKE tunnel configuration mode, use the following command:

ipsec-proposal *p2-name*

- *p2-name* – Specifies a name for the P2 proposal.

To cancel the specified P2 proposal, use the command **no ipsec-proposal**.

Specify a Phase 2 ID

To specify a Phase 2 ID of the IKE IPsec tunnel, in the IKE tunnel configuration mode, use the following command:

id {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}

- **auto** – Specifies the ID of Phase 2.
- **local** *ip-address/mask* – Specifies the local ID of Phase 2 automatically.
- **remote** *ip-address/mask* – Specifies the Phase 2 ID of the peer device. As the dial-up VPN initiator has no stable ID, the Phase 2 ID should be 0.0.0.0/0.
- **service** *service-name* – Specifies the service name.

You can configure up to 256 phase 2 IDs and use them to establish multiple IKE tunnels. If the center device has been configured with multiple phase 2 IDs, it can negotiate with a remote client to create multiple IPSec SAs. After auto routing is enabled, a route entry whose destination IP address is the local ID of the peer and next hop is the egress IP address of the remote client as a gateway would be added to the routing table automatically once an IPSec SA had been created. When an IPSec SA is deleted, the corresponding route entry will be deleted from the routing table.

To restore the default configurations, use the command **no id** {**auto** | **local** *ip-address/mask* **remote** *ip-address/mask* **service** *service-name*}.

Creating an IPSec SA When There is Inclusion Relation for ID

When the remote ID of phase 2 ID configured in the center device contains the local ID of phase 2 ID configured in the remote client, an IPSec SA can still be successfully created between the center device and the remote client after this feature is configured. To enable this feature, in the IKE tunnel configuration mode, use the following command:

dialup-control-id

To restore to the default setting, use the command **no dialup-control-id**.

Configuring IPSec Balancing and Filtering

A central device can negotiate with a remote client to create multiple IPSec SAs. At the same time, encapsulated packets will be filtered when out-acrossing the IKE tunnel interface and be balanced when in-acrossing the IKE tunnel interface. If a packet's source IP address, destination IP address, and service type match a phase 2 ID, the packet will be processed by the central device; otherwise, the packet will be discarded.

To configure IPSec balancing and filtering, in the IKE tunnel configuration mode, use the following command:

check-id

To restore to the default setting, use the command **no check-id**.

Enabling Auto Connection

The device has two methods of establishing SA: auto and traffic intrigued.

- When it is auto, the device checks SA status every 60 seconds and initiates negotiation request when SA is not established
- When it is traffic intrigued, the tunnel sends negotiation requests only when there is traffic passing through the tunnel.

By default, traffic intrigued mode is used.

To enable auto connection, in the IKE tunnel configuration mode, use the following command:

auto-connect

To restore to the default setting, use the command **no auto-connect**.



Notes: Auto connection works only when the peer IP is static and the local device is initiator.

Configuring Packet Fragmentation

To allow IP packet fragmentation on the forwarding device, in the IKE configuration mode, use the following command:

df-bit {**copy** | **clear** | **set**}

- **copy** – Copies the IP packet DF options from the sender directly. This is the default value.
- **clear** – Allows packet fragmentation.
- **set** – Disallows packet fragmentation.

To restore to the default value, use the command **no df-bit**.

Configuring Anti-replay

Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled.

To configure anti-replay for IKE IPsec tunnel, in the IKE IPsec tunnel configuration mode, use the following command:

anti-replay {**32** | **64** | **128** | **256** | **512**}

- **32** - Specifies the anti-replay window as 32.
- **64** - Specifies the anti-replay window as 64.
- **128** - Specifies the anti-replay window as 128.

- **256** - Specifies the anti-replay window as 256.
- **512** - Specifies the anti-replay window as 512.

When the network condition is poor, choose a larger window.

To disable anti-replay, use the command **no anti-replay**.

Configuring Commit Bit

The commit bit function is used to avoid packet loss and time difference in the tunnel. Configuring this function on this end makes the corresponding peer to use it. However, commit bit may slow the responding speed.

To configure commit bit, in the IKE IPsec tunnel configuration mode, use the command: **responder-set-commit**

To disallow the responder to set commit bit, use the command: **no responder-set-commit**

Configuring Idle Time

Idle time length is the longest time the tunnel can exist without traffic passing through. When the time is over, SA will be cleared.

To configure the idle time, in the IKE IPsec tunnel configuration mode, use the following command:

idle-time *time-value*

- *time-value* – Specifies a time value. The value range is 120 to 3000 seconds.

To disable idle time, in the IKE IPsec tunnel configuration mode, use the following command:

no idle-time

Specifying Description

To give some description of an IKE tunnel, in the IKE tunnel configuration mode, use the following command:

description *string*

- *string* – Type the description you want.

To delete IKE tunnel description, use the command **no description**.

Configuring Auto Routing

For route-based dial-up VPN or PnPVPN, the IP addresses of the branches are always changing, causing operational inconvenience for the administrator if manual routing is used. The auto routing function allows the device to automatically add routing entries from center to branch to avoid complexity of manual routing.

By default the auto routing is disabled. To enable it, in the ISAKMP gateway configuration mode, use the following command:

generate-route

For dial-up VPN, the Phase 2 local ID of auto generated route is its destination address and its next hop is the peer IP address. For information about how to configure a Phase 2 ID, see Specify a Phase 2 ID.

For PnPVPN, the destination address of auto generated route is the AND operation result of the start IP and netmask of client DHCP address pool (dhcp-pool-addr-start & dhcp-pool-netmask), and the next hop address is the peer IP address. For information about client DHCP address pool and netmask, see Configuring a PnPVPN Server Using CLI.

To disable auto routing, use the command **no generate-route**.



Notes:

- If the Phase 2 local ID of initiator in a dial-up VPN is 0.0.0.0/0, you are strongly suggested not to enable auto routing on the center device.
- When the branch office accesses the center, you can use the command **`no reverse-route`** to disable reverse routing and return all the reverse data from the original paths on the center device. The command line will show the number of imported users.

Configuring a Dial-up User

This section describes how to create a dial-up user, including user account and pre-shared key.

Creating a Dial-up User Account

To create a dial-up user account, in the global configuration mode, use the following command:

user *user-name* **aaa-server local**

- *user-name* – Type the user name.

This command leads you into the user configuration mode, where you can specify the user IKE ID with the following command:

ike-id {**fqdn** *string* | **asn1dn** *string*}

- **fqdn** *string* – Specifies to use IKE ID of FQDN type. *string* is the ID content.
- **asn1dn** *string* – Specifies to use ID of Asn1dn type, which only applies to authentication with certificate.

To cancel the IKE ID setting, in the user configuration mode, use the following command:

no ike-id

Generating a Pre-shared Key for Dial-up User

The center device generates a pre-shared key using dial-up user's username and IKE ID.

To generate a pre-shared key, in any mode, use the following command:

exec generate-user-key rootkey *pre-share-key* **userid** *string*

- *pre-share-key* – Specifies the pre-shared key of the device.
- *string* – Specifies the IKE ID of username.

Configuring the Dial-up Client

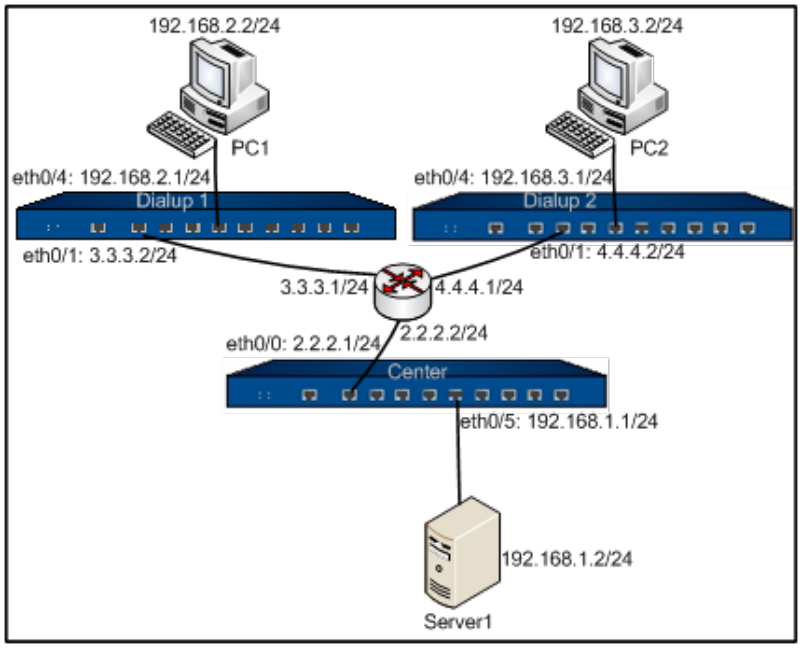
The remote client should configure parameters corresponding to the center device, including P1 proposal, P2 proposal, ISAKMP gateway and tunnel. The configuration commands are similar to those of center device, but if the local ID of initiator's ISAKMP gateway uses pre-shared key, the key must be the corresponding pre-shared key of the center device.

Example of Configuring Dial-up VPN

This section provides a configuration example of dial-up VPN.

Requirement

Two dial-up clients (user1 and user 2) and the center device (2.2.2.1/24) consist of a dial-up VPN. The goal is to allow two computers (PC1 and PC2) accessing the center device protected server (Server1) using secured VPN tunnel.



Configuring the Center Device

Step 1: Configure interfaces

```
hostname(config)# zone vpnzone
hostname(config-zone-vpnzone)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone vpnzone
hostname(config-if-eth0/0)# ip address 2.2.2.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/5
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.1.1/24
hostname(config-if-eth0/5)# exit
```

Step 2: Configure a dial-up user account and pre-shared key

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# ike_id fqdn hillstone1
hostname(config-user)# exit
hostname(config-aaa-server)# user user2
hostname(config-user)# ike_id fqdn hillstone2
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# exit
hostname# exec generate-user-key rootkey 123456 userid hillstone1
userkey: 3zPNDY6MmI8Wejk5fa3jhPU39p8=
hostname# exec generate-user-key rootkey 123456 userid hillstone2
userkey: tAFW+48HcAr15+NcISm6TZJZzGU=
hostname# configure
hostname(config)#
```

Step 3: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.1.2/24 remote 0.0.0.0/0 service
any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 4: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone vpnzone
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone vpnzone
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring Dial-up Client 1

Step 1: Configure interfaces

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 3.3.3.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.2.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

Step 2: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
hostname(config-isakmp-peer)# pre-share 3zPNDY6MmI8Wejk5fa3jhPU39p8=
hostname(config-isakmp-peer)# local-id fqdn hillstone1
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.2.2/24 remote 192.168.1.2/24
service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring Dial-up Client 2

Step1: Configure interface

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 4.4.4.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/5)# zone trust
hostname(config-if-eth0/5)# ip address 192.168.3.1/24
hostname(config-if-eth0/5)# exit
hostname(config)#
```

Step2: Configure IKE VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)#
hostname(config)# isakmp peer test
hostname(config-isakmp-peer)# interface ethernet0/1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# peer 2.2.2.1
hostname(config-isakmp-peer)# pre-share tAFW+48HcAr15+NcISm6TZJZzGU=
hostname(config-isakmp-peer)#
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec vpn auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer test
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# id local 192.168.3.2/24 remote 192.168.1.2/24
service any
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure policy rules

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action tunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zonetrust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action fromtunnel vpn
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

PnPVPN

Overview

IPsec VPN requires sophisticated operation skills and high maintenance cost. To relieve network administrators from the heavy work, Hillstone provides an easy-to-use VPN technology - PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer. The PnPVPN Server issues most of the configuration commands to clients. The Hillstone device usually works as a PnPVPN Server and one Hillstone device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by headquarters engineer. With simple configuration, such as client ID, password and server IP settings, the PnPVPN Client can receive configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server.



Notes: The Hillstone device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instances and the supported client number of each device may vary from hardware platforms.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends its own ID and password to the server.
2. The server validates the ID and password when it receives the client request. If the client passes the authentication, the server issues configuration information including DHCP

address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc. to the client.

3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be configured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

The client supports to configure dual VPN dials and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

Configuring a PnPVPN Server

This section describes the configurations on the server, both in the command line interface and on the WebUI.

Configuring a PnPVPN Server Using CLI

Some of IPsec VPN commands also apply to PnPVPN configuration; in addition, PnPVPN has its unique configuration commands. The commands below in this chapter cannot complete PnPVPN command set alone; for complete PnPVPN settings, see Example of Configuring PnPVPN.

Configuring User's Network

After the client successfully negotiates with the server, the server will distribute some network setting parameters, including DNS server address, WINS server address, tunnel route, DHCP address pool address/netmask and gateway address, to the client. These parameters are configured in the corresponding user configuration modes, but some of them (settings of DNS, WINS and tunnel route) can also be set in IKE tunnel configuration. When there is a conflict between the two settings, configuration in the user configuration mode has higher priority over settings in the IKE tunnel configuration mode.

To enter the local user configuration mode, use the following command:

aaa-server *aaa-server-name* **type local** (this command leads you to the local AAA server configuration mode)

user *user-name*

- user-name – Specifies the user name.

The commands below complete a user's network settings. Among these parameters, settings of DHCP address pool, DHCP netmask and gateway are required while others are optional.

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of DNS server. You can define one primary DNS server and up to three alternative servers. To cancel the DNS server setting, use the command **no dns**.

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of WINS server. You can define one primary DNS server and one alternative WINS server. To cancel the WINS server setting, use the command **no wins**.

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – Specifies the tunnel route. A.B.C.D is the IP address prefix and Mask is the digit of subnet mask. To clear the settings, use the command **no split-tunnel-route A.B.C.D/Mask**.

dhcp-pool-address *start-ipaddr end-ipaddr*

- *start-ipaddr end-ipaddr* – Specifies the start IP address and end IP address of DHCP address pool. To cancel the setting, use the command **no dhcp-pool-address**.

dhcp-pool-netmask *A.B.C.D*

- *A.B.C.D* – Specifies the network mask of DHCP address pool. To cancel the setting, use the command no dhcp-pool-netmask.

dhcp-pool-gateway *A.B.C.D*

- *A.B.C.D* – Specifies the gateway address of DHCP address pool. This address is the Intranet interface's IP address of PnPVPN client and serves as the PC gateway address. As the IP address of PC is defined by the DHCP address pool and subnet mask, the gateway address and DHCP address pool should be in the same network segment. To cancel the setting, use the command **no dhcp-pool-gateway**.

Configuring Tunnel Network

If all or most of the clients use unified DNS, WINS or tunnel route setting, you can configure these parameters in the IKE tunnel mode to reduce workload of making settings in the user configuration mode.

To enter the IKE tunnel configuration mode, use the following command:

tunnel ipsec *tunnel-name* auto

- *tunnel-name* – Specifies the name of IKE tunnel.

To configure the DNS, WINS and tunnel route, use the following commands:

dns *A.B.C.D* [*A.B.C.D*] [*A.B.C.D*] [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of DNS server. You can define one primary server and up to three alternative servers. To cancel the setting, use the command **no dns**.

wins *A.B.C.D* [*A.B.C.D*]

- *A.B.C.D* – Specifies the IP address of WINS server. You can define one primary WINS server and one alternative server. To cancel the setting, use the command **no wins**.

split-tunnel-route *A.B.C.D/Mask*

- *A.B.C.D/Mask* – Specifies the tunnel route. A.B.C.D is the IP address prefix and Mask is the digit of subnet mask. To clear the settings, use the command **no split-tunnel-route**.

Configuring Wildcard of ISAKMP Gateway's Peer

When PnPVPN Server uses Radius server to authenticate, you are required to configure the wildcard of ISAKMP gateway's peer. The wildcard is used to match username and determine the PnPVPN Server of the accessed client (a Hillstone device can serve as multiple PnPVPN servers), so that the Radius server for user's authentication can be identified.

To configure the wildcard of ISAKMP gateway's peer, in the ISAKMP gateway configuration mode, use the following command:

peer-id fqdn wildcard *string*

- **fqdn** – Uses wildcard of FQDN type.
- **wildcard** *string* – Specifies the wildcard ID which is usually the client's domain name, like abc.com.

To cancel wildcard settings, use command **no peer-id**.

Configuring Tunnel Interface of PnPVPN Client

To allow the sub-networks in the branch office accessing the server, you can configure IP address and enable SNAT rule for the client tunnel interface on the PnPVPN server end. If SR Series plat-

form is used as the PnPVPN client, make sure that the version in the platform supports this function.



Notes: When this function is working, the PnPVPN server cannot access its clients.

To enter local user configuration mode, use the following command:

aaa-server *aaa-server-name* **type local** (This command leads you to the local AAA server configuration mode.)

user *user-name*

- *user-name* – Specifies the user name.

To configure tunnel interface of PnPVPN client, in the local user configuration mode, use the following command:

tunnel-ip-address *A.B.C.D* [**snat**]

- *A.B.C.D* – Specifies the IP address of client tunnel interface, but it should not conflict with the existing IP addresses in the client.
- **snat** – Enables SNAT rule. In default, the SNAT rule on tunnel interface is disabled.

To cancel tunnel interface of PnPVPN client, in the local user configuration mode, use the following command:

no tunnel-ip-address

Configuring a PnPVPN Sever Using WebUI

This section describes how to configure PnPVPN server in the WebUI, including:

- Configuring a User
- Configuring IKE VPN
- Configuring an Tunnel Interface

- Configuring a Route
- Configuring a Policy



Notes: PnPVPN support two types of authentication server: Local and Radius.

Configuring a User

To configure a user, take the following steps:

1. Select **Objects > Local User** from the menu bar.
2. In the Local User dialog, select a local server from the **Local server** drop-down list. Click **New**, and select **User** from the drop-down list.
3. On the **Basic** tab in the User Configuration dialog, type a name for the user into the **Name** box.
4. Specify a password for the user in the **Password** box and confirm it in the **Confirm password** box.
5. Click **FQDN** in the IKE ID section, and type the ID's content into the text box below. The ID is used in authentication.
6. Click the **PnPVPN** tab and fill out options in the tab. If the user does not use configured DNS, WINS or tunnel route of the tunnel, these options must be configured.
7. Configure other options as needed.
8. Click **OK** to save the settings.

Configuring IKE VPN

This section introduces how to configure IKE VPN, including how to configure P1 proposal, P2 proposal, VPN peer and tunnel.

To configure P1 proposal, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page and click the **Phase1 Proposal** tab.
2. Click **New**. In the Phase1 Proposal Configuration dialog, finish the options as described below:
    - **Proposal name**: Type the name of the Phase1 proposal.
    - **Authentication**: Select **pre-share**.
    - **HASH**: Select **Group2**.
3. You can fill out other options or leave them blank as needed.
4. Click **OK** to save the settings.

To configure P2 proposal, use the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page and click the **Phase2 Proposal** tab.
2. Click **New**.
3. In the Phase2 Proposal Configuration dialog, type the name of P2 proposal into the **Proposal name** box.
4. Select a protocol, HASH algorithm, encryption algorithm and PFS group as needed.
5. You can fill out other options or use the default value as needed.
6. Click **OK** to save the settings.

To configure the peer, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page. Click the **VPN Peer List** tab.
2. In the Peer Configuration dialog, click **New**.

3. On the **Basic** tab, configure the options below:

    - **Peer name**: Type the name of the ISAKMP gateway.
    - **Interface**: Select an interface bound to the ISAKMP gateway.
    - **Mode**: Select **Aggressive**.
    - **Type**: Select **user group**, and select the AAA server you need from the **AAA server** drop-down list.
    - **Proposal 1**: Select a P1 proposal you want from the list.
    - **Pre-shared key**: Type the pre-shared key into the box.

4. Configure other options as needed or use the default values.
5. Click **Generate**. In the Generate user key dialog, type the IKE ID into the **IKE ID** box, and then click **Generate**. The generated user key will be displayed in the Generate result box. PnPVPN client uses this key as the password to authenticate the login users. Then, close the dialog.
6. Click **OK** to save the settings.



Notes: If Radius server works as the authentication server, wildcard must be configured.

To configure a tunnel, take the following steps:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.
2. On the upper-left of the IKE VPN List, Click **New**.

3. Under **Step 1: Peer**, click **Import** in the Peer name section, and select a peer you want from the drop down list; type the IP address of the peer into the **Peer address** box. Or, you can create a new peer (ISAKMP gateway) on this tab.
4. Click **Step 2: Tunnel** and configure the options:
    - **Name**: Type a name for the tunnel.
    - **Mode**: Select **tunnel**.
    - **P2 proposal**: Select a proposal you need from the drop down list.
5. Click the **Advanced** tab. In this tab, configure DNS, WINS and tunnel route (tunnel users will use the DNS and WINS defined here).
6. Configure other options as needed or use the default values.
7. Click **OK** to save the settings.



Notes: If Radius server works as the authentication server, wildcard must be configured.

Configuring a Tunnel Interface

To configure tunnel interface, take the following steps:

1. On the Navigation pane, click **Configure > Network > Network** to visit the Network page.
2. Click **New** on the upper-left of the interface list, and select **Tunnel Interface** from the drop-down list. Configure the following options:
    - **Name**: Type the number of the tunnel.
    - **Binding zone**: Select **Layer 3 zone**.
    - **Zone**: Select a zone for the interface from the drop-down list.

3. Under **Tunnel binding**, select **IPsec VPN** and select VPN tunnel from the **VPN name** drop down list. Gateway address is not needed here.

4. Click **OK** to save settings.

Configuring a Route

To allow hosts in the server network to access the client network, you need to add static routes.

To add a route, take the following steps:

1. On the Navigation pane, click **Configure > Network > Routing** to visit the Routing page.

2. On the **Destination Route** tab, click **New**.

3. In the Destination Route Configuration dialog, type the IP address for the route into the **Destination** box.

4. Type the corresponding subnet mask into the **Subnet mask** box.

5. To specify the type of next hop, click **Interface**, and select the **VPN tunnel interface** from the **Interface** drop-down list below, then type the gateway address for the tunnel's peer into the optional box below.

6. Configure other options as needed or use the default values.

7. Click **OK** to save the settings.

Configuring a Policy

Policies are configured according to the network deployment (on the Navigation pane, click **Configure** > **Security** > **Policy** to visit the Policy page).

Configuring a PnPVPN Client

This section describes how to configure a PnPVPN Client. To configure a PnPVPN, take the following steps:

1. On the Navigation pane, click Configure > Network > IPsec VPN to visit the IPsec VPN page.
2. On the Task tab in the right auxiliary pane, click PnPVPN Client.
3. In the PnPVPN Configuration dialog, finish the options.
    - **Server address 1**: Type the IP address of PnPVPN Server into the box. This option is required.
    - **Server address 2**: Type the IP address of PnPVPN Server into the box. The server address 1 and the server address 2 can be the same or different. It is optional.
    - **ID**: Specifies the IKE ID assigned to the client by the server.
    - **Password**: Specifies the password assigned to the client by the server.
    - **Confirm password**: Enter the password again to make confirmation.
    - **Auto save**: Select **Enable** to auto save the DHCP and WINS information released by PnPVPN Server.
    - **Outgoing IF 1**: Specifies the interface connecting to the Internet. This option is required.
    - **Outgoing IF 2**: Specifies the interface connecting to the Internet. The IF1 and the IF2 can be the same or different. It is optional.
    - **Incoming IF**: Specifies the interface on PnPVPN Server accessed by Intranet PC or application servers. Click the interface you want. If **Incoming IF** is selected, also select an interface from the **Interface** drop-down list; if multiple Intranet interfaces connect to PnPVPN, you should click **BGroup IF**, and add interface members of that bgroup. To add interface members, select the interface(s) you want from the **Avail-**

able list, and add it to the **Selected** list. To delete an interface member, select it and remove it from the **Selected** list .

4. Click **OK** to save the settings.

Example of Configuring PnPVPN

This section describes an example of PnPVPN configuration.

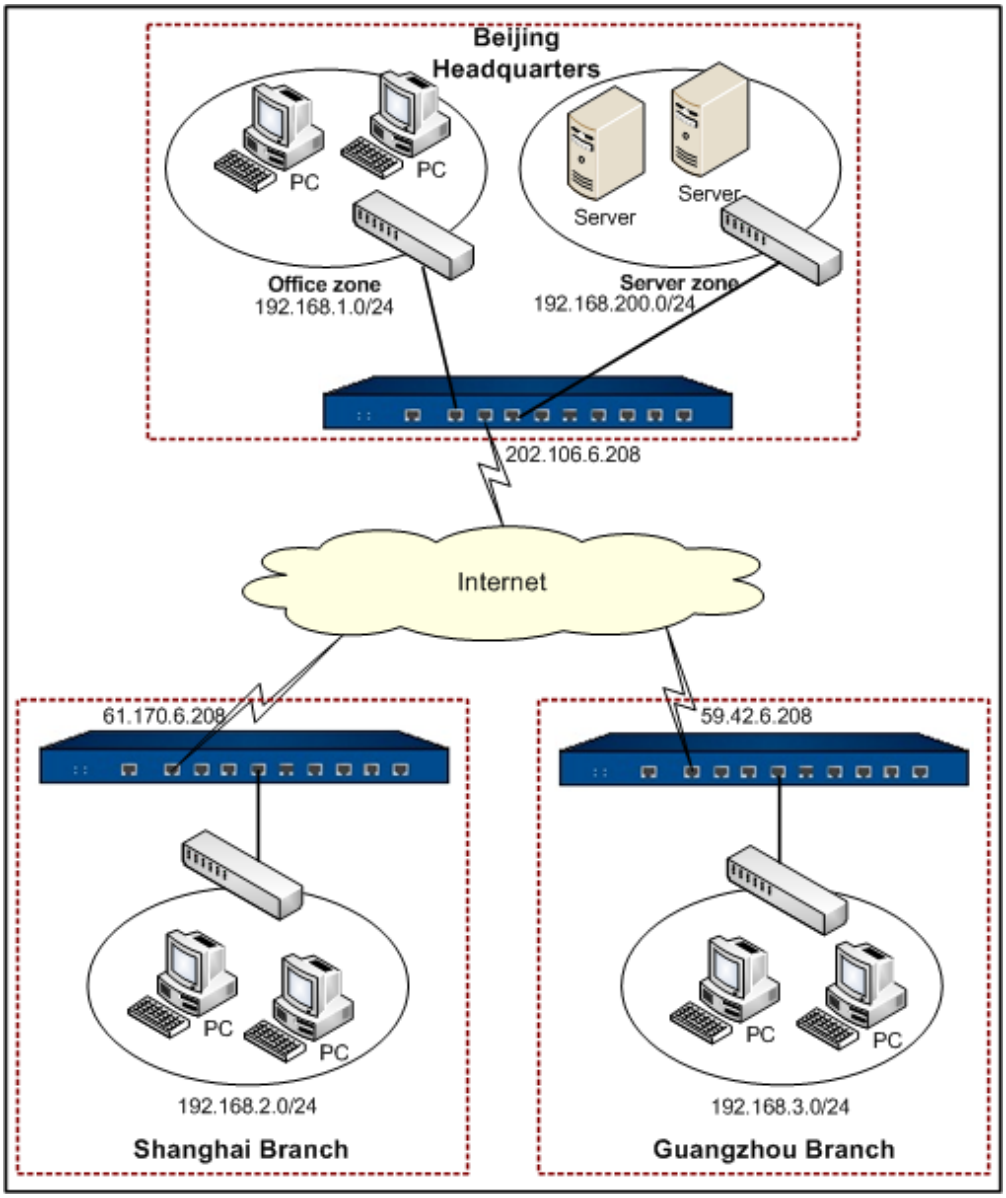
Requirement

A company has its headquarters in Beijing and two branch offices in Shanghai and Guangzhou, all three of which have Internet access. Its business demands that a VPN network should be established. The goals of the network are:

- Employees in Guangzhou Branch and Shanghai Branch can access the headquarters database via VPN;
- All the employees (including the Beijing headquarters and two branches) can share resources via VPN.

PnPVPN is a practical and easy-to-use method to meet the requirements above. Take the following steps:

- The headquarters uses a next-genration firewall as the PnPVPN Server and chooses the local authentication.
- Each of the two branches has a next-generation firewall, working as the PnPVPN Client and accessing the headquarters VPN network.
- To share resource among all employees in the three places, you should configure policies and routes.



According to the topology, the network environment can be described as follows:

- The headquarters LAN network segment is 192.168.1.0/24 and it uses ethernet0/0 of trust zone to access the network.
- The headquarters server group network segment is 192.168.200.0/24 and it uses ethernet0/2 of trust zone to access the network.

- The headquarter security device use ethernet 0/1 (IP: 202.106.6.208) of untrust zone to access the network.
- Shanghai Branch uses an interface with IP 61.170.6.208 to access the Internet, and Guangzhou Branch uses an interface with IP 59.42.6.208 to access the Internet.
- PnPVPN Server will allocate the network segment 192.168.2.0/2 to Shanghai Branch and 192.168.3.0/24 to Guangzhou Branch.

Configuration Steps

Take the steps below to configure the server end and client ends:

Configuring the Server

Step 1: Configure the local AAA server

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure the network in Shanghai Branch

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# ike-id fqdn shanghai
hostname(config-user)# dhcp-pool-address 192.168.2.1 192.168.2.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.2.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.3.0/24
hostname(config-user)# exit
```

```
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure the network in Guangzhou Branch

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user guangzhou
hostname(config-user)# ike-id fqdn guangzhou
hostname(config-user)# dhcp-pool-address 192.168.3.1 192.168.3.100
hostname(config-user)# dhcp-pool-netmask 255.255.255.0
hostname(config-user)# dhcp-pool-gateway 192.168.3.101
hostname(config-user)# split-tunnel-route 192.168.200.0/24
hostname(config-user)# split-tunnel-route 192.168.1.0/24
hostname(config-user)# split-tunnel-route 192.168.2.0/24
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 4: Configure a PnPVPN Server

```
hostname(config)# isakmp proposal test1
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal test2
hostname(config-ipsec-proposal)# group 2
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer test1
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# interface ethernet0/1
```

```
hostname(config-isakmp-peer)# aaa-server test
hostname(config-isakmp-peer)# isakmp-proposal test1
hostname(config-isakmp-peer)# pre-share 123456
hostname(config-isakmp-peer)#generate-route
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec test auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal test2
hostname(config-tunnel-ipsec-auto)# isakmp-peer test1
hostname(config-tunnel-ipsec-auto)# mode tunnel
hostname(config-tunnel-ipsec-auto)# id auto
hostname(config-tunnel-ipsec-auto)# dns 192.168.200.1 192.168.200.11
hostname(config-tunnel-ipsec-auto)# wins 192.168.200.2 192.168.200.12
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 5: Generate client private keys

```
hostname(config)# exec generate-user-key rootkey 123456 userid shanghai
userkey: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
hostname(config)# exec generate-user-key rootkey 123456 userid guangzhou
userkey: SdqhY4+dPThTtpipW2hs2OMB5Ps=
```

Step 6: Configure policies

```
hostname(config)# zone VPN
hostname(config-zone-VPN)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone VPN
hostname(config-if-tun1)# tunnel ipsec test
hostname(config-if-tun1)# exit
```

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone VPN
hostname(config-policy-rule)# dst-zone VPN
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring the Clients

In the Shanghai Branch:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.
2. On the **Task** tab in the right auxiliary pane, click **PnPVPN Client**. In the PnPVPN Configuration dialog, configure the options as below:
    - **Server address**: 202.106.6.208
    - **ID**: shanghai
    - **Password**: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
    - **Confirm password**: kyZAKmLWCc5Nz75fseDiM2r+4Vg=
    - **Auto save**: Select the **Enable** checkbox
    - **Outgoing IF**: ethernet0/0
    - **Incoming IF**: ethernet0/3
3. Click **OK** to save your settings.

In the Guangzhou Branch:

1. On the Navigation pane, click **Configure > Network > IPsec VPN** to visit the IPsec VPN page.
2. On the **Task** tab in the right auxiliary pane, click **PnPVPN Client**. In the PnPVPN Configuration dialog, configure the options as below:
    - **Server address**: 202.106.6.208
    - **ID**: guangzhou

- **Password**: SdqhY4+dPThTtpipW2hs2OMB5Ps=
- **Confirm password**: SdqhY4+dPThTtpipW2hs2OMB5Ps=
- **Auto save**: Select the **Enable** checkbox
- **Outgoing IF**: ethernet0/0
- **Incoming IF**: ethernet0/3

3. Click **OK** to save your settings.

GRE

Overview

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol inter-network. StoneOS uses GRE over IPSEC feature to ensure the security of routing information passing between networks.

Configuring GRE

This section introduces how to configure GRE, including:

- Configuring a GRE tunnel
- Binding the GRE tunnel to a tunnel interface

Configuring a GRE Tunnel

Configurations for GRE tunnel should be performed in the GRE tunnel configuration mode.

To enter the GRE tunnel configuration mode, in the global configuration mode, use the following command:

tunnel gre *gre-tunnel-name*

- *gre-tunnel-name* – Specifies the name of the new GRE tunnel. This command creates a new GRE tunnel; if the tunnel with this name exists, you will enter its configuration mode directly.

To delete the specified GRE tunnel, use the following command:

no tunnel gre *gre-tunnel-name*

In the GRE tunnel configuration mode, you need to configure the following parameters for the tunnel:

- Source interface/address
- Destination address
- Egress interface
- IPsec VPN tunnel (optional)
- Verification key

Specifying a Source Interface/Address

To define a source interface for the GRE tunnel, in the GRE tunnel configuration mode, use the following command:

source {**interface** *interface-name* [**ipv6**] |{*ipv4-address* | *ipv6-address*} }

- **interface** *interface-name* [**ipv6**] – Specifies the name of interface as the source interface of the GRE tunnel.
- *ipv4-address* | *ipv6-address* – Specifies the IP address (Ipv4 and IPv6).

To cancel source address setting, in the GRE tunnel configuration mode, use the following command:

no source

Specifying a Destination Address

To specify a destination address for the GRE tunnel, in the GRE tunnel configuration mode, use the following command:

destination{*ipv4-address* | *ipv6-address*}

- *ipv4-address* | *ipv6-address* – Specifies the destination address for the GRE tunnel.

To cancel the specified destination address, in the GRE tunnel configuration mode, use the following command:

no destination

Specifying an Egress Interface

To specify the egress interface for the GRE tunnel, in the GER tunnel configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of egress interface.

To cancel the egress interface setting, in the GRE tunnel configuration mode, use the following command:

no interface

Specifying an IPsec VPN Tunnel

When using GRE over IPsec function, you need to specify an IPsec VPN tunnel to encapsulate the tunnel data.

To specify an IPsec VPN tunnel, in the GRE tunnel configuration mode, use the following command:

next-tunnel ipsec *tunnel-name*

- *tunnel-name* – Specifies the name of IPsec VPN tunnel.

To cancel the specified IPsec VPN tunnel, in the GRE tunnel configuration mode, use the following command:

no next-tunnel

Specifying a Verification Key

By specifying a verification key, the system encapsulates and verifies the packets. When the key carried by the packets is the same as the key configured in the receiver, the packets will be decrypted. If the keys are not the same, the packets will be dropped. To specify the verification key, in the GRE tunnel configuration mode, use the following command:

key *key-value*

- *key-value* – Specifies the verification key. The value ranges from 0 to 4294967295.

To cancel the configurations, use the following command in the GRE tunnel configuration mode:

no key

Binding the GRE Tunnel to a Tunnel Interface

A well configured GRE tunnel needs to be bound to the tunnel interface so that it can work.

To bind the GRE tunnel to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel gre *gre-tunnel-name* [**gw** *ip-address*]

- *gre-tunnel-name* – Specifies the name of the well configured GRE tunnel which binds to the interface.
- **gw** *ip-address* – This parameter is required when multiple tunnels bind to this interface. It defines the next hop (the peer tunnel interface) IP address of GRE tunnel. The default value is 0.0.0.0.

To cancel the binding of GRE tunnel to the tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel gre *gre-tunnel-name*

Viewing GRE Tunnel Information

To view GRE tunnel setting information, in any mode, use the following command:

show tunnel gre [*gre-tunnel-name*]

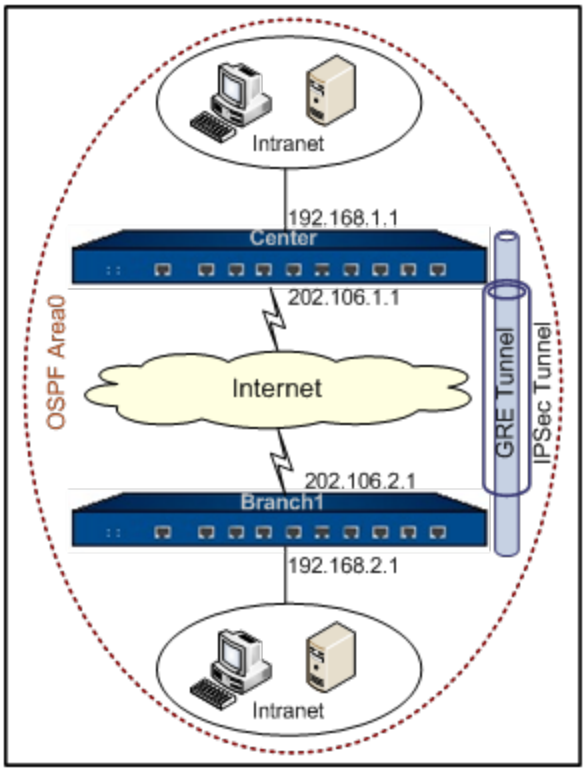
- *gre-tunnel-name* – Specifies the name of GRE tunnel you want to view.

Example of Configuring GRE Tunnel

This section provides a configuration example of GRE over IPsec with OSPF in a Hillstone device.

Requirement

The headquarters (Center) and the branch office (Branch1) are connected by the Internet using OSPF protocol. The connection uses GRE over IPsec technique to ensure secure data transmission between the center and the branch. The figure below is the topology of the network layout.



Configuration Steps

Configurations for this requirement include settings on the headquarters device (Center) and on the branch office device (Branch1).

Configuring the Center

The following commands are the necessary settings of IPsec VPN and OSPF.

Step 1: Configure the interface

```
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#exit
```

Step 2: Configure the IPsec VPN

```
hostname(config)# isakmp proposal branch1
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal branch1
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer branch1
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.2.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp branch1
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec branch1 auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer branch1
hostname(config-tunnel-ipsec-auto)# ipsec-proposal branch1
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure the GRE tunnel

```
hostname(config)# tunnel gre center-branch1
hostname(config-tunnel-gre)# source 202.106.1.1
hostname(config-tunnel-gre)# destination 202.106.2.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec branch1
hostname(config-tunnel-gre)# exit
hostname(config)#
```

Step 4: Bind the GRE tunnel to the tunnel interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.1/24
hostname(config-if-tun1)# tunnel gre center-branch1 gw 172.16.1.2
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure OSPF

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.1
hostname(config-router)# network 172.16.1.1/24 area 0
hostname(config-router)# network 192.168.1.1/24 area 0
hostname(config-router)# exit
hostname(config-vrouter)# exit
hostname(config)#
```

Step 6: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule
```

```
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configuring the Branch

Step 1: Configure the interface

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 202.106.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/1)# zone trust
```

```
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 2: Configure the IPsec VPN

```
hostname(config)# isakmp proposal center
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal center
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer center
hostname(config-isakmp-peer)# interface ethernet0/0
hostname(config-isakmp-peer)# peer 202.106.1.1
hostname(config-isakmp-peer)# pre-share 111111
hostname(config-isakmp-peer)# isakmp center
hostname(config-isakmp-peer)# exit
hostname(config)# tunnel ipsec center auto
hostname(config-tunnel-ipsec-auto)# isakmp-peer center
hostname(config-tunnel-ipsec-auto)# ipsec-proposal center
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure the GRE tunnel

```
hostname(config)# tunnel gre branch1
hostname(config-tunnel-gre)# source 202.106.2.1
hostname(config-tunnel-gre)# destination 202.106.1.1
hostname(config-tunnel-gre)# interface ethernet0/0
hostname(config-tunnel-gre)# next-tunnel ipsec center
hostname(config-tunnel-gre)# exit
```

```
hostname(config)#
```

Step 4: Bind the GRE tunnel to the tunnel interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 172.16.1.2/24
hostname(config-if-tun1)# tunnel gre branch1 gw 172.16.1.1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure OSPF

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 172.16.1.2
hostname(config-router)# network 172.16.1.2/24 area 0
hostname(config-router)# network 192.168.2.1/24 area 0
hostname(config-router)# exit
hostname(config-vrouter)# exit
hostname(config)#
```

Step 6: Configure a policy

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)#
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

L2TP

Overview

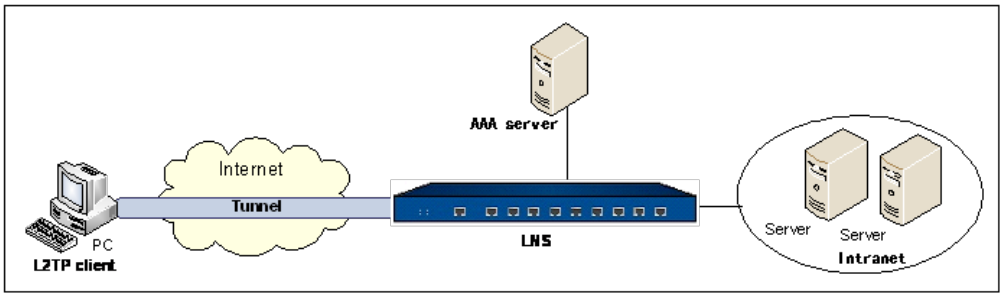
L2TP (Layer Two Tunneling Protocol) is a VPDN technique that allows dial-up users to launch VPN connection from L2TP clients or L2TP access concentrators (LAC), and connect to a L2TP network server (LNS) via PPP. After the connection has been established successfully, LNS will assign IP addresses to legal users and permit them to access the private network.

The device acts as a LNS or a LAC client in the L2TP tunnel network. When the device acts as a LNS, the device accepts connections from L2TP clients or LACs, implements authentication and authorization, and assigns IP addresses, DNS server addresses and WINS server addresses to legal users. When the device acts as a LAC client, the device actively initiates PPP negotiation and authentication. After the tunnel is established, the traffic will be transmitted to the opposite end through the L2TP VPN tunnel.

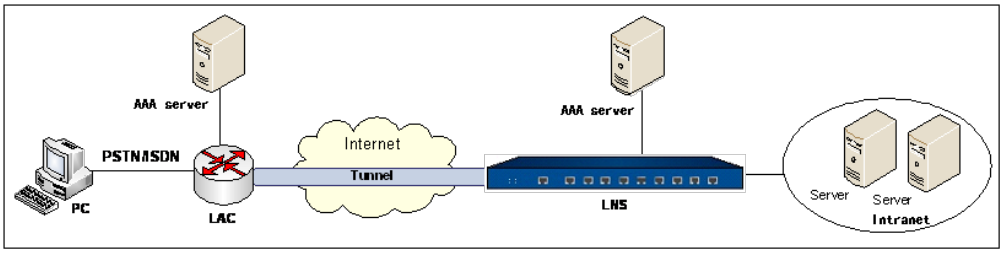
Note: For more information about L2TP, see RFC2661.

Typical L2TP Tunnel Network

There are two kinds of typical L2TP tunnel network modes:



The figure above shows the network topology where the L2TP client directly sends requests for connection to the LNS, and attempts to establish a tunnel. Any PC installed with Windows 2000/2003/XP/Vista or Linux system can serve as the L2TP client.



The figure above shows the network topology where the remote user dials up to LAC via PSTN/ISDN, and the LAC launches a VPN connection and attempts to establish a tunnel. LAC is the device that provides access service for remote dial-up users. It lies between the remote dial-up user and LNS, and is responsible for data forwarding between them. The connection between LAC and remote dial-up users adopts PPP or local connection, while the connection between LAC and LNS requires a tunnel established over L2TP.

L2TP over IPSec

L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPsec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the L2TP tunnel.

To configure L2TP over IPsec, take the following steps:

1. Configure a L2TP client, and make sure IPsec encryption is enabled. For more information about how to configure IPsec encryption on a client, see the user manual of your OS; for the configuration on Windows XP, see Example of Configuring L2TP over IPsec.
2. Configure IPsec VPN. For more information, see IPsec Protocol.
3. Configure a L2TP instance, and reference the configured IPsec tunnel.
4. Configure a policy rule.

When using the L2TP client on Windows systems, keep in mind that:

- The L2TP client on Windows systems only supports the IKE negotiation of the main mode; therefore, you need to configure the IKE negotiation mode to main mode on LNS. For the supported mode of the L2TP client on other systems, see related user manual.

- IPsec on Windows systems only supports the transport mode; therefore, you need to configure IPsec to transparent mode on LNS.

Configuring LNS

The configurations of LNS include:

- Configuring an address pool
- Configuring a L2TP instance
- Binding the L2TP instance to a tunnel interface
- Kicking out a user
- Restarting a tunnel

Configuring an Address Pool

LNS assigns the IP addresses in the address pool to users. After the client has established a connection to LNS successfully, LNS will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and assigns them to the client. To create a L2TP address pool, in the global configuration mode, use the following command:

l2tp pool *pool-name*

- *pool-name* – Specifies the name of the address pool.

The above command creates the address pool with the specified name, and leads you to the L2TP address pool configuration mode; if the specified name exists, the system will directly enter the L2TP address pool configuration mode.

To delete the specified L2TP address pool, in the global configuration mode, use the following command:

no l2tp pool *pool-name*

You can configure the following options in the L2TP address pool configuration mode:

- IP range of the address pool
- Reserved IP address
- IP binding rules

Configuring the IP Range of the Address Pool

To configure an IP range of the address pool, in the L2TP address pool configuration mode, use the following command:

address *start-ip end-ip*

- *start-ip* – Specifies the start IP of the IP range.
- *end-ip* – Specifies the end IP of the IP range.

You can specify up to 60000 IP addresses for an address pool.

To delete the specified IP range, in the L2TP address pool configuration mode, use the following command:

no address

Configuring the Reserved IP Address

Some IP addresses can be reserved in the reserved address pool, and they will not be allocated. When allocating IP addresses in the address pool, LNS will reserve the addresses that are occupied by other services (such as gateway, FTP server, etc.). To configure the reserved IP address, in the L2TP address pool configuration mode, use the following command:

exclude-address *start-ip end-ip*

- *start-ip* – Specifies the start IP of the reserved IP address.
- *end-ip* – Specifies the end IP of the reserved IP address.

To delete the specified reserved IP address, in the L2TP address pool configuration mode, use the following command:

no exclude *address*

Configuring IP Binding Rules

L2TP provides fixed IP addresses by creating and implementing IP binding rules that consist of static IP binding rule and role-IP binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, the system will assign the binding IP to the client. The rule-IP binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, the system will assign an IP address within the IP range to the client.

When LNS is allocating IP addresses in the address pool, the system will check the IP binding rule and determine how to assign IP addresses for the client based on the specific checking order below:

1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, further check other configurations. Note if the binding IP address is in use, the user will be unable to log in when it is in use.
2. Check if the client is configured with any role-IP binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.



Notes: The IP addresses defined in the static IP binding rule and role-IP binding rule should not be overlapped.

Configuring a Static IP Binding Rule

To configure a static IP binding rule, in the L2TP address pool configuration mode, use the following command:

ip-binding user *user-name ip-address*

- **user** *user-name* – Specifies the username of the client.
- *ip-address* – Specifies the binding IP address which must be an available address in the address pool.

To cancel the specified static IP binding rule, in the L2TP address pool configuration mode, use the following command:

no ip-binding user *user-name*

Configuring a Role-IP Binding Rule

To configure a role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

ip-binding role *role-name* **ip_range** *start-ip end-ip*

- **role** *role-name* – Specifies the name of the role.
- **ip_range** *start-ip end-ip* – Specifies the start IP and end IP of the binding IP range which must be an available IP range in the address pool.

To cancel the specified role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

no ip-binding role *role-name*

Moving a role-IP Binding Rule

One user can be bound to one or multiple roles, and different roles can be configured with different role-IP binding rules. For the user that is bound to multiple roles and the roles are also configured with their corresponding role-IP binding rules, the system will query the role-IP binding rules in turn, and assign an IP address based on the first matched rule. By default the system will put the new rule at the bottom of all rules. You can move a role-IP binding rule to change its matching sequence. To move a role-IP binding rule, in the L2TP address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role –name1* – Specifies the name of the role-IP binding rule that will be moved.
- **before** *role-name2* – Moves the role-IP binding rule before the rule named role-name2.
- **after** *role-name2* – Moves the role-IP binding rule after the rule named role-name2.

- **top** – Moves the role-IP binding rule to the top of all the rules.
- **bottom** – Moves the role-IP binding rule to the bottom of all the rules.

Configuring a L2TP Instance

To create an L2TP instance, in the global configuration mode, use the following command:

tunnel l2tp *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP instance.

After executing the above command, the system will create the L2TP instance with the specified name, and enter the L2TP instance configuration mode; if the specified name exists, the system will directly enter the L2TP instance configuration mode.

To delete the specified L2TP instance, in the global configuration mode, use the following command:

no tunnel l2tp *tunnel-name*

You can configure the following options in the L2TP instance configuration mode:

- IP address assignment
- Address pool
- DNS server
- WINS server
- Egress interface of the tunnel
- AAA server
- PPP authentication protocol
- Hello interval
- Tunnel authentication

- Tunnel password
- Local name of LNS
- AVP hidden
- Window size of the tunnel data
- Multi-Logon
- Enabling/disabling user-specified client IP
- Retry times of control packets
- Enabling/Disabling Calculating the Checksum of UDP Packet
- Referencing the User Going Offline Alarm Profile

Specifying the IP Address Assignment Method

LNS assigns IP addresses and DNS server address to users using the address pool or the local AAA server. By default, LNS assigns IP addresses by address pool.

To specify the IP address assignment method for the L2TP instance, use the following command in the L2TP instance configuration mode:

assign-client-ip from { **pool** | **aaa-server** }

- **pool** – Uses the address pool to assign IP addresses and DNS server address.
- **aaa-server** – Uses the AAA server to assign IP addresses and DNS server address.



Notes: The type of the local AAA server must be Radius.

Specifying an Address Pool

To specify a L2TP address pool for the L2TP instance, in the L2TP instance configuration mode, use the following command:

pool *pool-name*

- *pool-name* – Specifies the name of the L2TP address pool defined in the system.

To cancel the specified L2TP address pool, in the L2TP instance configuration mode, use the following command:

no pool

Configuring a DNS Server

To configure a DNS server, in the L2TP instance configuration mode, use the following command:

dns *address1* [*address2*]

- *address1* – Specifies the IP address of the DNS server. You can configure up to two DNS servers.

To cancel the specified DNS server, in the L2TP instance configuration mode, use the following command:

no dns

Configuring a WINS Server

To configure a WINS server, in the L2TP instance configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* – Specifies the IP address of the WINS server. You can configure up to two WINS servers.

To cancel the specified WINS server, in the L2TP instance configuration mode, use the following command:

no wins

Specifying the Egress Interface of the Tunnel

To specify the egress interface of the tunnel, in the L2TP instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the interface.

To cancel the specified egress interface, in the L2TP instance configuration mode, use the following command:

no interface

Specifying an AAA Server

The AAA server specified here is used by LNS for L2TP authentication. To specify an AAA server, in the L2TP instance configuration mode, use the following command:

aaa-server *aaa-server-name* [**domain** *domain-name* [*keep-domain-name*]]

- *aaa-server-name* – Specifies the name of the AAA server.
- *domain domain-name* – Specifies the domain name of the AAA server to distinguish different AAA servers.
- *keep-domain-name* – After specifying this parameter, the AAA server uses the full name of the user, including the username and the domain name, to perform the authentication.

To cancel the specified AAA server, in the L2TP instance configuration mode, use the following command:

no aaa-server *aaa-server-name* [**domain** *domain-name*]

Specifying a PPP Authentication Protocol

When establishing a connection with the client or LAC, the LNS can adopt either PAP or CHAP for authentication during the PPP negotiation. To specify a PPP authentication protocol, in the L2TP instance configuration mode, use the following command:

ppp-auth {**pap** | **chap** | **any**}

- **pap** – Uses PAP for PPP authentication.
- **chap** – Uses CHAP for PPP authentication. This is the default option.

- **any** – Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

To restore to the default authentication configuration, in the L2TP instance configuration mode, use the following command:

no ppp-auth

Specifying the Hello Interval

L2TP uses Hello packets to detect if the tunnel is connected. LNS sends Hello packets to the L2TP client or LAC regularly, and will drop the connection to the tunnel if no response is returned after the specified period. To specify the Hello interval, in the L2TP instance configuration mode, use the following command:

keepalive *time*

- *time* – Specifies the Hello interval. The value range is 60 to 1800 seconds. The default value is 60.

To restore to the default Hello interval, in the L2TP instance configuration mode, use the following command:

no keepalive

Enabling Tunnel Authentication

Before establishing a tunnel, you can enable tunnel authentication to assure the security of the connection. The tunnel authentication can be launched by either LNS or LAC. The tunnel cannot be established unless the both ends are authenticated, i.e., the secret strings of the two ends are consistent. By default tunnel authentication is disabled. To enable the function, in the L2TP instance configuration mode, use the following command:

tunnel-authentication

To disable tunnel authentication, in the L2TP instance configuration mode, use the following command:

no tunnel-authentication

Specifying the Secret String

To specify the secret string that is used for LNS tunnel authentication, in the L2TP instance configuration mode, use the following command:

secret *secret-string* [**peer-name** *name*]

- *secret-string* – Specifies the secret string for the tunnel. The value range is 30 to 60 characters.
- **peer-name** *name* – Specifies the host name of LAC. If multiple LACs are connected to LNS, you can specify different secret strings for different LACs by this parameter. If this parameter is not specified, the system will use the same secret string for all the LACs.

To cancel the specified secret string, in the L2TP instance configuration mode, use the following command: **no secret** *secret-string* [**peer-name** *name*]

Specifying the Local Name of LNS

To specify the local name of LNS, in the L2TP instance configuration mode, use the following command:

local-name *name*

- *name* – Specifies the name of the LNS tunnel. The value range is 6 to 30 characters. The default name is LNS.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no local-name

Enabling AVP Hidden

L2TP uses AVP (attribute value pair) to transfer and negotiate some L2TP parameters and attributes. By default AVP is transferred in plain text. For data security consideration, you can encrypt the data by the secret string to hide the AVP during the transmission. To enable or disable AVP hidden, in the L2TP instance configuration mode, use the following commands:

- Enable: **avp-hidden**
- Disable (default): **no avp-hidden**



Notes: To enable AVP hidden, you must configure the secret string for the tunnel.

Specifying the Window Size of the Tunnel Data

To configure the window size for the data transmitted through the tunnel, in the L2TP instance configuration mode, use the following command:

tunnel-receive-window *window-size*

- *window-size* – Specifies the window size. The value range is 4 to 800 packets. The default value is 8.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no tunnel-receive-window

Configuring Multi-Logon

Multi-logon function allows a user to log on and be authenticated on different hosts simultaneously. This function is enabled by default. To enable or disable multi-logon, in the L2TP instance configuration mode, use the following commands:

- Enable: **allow-multi-logon**
- Disable: **no allow-multi-logon**

Enabling/Disabling User-Specified Client IP

By default the client IP is selected from the address pool, and allocated by LNS automatically. If this function is enabled, you can specify an IP address. However, this IP address must belong to the specified address pool, and be consistent with the username and role. If the specified IP is already in use, the system will not allow the user to log on. To enable or disable user-specified client IP, in the L2TP instance configuration mode, use the following commands:

- Enable (default): **accept-client-ip**
- Disable: **no accept-client-ip**

Specifying the Retry Times of Control Packets

L2TP uses two types of packets: control packets and data packets. The control packets are responsible for establishing, maintaining and clearing the L2TP tunnel, while the data packets are responsible for transmitting data. The transmission of data packets is not reliable. Even if data is lost, the transmission will not be retried; while the transmission of control packets is reliable. If no response is received from the peer after the specified retry times, the system will determine the tunnel connection is disconnected. The interval of re-transmitting control packets starts from 1 second, and increases by the multiples of 2, i.e., 1 second, 2 seconds, 4 seconds, 8 seconds, 16 seconds…

To specify the retry times of control packets, in the L2TP instance configuration mode, use the following command:

transmit-retry *times*

- *times* – Specifies the retry times of control packets. The value range is 1 to 10 times. The default value is 5.

To restore to the default value, in the L2TP instance configuration mode, use the following command:

no transmit-retry

Referencing an IPsec Tunnel

When configuring L2TP over IPsec, you need to combine an IPsec tunnel to the L2TP tunnel in order to encrypt data. To reference an IPsec tunnel in the L2TP instance, in the L2TP instance configuration mode, use the following command:

next-tunnel ipsec *tunnel-name*

- *tunnel-name* – Specifies the name of the IPsec VPN tunnel defined in the system.

To cancel the specified IPsec tunnel, in the L2TP instance configuration mode, use the following command:

no next-tunnel ipsec

Configuring Mandatory LCP Phase

After a remote dial-up user connects to the LAC, the LAC starts the L2TP VPN to the LNS and establishes the tunnel. When the LNS authenticates the users, it can execute the LCP (Link Control Protocol) phase or not.

By default, the LNS does not execute the LCP phase with the L2TP client. Instead, it authenticates the L2TP client based on the authentication type specified by the Proxy Authen Type AVP in the ICCN (Incoming-Call-Connected) packets.

To configure the mandatory LCP phase between the LNS and the L2TP client, use the following command in the L2TP instance configuration mode:

ppp-lcp-force

To disable the mandatory LCP phase, use the **no ppp-lcp-force** command.

When a remote dial-up user connects to the LNS directly, the ICCN packets will not carry the Proxy Authen Type AVP. The LNS will always execute the LCP phase with the L2TP client.

Enabling/Disabling Calculating the Checksum of UDP Packet

System will calculate the checksum of UDP packet is disabled. If you need to improve the performance of the device, you can disable this function. To enable/disable calculating the checksum of UDP packet, in the L2TP instance configuration mode, use the following command:

- Enable: **l2tp-udp-checksum enable**
- Disable: **l2tp-udp-checksum disable**

Referencing the User Going Offline Alarm Profile

The system supports the User Going Offline Alarm function. When you configure an L2TP VPN instance, you can reference a configured user going offline alarm profile to monitor the offline status of users. When the number of users going offline exceeds the specified threshold within a

specified period of time, the system generates an alarm.

To reference a user going offline alarm profile, in L2TP instance configuration mode, use the following command:

user-logout-alarm*profile_name*

- *profile_name* – Specifies the name of the configured user going offline alarm profile.

To delete the user going offline alarm profile, in L2TP instance configuration mode, use the following command:

no user-logout-alarm



Notes:

- Before you reference a user going offline alarm profile, you need to configure the user going offline alarm profile. For more information, see Creating a User Going Offline Alarm Profile.
- Only the L2TP VPN function can reference user going offline alarm profiles. The total number of times that all user going offline alarm profiles are referenced in the system cannot exceed 8.
- When a user going offline alarm profile is referenced, you cannot modify the alarm threshold.

Binding the L2TP Instance to a Tunnel Interface

The configured L2TP instance will not take effect until it is bound to a tunnel interface. When a L2TP instance is only bound to a tunnel interface and you do not specify the domain name to the L2TP tunnel (the tunnel with a L2TP instance bound), all clients that connect to a certain LNS will be divided to the VR that relates to the this LNS.

You can also bind multiple tunnel interfaces to one L2TP instance and specify a domain name for each L2TP tunnel. When clients connect to the LNS and the user pass the authentication, the system will divide users into a L2TP tunnel with the same domain name specified. Then, if the

tunnel interfaces belong to different VRs, LNS, by using the authentication server, can repeatedly distribute the internal resource addresses to the clients in each L2TP tunnel

Each tunnel interface can only be bound with one L2TP instance. To bind the L2TP instance to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel l2tp *tunnel-name* [**bind-to-domain** *domain-name*]

- *tunnel-name* – Specifies the name of the L2TP instance defined in the system.
- **bind-to-domain** *domain-name* – Binds the domain name to the L2TP tunnel. If you bind the domain name, usernames without the domain name cannot dial up successfully. If you do not bind the domain name, LNS will omit the domain name of usernames when authenticating users.

To cancel the binding and the specified domain name, in the tunnel interface configuration mode, use the following command:

no tunnel l2tp *tunnel-name*

To cancel the specified domain name, in the tunnel interface configuration mode, user the following command:

no tunnel l2tp *tunnel-name* **bind-to-domain** *domain-name*

Specifying the ACF Information Carried by PPP Data

When establishing a connection with the client or LAC, you can specify whether the PPP data message sent by the LNS contains the ACF field information (Address Control Field) when encapsulating the PPP data message, that is, the address and control field carried by PPP data message . In the global configuration mode, use the following command:

l2tp-include-ppp-acf

In the global configuration mode, use the following command to cancel PPP data containing ACF information

no l2tp-include-ppp-acf

Kicking out a User

To kick out a user from the LNS connection, in the execution mode, use the following command:

exec l2tp *tunnel-name* **kickout user** *user-name*

- *tunnel-name* – Specifies the name of the L2TP instance.
- *user-name* – Specifies the name of the user who will be kicked out.

Restarting a Tunnel

After the tunnel is restarted, all the connections to the tunnel will be cleared. To restart a tunnel, in any mode, use the following command:

clear l2tp *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP instance.

Viewing L2TP Information

To view the L2TP information, use the following commands:

- Show the L2TP instance information:

  show tunnel l2tp [*l2tp-tunnel-name*]

- Show the L2TP tunnel status:

  show l2tp tunnel *l2tp-tunnel-name*

- Show the specified client information of the L2TP instance:

  show l2tp client {*tunnel-namel2tp-tunnel-name* [**user***user-name*] [**public-ip***ip_address*] | **tunnel-id***ID*}

- Show the L2TP address pool configuration:

  show l2tp pool [*pool-name*]

- Show the L2TP address pool statistics:

  show l2tp pool *pool-name* **statistics**

- Show all the clients of the L2TP instance:

  show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

Configuring L2TP Client

To establish a L2TP tunnel between the L2TP client and LNS, you need to configure a L2TP client. For more information about L2TP on Windows 2000/2003/XP/Vista, see the corresponding Windows 2000/2003/XP/Vista documents.



Notes: When establishing a dial-up connection to LNS from the L2TP client on Windows system, make sure the system has not been not installed with Hillstone Secure Defender.

Configuring Device as L2TP Client

The configurations of L2TP Client include:

- Configuring a L2TP Client Instance
- Clear L2TP Client Connection
- View L2TP Client Instance Information

Configuring a L2TP Client Instance

To create an L2TP client instance, in the global configuration mode, use the following command:

tunnel l2tp-client *tunnel-name*

- *tunnel-name* – Specifies the name of the L2TP client instance.

After executing the above command, the system will create the L2TP client instance with the specified name, and enter the L2TP client instance configuration mode; if the specified name exists, the system will directly enter the L2TP client instance configuration mode.

To delete the specified L2TP client instance, in the global configuration mode, use the following command:

no tunnel l2tp-client*tunnel-name*

You can configure the following options in the L2TP client instance configuration mode:

- Specifying the Tunnel Interface
- Specifying IP Address of LNS
- Specifying Keepalive of Tunnel
- Configuring Auto Connect
- Specifying a PPP Authentication Protocol
- Specifying the LCP-echo Interval and Transmit Retries
- Specifying the User Name and Password of L2TP Client
- Specifying the Retry Times of Control Packets

Specifying the Tunnel Interface

To specify the tunnel interface used to bind to the L2TP VPN tunnel, tunnel interface transmits traffic to/from L2TP VPN tunnel, in the L2TP client instance configuration mode, use the following command:

interface*interface-name*

- *interface-name* – Specifies the name of tunnel interface.

To cancel the specified tunnel interface in the L2TP client instance configuration mode, use the following command:

no interface

Specifying IP Address of LNS

To specify the IP address of the LNS server, in the L2TP client instance configuration mode, use the following command:

lns ip*ip-address*

- *ip-address*- Specifies the IP address of the LNS server.

To cancel the specified LNS server, in the L2TP client instance configuration mode, use the following command:

no lns ip*ip-address*

Specifying Keepalive of Tunnel

To ensure normal communication between the LNS and L2TP client, the L2TP client periodically sends Hello packets to check whether the LNS is properly connected. Keepalive indicates the interval at which the L2TP client sends two Hello packets. The smaller the value, the quicker the fault sensing; the larger the value, the lower the occupied bandwidths. To specify the Hello interval, in the L2TP client instance configuration mode, use the following command:

keepalive*time*

time – Specifies the Hello interval. The value range is 60 to 1800 seconds. The default value is 60.

To restore to the default Hello interval, in the L2TP client instance configuration mode, use the following command:

no keepalive

Configuring Auto Connect

After the auto connect function is enabled, the L2TP client and LNS can establish tunnels. Users can access the intranet connected to the LNS, without performing the PPP dialup. In the L2TP client instance configuration mode, use the following command:

l2tp-auto-client

To disable the auto connect function, in the L2TP client instance configuration mode, use the following command:

no l2tp-auto-client

Specifying a PPP Authentication Protocol

When establishing a connection with the LNS, the L2TP client can adopt either PAP or CHAP for authentication during the PPP negotiation. To specify a PPP authentication protocol, in the L2TP client instance configuration mode, use the following command:

ppp-auth {**pap** | **chap** | **any**}

- **pap** – Uses PAP for PPP authentication.
- **chap** – Uses CHAP for PPP authentication. This is the default option.
- **any** – Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

To restore to the default authentication configuration, in the L2TP client instance configuration mode, use the following command:

no ppp-auth

Specifying the LCP-echo Interval and Transmit Retries

Specifies the interval and retry times for sending LCP Echo packets, in the L2TP client instance configuration mode, use the following command:

ppp-lcp-echo interval *time* **retry** *times*

- **interval** *time* – Specifies the interval at which LCP Echo packets are sent. The value range is 0 to 1000 seconds. The default value is 30.
- **retry** *times* - Specifies the retry times for sending LCP Echo packets. If L2TP client has not received any response after the specified retry times, it will determine the connection is disconnected. The default value is 4.

To restore to the default value, in the L2TP client instance configuration mode, use the following command:

no ppp-lcp-echo interval *time* **retry** *times*

Specifying the User Name and Password of L2TPClient

The L2TP client uses the user name and password to initiate a request to the LNS for establishing an L2TP VPN tunnel.

Specifies the name and password of the L2TP client, in the L2TP client instance configuration mode, use the following command:

user*user-name***password***password*

- *user-name* - Specifies the name of the L2TPclient, The value range is 1 to 31 characters.
- *password* - Specifies the password of the L2TP client, The value range is 4 to 63 characters.

Specifying the Retry Times of Control Packets

To specify the retry times of control packets, in the L2TP client instance configuration mode, use the following command:

transmit-retry*times*

times – Specifies the retry times of control packets. The value range is 1 to 10 times. The default value is 5.

To restore to the default value, in the L2TP client instance configuration mode, use the following command:

no transmit-retry

Clear L2TP Client Connection

To clear the connection of L2TP client, in any mode, use the following command:

clear l2tp-client [*tunnel-name*]

- *tunnel-name* - Specifies the name of L2TP client connection.

View L2TP Client Instance Information

To view the L2TP client information, use the following commands:

Show the L2TP client instance information:

show tunnel l2tp-client [*tunnel-name*]

Show the dialing information of the L2TP client:

show l2tp-client [*tunnel-name*]

Configuring L2TPv3 Tunnel

L2TPv3(Layer Two Tunneling Protocol - Version 3) is an IP-based high-performance tunneling technology and used to transparently transmit Layer 2 traffic.

To configure the L2TPv3 tunnel, in the globle configuration mode, use the following command:

tunnel l2tpv3*tunnel-name*

- *tunnel-name* - Specifies the name of the L2TPv3 tunnel.

To delete the specified L2TPv3 tunnel, use the following command:

no tunnel l2tpv3*tunnel-name*

To cofigure the egress interface for L2TPv3 tunnel, in the L2TPv3 tunnel configuration mode, use the following command:

interface*interface-name*

- *interface-name* - Specifies the name of the egress interface for L2TPv3 tunnel.

To delete the egrss interface for specified L2TPv3 tunnel, use the following command:

no interface

To configure local session-id and remote session-id for interoperation between the local and remote devices of an L2TPv3 tunnel, in the L2TPv3 tunnel configuration mode, use the following command:

id*local-session-id remote-session-id*

- *local-session-id* - Specifies the local session-id for L2TPv3 tunnel.
- *remote-session-id* - Specifies the remote session-id for L2TPv3 tunnel.

All packets must match the configured cookie value or be discarded. Cookies are used in security checks performed at the endpoints of a tunnel to prevent network spoofing and attacks.

The local and remote cookie values must be the same.

To configure the local cookie, in the L2TPv3 tunnel configuration mode, use the following command:

cookie local {**4** *lower-value* | **8***lower-value high-value*}

- **4** *lower-value* - Specifies a 4-byte local cookie value in simple text.
- **8***lower-value high-value* - Specifies the four low-order bytes of an 8-byte local cookie value in simple text.

To delete the specified local cookie, use the following command:

no cookie local

To configure the remote cookie, in the L2TPv3 tunnel configuration mode, use the following command:

cookie remote {**4** *lower-value* | **8***lower-value high-value*}

- **4** *lower-value* - Specifies a 4-byte local cookie value in simple text.
- **8***lower-value high-value* - Specifies the four low-order bytes of an 8-byte local cookie value in simple text.

To delete the specified remote cookie, use the following command:

no cookie remote

To configure the destination IP address of L2TPv3 tunnel, in the L2TPv3 tunnel configuration mode, use the following command:

destination*ip-address*

- *ip-address* - Speicifies the destination IP address of L2TPv3 tunnel.

To delete the specified destination IP address, use the following command:

no destination

To configure the zone of L2TPv3 tunnel, in the L2TPv3 tunnel configuration mode, use the following command:

zone *zone*

- *zone* - Speicifies the destination IP address of L2TPv3 tunnel.

To delete the specified zone, use the following command:

no zone

To bind tunnel interface for L2TPv3 tunnel, in the tunnel interface configuration mode, use the following command:

tunnel l2tpv3 *tunnel-name* [**filter ipv6**]

- *tunnel-name* - Specifies the name of L2TPv3 tunnel.
- **filter ipv6** - Configure IPv6 packet filtering for the L2TPv3 tunnel.

To cancel the configuration of binding tunnel interface for L2TPv3 tunnel, use the following command:

no tunnel l2tpv3*tunnel-name*

To view L2TPv3 tunnel information, in the tunnel interface configuration mode, use the following command:

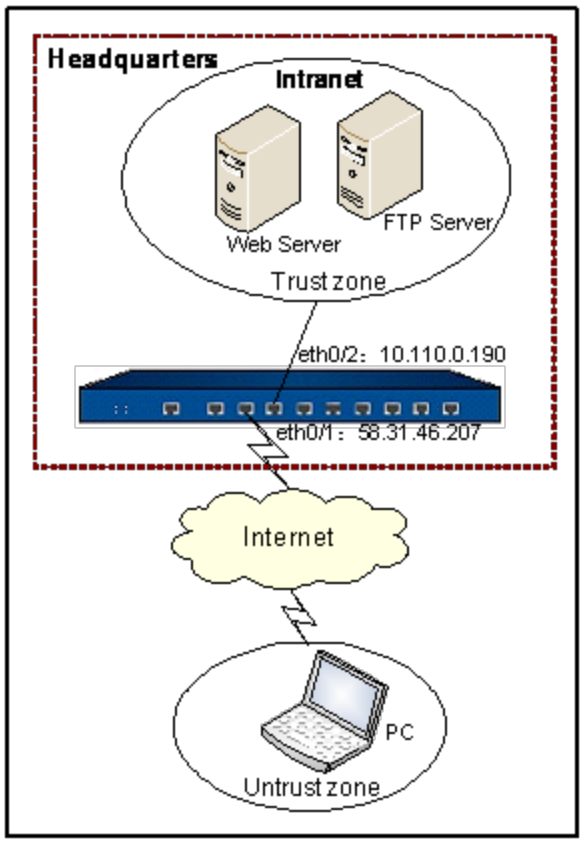
show tunnel l2tpv3 *tunnel-name*

Example of Configuring L2TP

This section describes a typical L2TP configuration example.

Requirement

A remote employee needs to visit the Intranet of the headquarters via L2TP VPN. The network topology is shown as below:



Configuration Steps

Configure LNS and L2TP client respectively.

Configurations on LNS

Step 1 : Configure interfaces

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 58.31.46.207/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
```

```
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 2 : Configure a local AAA server

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3 : Configure the LNS address pool and specify the IP range

```
hostname(config)# l2tp pool pool1
hostname(config-l2tp-pool)# address 10.232.241.2 10.232.244.254
hostname(config-l2tp-pool)#dns 202.106.0.20 10.188.7.10
hostname(config-l2tp-pool)# exit
hostname(config)#
```

Step 4 : Configure a L2TP instance

```
hostname(config)# tunnel l2tp test
hostname(config-tunnel-l2tp)# pool pool1
hostname(config-tunnel-l2tp)# interface ethernet0/1
hostname(config-tunnel-l2tp)# ppp-auth any
hostname(config-tunnel-l2tp)# keepalive 1800
hostname(config-tunnel-l2tp)# aaa-server local
hostname(config-tunnel-l2tp)# exit
hostname(config)#
```

Step 5 : Create a tunnel interface and bind the L2TP instance named test to the interface

```
hostname(config)# interface tunnel1
```

```
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ip address 10.232.241.1 255.255.248.0
hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp test
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 6 : Configure a policy rule

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configurations on the Client

The following sections describe how to configure the client in a Windows XP system. The configuration steps are:

1. Create a L2TP dial-up connection.
2. Configure the dial-up connection and modify the properties.
3. Modify the registry to disable IPsec encryption.

Creating a L2TP Dial-up Connection

To create a L2TP connection on Windows XP, take the following steps:

1. Click **Start > Control Panel > Network Connections**.
2. Click **Create a new connection > Connect to the network at my workplace**, and click **Next**.
3. In the New Connection Wizard dialog, click **Virtual Private Network Connection**, and click **Next**.
4. Type **L2TP** into the **Company Name** box, and click **Next**.
5. Select **Do not dial the initial connection**, and click **Next**.
6. Type the LNS IP address 58.31.46.207 into the **Host name** or **IP address** box, and click **Next**.
7. Complete other L2TP client configurations as prompted.

Configuring L2TP Dial-up Connection

To modify the properties of the dial-up connection, take the following steps:

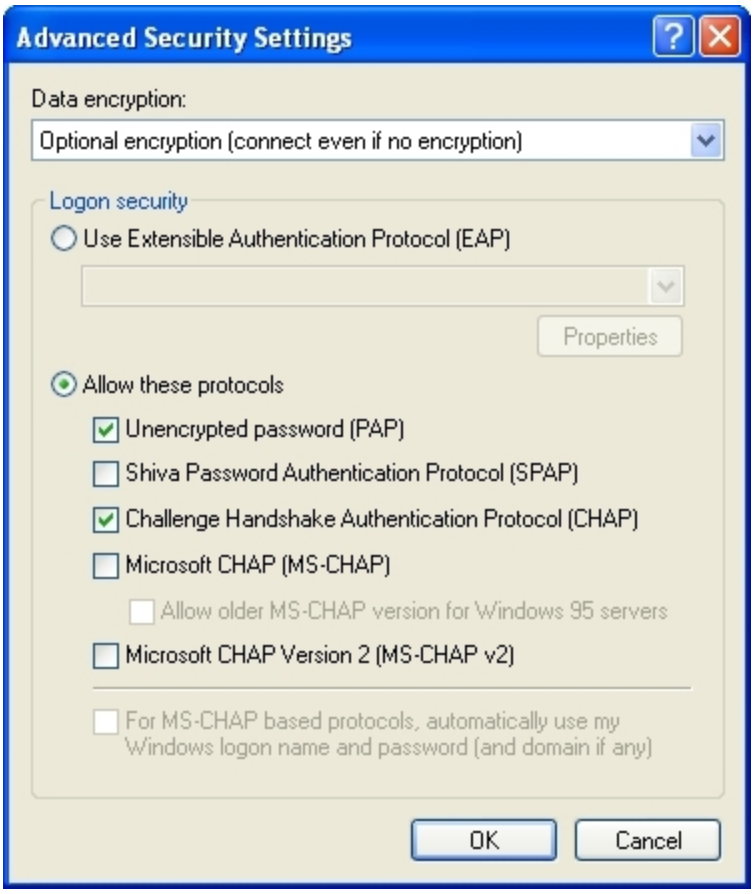
1. In My Network Places, double click the connection named L2TP.



2. In the Connect L2TP dialog shown below, click **Properties**.

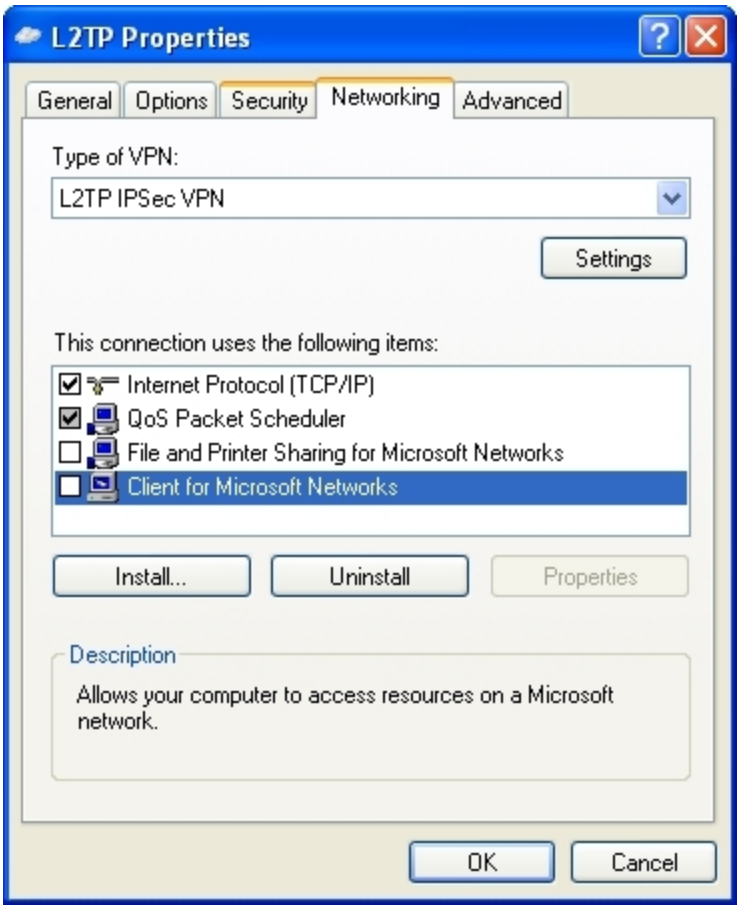
3. In the L2TP Properties dialog, click the **Security** tab, and click **Advanced (custom settings)**. Click **Settings** behind.

4. In the Advanced Security Settings dialog, select **Optional encryption (connect even if no encryption)** from the **Data encryption** drop-down list, click **Allow these protocols** in the Logon security box, and select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**, as shown below:



5. In the L2TP Properties dialog, click the **Network** tab. Select **L2TP IPsec VPN** from the **Type of VPN** drop-down list, and select **Internet Protocol (TCP/IP)** in the **This connection**

uses the following items box, as shown below:



6. Click **OK** to save the changes.

Modifying the Registry

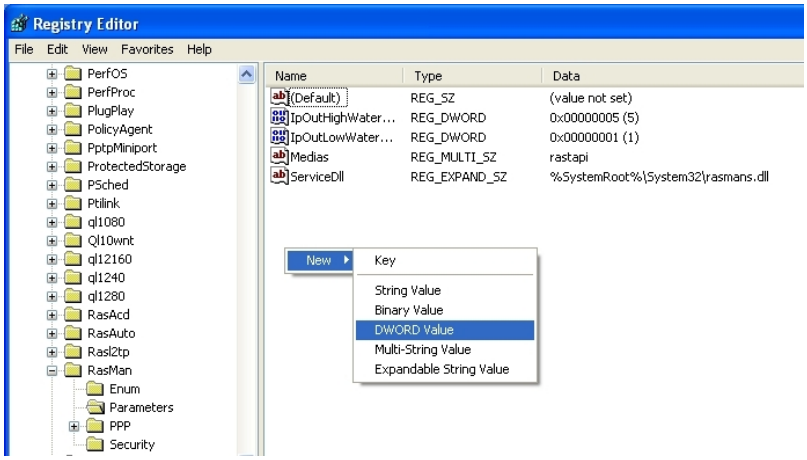
By default Windows XP enables IPsec encryption on the L2TP connection. You can disable the default action by modifying the Windows XP registry. If IPsec encryption is not disabled, the L2TP client will be disconnected automatically during dialing up.

To modify the registry, take the following steps:

1. Click **Start** > **Run**, and type Regedt32 into the **Open** box.

2. In the Registry Editor dialog, navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters.

3. Add a DWORD value for Parameters. Click **Parameters**, and right-click any blank place in the right pane. From the menu, click **New > DWORD** value, as shown below. Specify the name as ProhibitIPsec, type as REG_DWORD, and value as 1. Click **OK** to save the settings.



4. Exit the registry editor and restart the system to make the modification take effect.

Connecting to LNS from the Client

After the above LNS and client configuration, you can initiate a VPN connection to LNS and establish a tunnel from the client.

In My Network Places, double click the dial-up connection named L2TP. In the Connect L2TP dialog, type shanghai and 123456 into the **User name** and **Password** boxes respectively, and click **Connect**, as shown below.



After the dial-up connection has been established, the employee in Shanghai can gain access to the Web server and FTP server in the Intranet securely over L2TP.

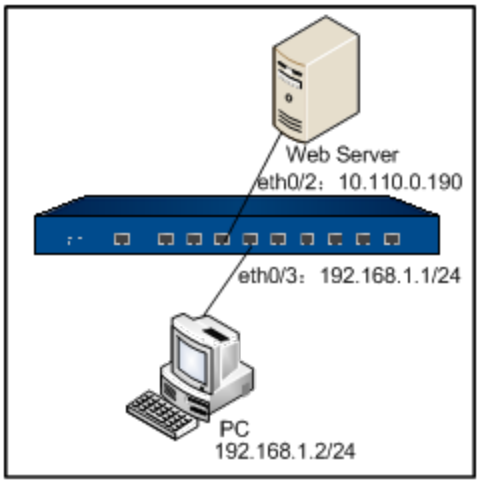
In MS-DOS, the command ipconfig will return the address in the LNS address pool 10.232.241.215, i.e., the IP address allocated to PC by LNS.

Example of Configuring L2TP over IPsec

This section describes a typical L2TP over IPsec configuration example.

Requirement

An employee needs to visit the Web server in the Intranet via L2TP VPN. Data transmission between the PC and LNS is encrypted by IPsec. The network topology is shown below.



Configuration Steps

Configure LNS and L2TP client respectively.

Configurations on LNS

Step 1: Configure interfaces

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.110.0.190/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone untrust
hostname(config-if-eth0/3)# ip address 192.168.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 2: Configure IPsec VPN

```
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# authentication pre-share
hostname(config-isakmp-proposal)# hash sha
```

```
hostname(config-isakmp-proposal)# exit
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha
hostname(config-ipsec-proposal)# encryption 3des
hostname(config-ipsec-proposal)# exit
hostname(config)# isakmp peer east
hostname(config-isakmp-peer)# interface ethernet0/3
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# accept-all-peer-id
hostname(config-isakmp-peer)# mode main
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# pre-share hello1
hostname(config-isakmp-peer)# aaa-server local
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# mode transport
hostname(config-tunnel-ipsec-auto)# isakmp-peer east
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# accept-all-proxy-id
hostname(config-tunnel-ipsec-auto)# exit
hostname(config)#
```

Step 3: Configure a local AAA server

```
hostname(config)# aaa-server test type local
hostname(config-aaa-server)# user shanghai
hostname(config-user)# password 123456
hostname(config-user)# exit
```

```
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 4: Configure the LNS address pool and specify the IP range

```
hostname(config)# l2tp pool pool2
hostname(config-l2tp-pool)# address 10.10.10.2 10.10.10.100
hostname(config-l2tp-pool)#dns 202.106.0.20
hostname(config-l2tp-pool)# exit
hostname(config)#
```

Step 5: Configure a L2TP instance and reference an IPsec tunnel

```
hostname(config)# tunnel l2tp l2tp1
hostname(config-tunnel-l2tp)# pool pool2
hostname(config-tunnel-l2tp)# interface ethernet0/3
hostname(config-tunnel-l2tp)# next-tunnel ipsec vpn1
hostname(config-tunnel-l2tp)# ppp-auth chap
hostname(config-tunnel-l2tp)# keepalive 1800
hostname(config-tunnel-l2tp)# aaa-server test
hostname(config-tunnel-l2tp)# exit
hostname(config)#
```

Step 6: Create a tunnel interface and bind the L2TP instance named l2tp1 to the interface

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone dmz
hostname(config-if-tun1)# ip address 10.10.10.1/24
hostname(config-if-tun1)# manage ping
hostname(config-if-tun1)# tunnel l2tp l2tp1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 7: Configure a policy rule

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone dmz
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Configurations on the Client

The following sections describe how to configure the client in a Windows XP system. The configuration steps are:

1. Create a L2TP dial-up connection.
2. Configure the dial-up connection and modify the properties.
3. Modify the registry to enable IPsec encryption.

Creating L2TP Dial-up Connection

To create a L2TP connection on Windows XP, take the following steps:

1. Click **Start > Control Panel > Network Connections**.
2. Click **Create a new connection > Connect to the network at my workplace**, and click **Next**.

3. In the New Connection Wizard dialog, click **Virtual Private Network Connection**, and click **Next**.
4. Type **L2TP over IPsec** into the **Company Name** box, and click **Next**.
5. Select **Do not dial the initial connection**, and click **Next**.
6. Type the LNS IP address 192.168.1.1 into the **Host name** or **IP address** box, and click **Next**.
7. Complete other L2TP client configurations as prompted.

Configuring the L2TP Dial-up Connection

To modify the properties of the dial-up connection, take the following steps:

1. In My Network Places, double click the connection named L2TP over IPsec.
2. In the Connect L2TP over IPsec dialog, click **Properties**.
3. Click tabs to configure properties, as described below:

   • Security:

   - Click **Advanced (custom settings)**, and then click **Settings** behind. In the Advanced Security Settings dialog, select **Optional encryption (connect even if no encryption)** from the **Data encryption** drop-down list, click **Allow these protocols** in the Logon security box, and select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**. Click **OK** to save the settings.
   - Click **IPsec settings**. In the IPsec Settings dialog, select **Use pre-shared key for authentication**, and type hello1 into the **Key** box. Click **OK** to save the changes.

   • Network:

   - Select **L2TP IPsec VPN** from the **Type of VPN** drop-down list, and select **Internet Protocol (TCP/IP)** in the **This connection uses the following items** box.

4. Click **OK** to save the changes and close the dialog.

Enabling IPsec Encryption

By default Windows XP enables IPsec encryption on the L2TP connection. If disabled, you can re-enable the default action by modifying the Windows XP registry.

To modify the registry, take the following steps:

1. Click **Start > Run**, and type Regedt32 into the **Open** box.
2. In the Registry Editor dialog, navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\RasMan\Parameters.
3. Add a DWORD value for Parameters. Click **Parameters**, and right click any blank place in the right pane. From the menu, click **New > DWORD value**. Specify the name as ProhibitIPsec, type as REG_DWORD, and value as 0. Click **OK** to save the settings.
4. Exit the registry editor and restart the system to make the modification take effect.

Connecting LNS from the Client

After the above LNS and client configuration, you can initiate a VPN connection to LNS and establish a tunnel from the client.

In **My Network Places**, double click the dial-up connection named L2TP over IPsec. In the Connect L2TP over IPsec dialog, type shanghai and 123456 into the **User name** and **Password** boxes respectively, and click **Connect**. After the dial-up connection has been established, the employee in Shanghai can gain access to the Web server in the Intranet securely over L2TP.

VXLAN

Overview

Virtual extensible local area network (VXLAN) is a tunnel encapsulation technology for large layer 2 network expansion overe NOV3 that uses MAC-in-UDP encapsulation. VXLAN uses a 24-bit network segment ID, called VXLAN network identifier (VNI), to identify users. This VNI is

similar to a VLAN ID and supports a maximum of 16M [(2^24 - 1)/1024^2] VXLAN segments. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks to ensure uninterrupted services during VM migration, the IP address of the VM must remain unchanged.

VXLAN uses VTEP (VXLAN Tunnel Endpoint) equipment to encapsulate and decapsulate VXLAN packets, including ARP request packets and normal VXLAN data packets. VETP encapsulates the original Ethernet frame through VXLAN and sends it to the peer VTEP device. The peer VETP device decapsulates the VXLAN packet after receiving it, and then forwards it according to the original MAC. The VTEP can be a physical switch, a physical server, or other VXLAN-enabled Hardware equipment or software.

Creating a VXLAN Static Tunnel

To create a VXLAN static tunnel and enter the VXLAN tunnel configuration mode, in the global configuration mode, use the following command:

tunnel vxlan*name*

- *name* - Specified the name of the VXLAN static tunnel that will be created.

To delete the specified VXLAN static tunnel, in the global configuration mode, use the command**no tunnel vxlan***name*.

To configure the destination VETP IP address of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the following command:

destination*ipv4-address*

- *ipv4-address* - Specified the destination VETP IP address of the VXLAN static tunnel.

To delete the destination VETP IP address of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the command**no destination** .

To configure the VNI (VXLAN network identifier) of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the following command:

vni*id*

- *id* - Specified the network identifier of the VXLAN static tunnel. The value range is 1 to 16777215.

To delete the network identifier of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the command**no vni**.

To configure the egress interface of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the following command:

interface*interface-name*

- *interface-name* - Specified the egress interface of the VXLAN static tunnel.

To delete the egress interface of the VXLAN static tunnel, in the VXLAN tunnel configuration mode, use the command**no interface**.

To bind zone for the VXLAN static tunnel, in the tunnel interface configuration mode, use the following command:

zone{ *l2-zone* | *l3-zone*}

- *l2-zone* - Specified the name of the layer2 zone for the VXLAN tunnel.
- *l3-zone* - Specified the name of the layer3 zone for the VXLAN tunnel. This function is supported only by CloudEdge.

To delete the zone for the VXLAN static tunnel, in the tunnel interface configuration mode, use the command **no zone**{ *l2-zone* | *l3-zone*}.

Binding the VXLAN Tunnel to a Tunnel Interface

A well configured VXLAN tunnel needs to be bound to the tunnel interface so that it can work.

Note: To enable the VXLAN tunnel to work properly, the tunnel interface must be bound to the layer2 zone.

To bind the VXLAN tunnel to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel vxlan *vxlan-tunnel-name*

- *vxlan-tunnel-name* – Specifies the name of the well configured VXLAN tunnel which binds to the interface.

To cancel the binding of VXLAN tunnel to the tunnel interface, in the tunnel interface configuration mode, use the following command:

no tunnel vxlan *vxlan-tunnel-name*

Viewing VXLAN Configuration

In any mode, use the following command to view the configuration of the VXLAN static tunnel:
show tunnel vxlan*name*

Example:

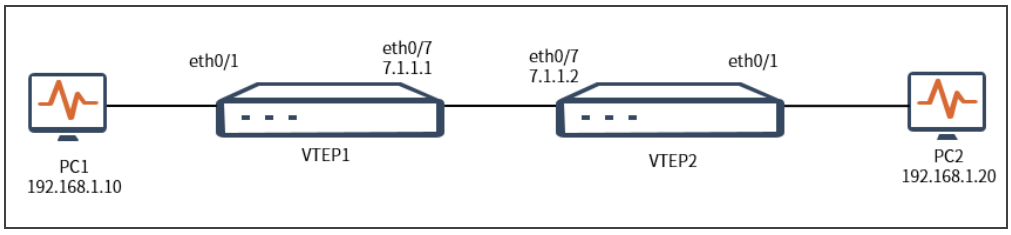
```
hostname#  show tunnel vxlan test
==================================
Name vni Interface Peer
(tunnel name, network identifier, egress interface, destination VETP IP address)
----------------------------------
test 3001 ethernet0/0 1.1.1.1
==================================
```

Example of Configuring VXLAN Static Unicast Tunnel

This example introduces how to configure VXLAN static unicast tunnel. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks, allowing a large number of tenant accesses to virtual networks.

In the topology below, PC1 and PC2 communicate through the VXLAN tunnel (VNI100).

Note: In the same tunnel, different VNIs cannot communicate with each other.



Configuration Steps

VTEP1 Configuratio

Step 1: Configure the interface.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
```

Step2: Configure VXLAN tunnel.

```
hostname(config)# tunnel vxlan tunnel1
hostname(config-tunnel-vxlan)# interface ethernet0/7
hostname(config-tunnel-vxlan)# destination 7.1.1.2
hostname(config-tunnel-vxlan)# vni 100
hostname(config-tunnel-vxlan)# exit
hostname(config)#
```

Step 3: Configure the tunnel interface and bind the Layer 2 security zone.

```
hostname(config)#  interface tunnel1
hostname(config-if-tun1)# zone l2-trust
hostname(config-if-tun1)#tunnel vxlan tunnel1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

VTEP2 Configuration

Step 1: Configure the interface.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
```

Step2: Configure VXLAN tunnel.

```
hostname(config)# tunnel vxlan tunnel1
hostname(config-tunnel-vxlan)# interface ethernet0/7
hostname(config-tunnel-vxlan)# destination 7.1.1.1
hostname(config-tunnel-vxlan)# vni 100
hostname(config-tunnel-vxlan)# exit
hostname(config)#
```

Step 3: Configure the tunnel interface and bind the Layer 2 security zone.

```
hostname(config)#  interface tunnel1
hostname(config-if-tun1)# zone l2-trust
hostname(config-if-tun1)#tunnel vxlan tunnel1
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 4: Configure the policy

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step5: Verify result

PC1 and PC2 can communicate with each other through the VXLAN tunnel successfully.

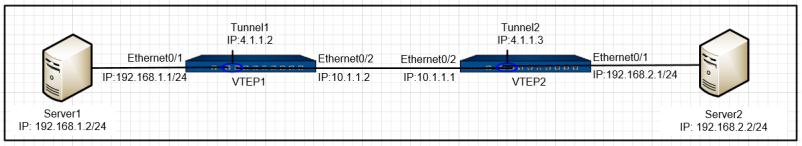
Examples of VXLAN

This section describes how to configure the VXLAN static tunnel:

Requirements for Networking

In an enterprise, there are two different departments with Server1 (IP: 192.168.1.2/24) and Server2 (IP: 192.168.2.2/24) respectively. There is no dedicated network to enable communication between these two servers, as they are located in different areas. The enterprise wants to deploy Hillstone device and establish a VXLAN static tunnel to implement that networks with different subnets can communicate with each other at Layer 3.

The topology is as follows:



- Requirement 1: The VXLAN static tunnel of VTEP1 is configured at Layer 3 zone and bound to the tunnel1 tunnel interface.
- Requirement 2: The VXLAN static tunnel of VTEP2 is configured at Layer 3 zone and bound to the tunnel2 tunnel interface.



Notes: Only CloudEdge supports to configure the VXLAN tunnel at Layer 3 zone.

Procedure of Requirement 1

Step 1: Configure the interface:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.1.1/24
hostname(config-if-eth0/1)# exit
```

Step 2: Configure the VXLAN tunnel:

```
hostname(config)# tunnel vxlan test1
hostname(config-tunnel-vxlan)# destination 10.1.1.1
hostname(config-tunnel-vxlan)# interface ethernet0/2
hostname(config-tunnel-vxlan)# vni 3001
hostname(config-tunnel-vxlan)# exit
```

Step 3: Configure the tunnel interface and bind the interface to Layer 3 zone:

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ip address 4.1.1.2/24
hostname(config-if-tun1)# tunnel vxlan test1
hostname(config-if-tun1)# exit
```

Step 4: Configure the route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.2.0/24 4.1.1.3
hostname(config-vrouter)# exit
```

Step 5: Configure the policy:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

Procedure of Requirement 2

Step 1: Configure the interface:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1/24
hostname(config-if-eth0/1)# exit
```

Step 2: Configure the VXLAN tunnel:

```
hostname(config)# tunnel vxlan test2
hostname(config-tunnel-vxlan)# destination 10.1.1.2
hostname(config-tunnel-vxlan)# interface ethernet0/2
hostname(config-tunnel-vxlan)# vni 3001
hostname(config-tunnel-vxlan)# exit
```

Step 3: Configure the tunnel interface and bind the interface to Layer 3 zone:

```
hostname(config)# interface tunnel2
hostname(config-if-tun2)# zone trust
hostname(config-if-tun2)# ip address 4.1.1.3/24
hostname(config-if-tun2)# tunnel vxlan test2
hostname(config-if-tun2)# exit
```

Step 4: Configure the route:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 192.168.1.0/24 4.1.1.2
hostname(config-vrouter)# exit
```

Step 5: Configure the policy:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
```

Chapter 10 Zero Trust Network Access (ZTNA)

Introduction

Compared with the traditional VPN access mode, which allows an authorized user to access any resources on the internal network, ZTNA (Zero Trust Network Access) starts with a default deny posture of zero trust on any entities, whether outside or inside the enterprise network perimeter. It grants controlled and least-privilege access to resources after assessment of user identity, device identity and other context-aware attributes, such as access time. It allows users to securely access private applications across clouds and data centers from any location and device.

Hillstone ZTNA solution supports management and control of user access based on dimensions including user identity, device identity and access time and grants access only to specific applications based on adaptive and granular policies. By persistently monitoring the state change of access endpoints, ZTNA solution flexibly adjusts the granted access range. ZTNA login process is as follows:

1. ZTNA user enters the server address, port number, user name and password on the client to request authentication and two-step verification, if any.
2. ZTNA server allocates private IP addresses to authenticated users and delivers the endpoint information collection script.
3. ZTNA client executes the script to collect endpoint information, such as OS version, firewall and anti-virus software installation information, IE security level, process running, etc. and reports to the ZTNA server.
4. ZTNA server parses endpoint information to obtain the endpoint tag and sends the user name appended with the endpoint tag to the authentication module.
5. Authentication module creates authenticated users, attends the endpoint tag and acquires user group information.

6. ZTNA server matches the user name, user group, endpoint tag and other conditions with ZTNA policies to determine application resources that the user can access.

7. ZTNA client receives the popped-up ZTNA portal, displaying the icons of application resources that the client is granted and is not granted access. The icons will be displayed with the application resource name and URL address.

ZTNA requires a license to work. The firewall provides 8 concurrent-users authorization by default (128 for X series and K9180). The upper limit for the number of concurrent online ZTNA users varies from hardware platforms. If you want to have a larger user number, consult your local agents to purchase new ZTNA license. For more information about the license, please refer to System Management > License Management.

ZTNA shares the Hillstone Secure Connect client with SSL VPN. To access ZTNA, please download and install the latest Hillstone Secure Connect client. Currently, ZTNA remote access solution supports access from Windows, macOS, Linux, iOS, Android, and ChineseOS endpoints. The firewall supports ZTNA access from Windows, macOS, Linux, iOS, Android and ChineseOS endpoints via corresponding clients. ZTNA intranet access solution supports access from Windows, macOS, Linux, and ChineseOS endpoints. The firewall supports ZTNA access from Windows, macOS, Linux and ChineseOS endpoints via corresponding clients. For information about client installation and usage on these endpoints, refer to:

- Hillstone Secure Connect Client for Windows
- Hillstone Secure Connect Client for macOS
- Hillstone Secure Connect Client for Linux
- Hillstone Secure Connect Client for iOS
- Hillstone Secure Connect Client for Android

Configuring ZTNA Service

This section describes the following configurations about ZTNA service:

- Configuring Endpoint Tag
- Managing Endpoint Item
- Configuring Application Resource/Application Resource Group
- Configuring ZTNA Policy
- Configuring Access Address Pool
- Configuring ZTNA Instance
- Configuring Two-Step Verification
- Configuring Single Packet Authorization (SPA)
- Managing Endpoint Tag Logs
- Other Configurations

Configuring Endpoint Tag

Endpoint tag identifies user endpoint information. The system attends an endpoint tag to a user based on endpoint information carried in user traffic. The user carrying a particular endpoint tag will be granted access to specific resources only. In this way, ZTNA implements check and control of user access privilege.

An endpoint tag is composed of one or multiple criteria sets, and a criteria set is composed of one or multiple conditions. Each endpoint tag contains at most 16 criteria sets and 16 conditions. The system supports a maximum of 1024 endpoint tags and up to 128 endpoint tags for each VSYS.

- The logical relationship between criteria sets is Or. When a user's endpoint tag matches any criteria set contained in an endpoint tag, the endpoint tag is considered to be matched.

- The logical relationship between the conditions contained in a criteria set is And. When a user's endpoint tag matches all conditions contained in a criteria set, the criteria set is considered to be matched.

This section describes the following endpoint tag configurations:

- Creating an Endpoint Tag
- Configuring a Criteria Set
- Configuring a Condition
- Configuring a Tip

Creating an Endpoint Tag

To configure an endpoint tag and enter the endpoint tag configuration mode, in the global configuration mode, use the following command:

endpoint-tag *tag-name* [*id*]

- *tag-name* - Specifies the endpoint tag name. The range is 1 to 95 characters. If the specified name already exists, you will enter the configuration mode of this endpoint tag directly. Each endpoint name should be unique in the VSYS it belongs to, while endpoint tags in different VSYS can share the same name.
- *id* - Specifies the endpoint tag ID. The value ranges from 1 to 128. If the ID is not specified, the system will automatically assign one. Each endpoint tag ID should be unique in the VSYS it belongs to, while endpoint tags in different VSYS can share the same ID.

To delete the specified endpoint tag, in the global configuration mode, use the following command:

no endpoint-tag *tag-name*

To change the name of an endpoint tag, in the endpoint tag configuration mode, use the following command:

name *tag-name*

- *tag-name* - Specifies the endpoint tag's new name. The length is 1 to 95 characters.

To add description to an endpoint tag, in the endpoint tag configuration mode, use the following command:

description *description*

- *description* - Specifies the description of the endpoint tag. The length is 1 to 255 characters.

To delete the description of an endpoint tag, in the endpoint tag configuration mode, use the following command:

no description

Configuring a Criteria Set

To configure a criteria set for the endpoint tag and enter the criteria set configuration mode, in the endpoint tag configuration mode, use the following command:

criteria-set [*id*]

- *id* - Specifies the criteria set ID. The value ranges from 1 to 16. If the ID is not specified, the system will automatically assign one. If the specified ID exists, you will enter the configuration mode of this criteria set directly.

To delete the specified criteria set, in the endpoint tag configuration mode, use the following command:

no criteria-set *id*

Configuring a Condition

The condition of an endpoint tag is composed of the following parts:

- OS type: only Windows is supported currently.
- Endpoint state: a string composed of "key name operator value".

To configure a condition for the endpoint tag, in the criteria set configuration mode, use the following command:

criteria [*id*]**os-type** {**windows** | **macOS** | **Linux** | **iOS** | **Android** | **ChineseOS**} **key** *key-name operator key-value*

- *id* - Specifies the condition ID. The value ranges from 1 to 16. If the ID is not specified, the system will automatically assign one.
- **os-type** {**windows** | **macOS** | **Linux** | **iOS** | **Android** | **ChineseOS**} - Specifies the OS type of the user endpoint.
- **key** *key-name operator key-value* - Specifies the endpoint item to be matched and the corresponding value. *key-name* is the name of the endpoint item. *operator* is the relational operator. *key-value* is the value of the endpoint item. For more information about the value, refer to Managing Endpoint Items.

To delete the specified condition of an endpoint tag, in the criteria set configuration mode, use the following command:

no criteria *id*

Configuring a Tip

For application resources that an end user is not allowed to access because the endpoint device does not match an endpoint tag, configure a tip to let the end user know the reason and update the endpoint device to obtain the access privilege. By default, the tip for each endpoint tag is "Access Failed Contact your administrator".

When a ZTNA policy binds multiple endpoint tags:

- If an end user matches any of the endpoint tags and is granted access to the application resource, no tip will be displayed for the corresponding application resource on the ZTNA portal.

- If an end user is not granted access to the application resource because no endpoint tag is matched, all tips will be displayed for the corresponding application resource on the ZTNA portal. If all bound endpoint tags are not configured with tips, the default tip will be displayed.

To configure a tip to be displayed when an end user is not granted access because an endpoint tag is not matched, in the endpoint tag configuration mode, use the following command:

tips *message*

- *message* - Specifies the tip to be displayed. The length is 1 to 511 characters. URL addresses are supported and will be displayed as hyperlinks on the ZTNA portal.

To delete the tip, in the endpoint tag configuration mode, use the following command:

no tips

Viewing Endpoint Tag Configuration Information

To view the configuration information of the specified endpoint tag and the ZTNA policy reference count, in any mode, use the following command:

show endpoint-tag name *tag-name*

- *tag-name* - Specifies the endpoint tag name.

To view the endpoint tag configuration information that matches the specified filter conditions and the ZTNA policy reference count and hit count of the endpoint tag, in any mode, use the following command.

show endpoint-tag filter {**name** *tag-name* | **description** *description*}

- **name** *tag-name* - Shows the endpoint tag configuration information that matches the specified endpoint tag name and the ZTNA policy reference count and hit count of the endpoint tag.
- **description** *description* - Shows the endpoint tag configuration information that matches the specified description and the ZTNA policy reference count and hit count of the endpoint tag.

To view the configuration information, the ZTNA policy reference count and hit count and descriptions of all endpoint tags, in any mode, use the following command:

show endpoint-tag

Managing Endpoint Items

Endpoint item management implements endpoint information collection configuration, script generation and delivery and persistent endpoint state monitoring. After a client logs in, the system will continuously monitor the endpoint state and update the attended endpoint tag and the granted resource access range, no matter whether the client accesses resources. The monitoring process is as follows:

1. The client periodically collects endpoint information based on the collection script and reports to the ZTNA server. By default, the client collects and reports collected endpoint information at the interval of 60 minutes. The interval can be modified as required via the **ztna-endpoint-information-monitor** command.
2. ZTNA server parses the received endpoint information and re-acquires the endpoint tag if the endpoint state changes. Then the endpoint tag attended to the authorized user will be updated, the ZTNA policy is re-matched and the resource access range granted to the user is updated as well. For existing sessions of this user, the system will process them based on the configuration of the **session-rematch** command.

Endpoint items include the predefined and custom ones. Configuration of predefined endpoint items enables the ZTNA server to acquire more endpoint information for granular application access control.

The system supports endpoint item management of the following operating systems:

- Windows endpoint item management
- macOS endpoint item management
- Linux endpoint item management
- iOS endpoint item management

- Android endpoint item management
- ChineseOS endpoint item management

Windows Endpoint Item Management

The following table shows the types of predefined Windows endpoint items supported by the system.

Predefined Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the Windows endpoint.	is、is-not	windows-7/8.1/10/11；windows-server-2008-R2/2012/2012-R2/2016/2019/2022
anti-virus	Checks whether anti-virus software is installed, enabled and updated in the Windows endpoint.	is、is-not	installed、enabled、updated
firewall	Checks whether firewall is installed and enabled in the Windows end-	is、is-not	installed、enabled

Predefined Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	point.		
anti-spyware	Checks whether anti-spy soft-ware is installed, enabled and updated in the Windows end-point.	is、is-not	installed、enabled、updated
windows-update	Checks whether Windows update is enabled in the Windows end-point.	is、is-not	enabled
ie-version	Checks the IE version of the Windows end-point.	=、!=、>、<、>=、<=	IE7 ~ IE11
ie-security-level	Collects the IE security level of the Windows endpoint.	=、!=、>、<、>=、<=	custom-define、low、medium-low、medium、medium-high、high

The following table shows the types of custom Windows endpoint items supported by the system.

Custom Windows Endpoint Items			
Endpoint Item Name (keyname)	**Description**	**Operator**	**Value**
process	Checks whether the specified process is running in the Windows endpoint.	exist、not-exist	Alias of the specified process
service-installed	Checks whether the specified service is installed in the Windows endpoint.	exist、not-exist	Alias of the specified service
service-running	Checks whether the specified service is running in the Windows endpoint.	exist、not-exist	Alias of the specified service
registry-key	Checks whether the specified registry key exists in the Windows endpoint.	exist、not-exist	Alias of the specified registry key
file	Checks whether	exist、not-	Alias of the spe-

Custom Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	the specified file exists in the Windows endpoint.	exist	cified file
hotfix	Checks whether the specified Windows hot fix is installed in the Windows endpoint.	exist、not-exist	Alias of the specified hot fix

Configuring a Custom Windows Endpoint Item

To configure custom Windows endpoint items, you need to enter the ztna-endpoint-information-windows-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-windows-profile

Defining Registry Key as Endpoint Item

You can configure the firewall to check whether the specified registry key exists in the Windows endpoint.

To define the registry key item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

registry-key alias *alias-name* **value** *registry-key-name*

- **alias** *alias-name* - Specifies the registry key's alias. The length is 1 to 31 characters.
- **value** *registry-key-name* - Specifies the actual name of registry key. The length is 1 to 255 characters.

Repeat this command to add up to 5 registry keys as endpoint items.

To delete the endpoint item configuration of the specified registry key, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no registry-key alias *alias-name*

Defining Running Process as Endpoint Item

You can configure the firewall to check whether the specified process is running in the Windows endpoint.

To define the process item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

process alias *alias-name* **value** *process-name*

- **alias** *alias-name* - Specifies the process's alias. The length is 1 to 31 characters.
- **value** *process-name* - Specifies the actual name of the process. The length is 1 to 255 characters.

Repeat this command to add up to 5 running processes as endpoint items.

To delete the endpoint item configuration of the specified process, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no process alias *alias-name*

Defining Running Service as Endpoint Item

You can configure the firewall to check whether the specified service is running in the Windows endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

service-running alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 running services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining Installed Service as Endpoint Item

You can configure the firewall to check whether the specified service is installed in the Windows endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

service-installed alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 installed services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no service-installed alias *alias-name*

Defining File as Endpoint Item

You can configure the firewall to check whether the specified file exists in the Windows endpoint.

To define the file item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

file alias *alias-name* **value** *file-name*

- **alias** *alias-name* - Specifies the file's alias. The length is 1 to 31 characters.
- **value** *file-name* - Specifies the file's absolute path. The length is 1 to 255 characters.

Repeat this command to add up to 5 files as endpoint items.

To delete the endpoint item configuration of the specified file, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no file alias *alias-name*

Defining Hot Fix as Endpoint Item

You can configure the firewall to check whether the specified hot fix is installed in the Windows endpoint.

To define the hot patch item that needs to be checked, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

hotfix alias *alias-name* **value** *hotfix-name*

- **alias** *alias-name* - Specifies the hot fix's alias. The length is 1 to 31 characters.
- **value** *hotfix-name* - Specifies the actual name of the hot fix. The length is 1 to 255 characters.

Repeat this command to add up to 5 hot fixes as endpoint items.

To delete the endpoint item configuration of the specified hot fix, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no hotfix alias *alias-name*

Viewing Windows Endpoint Item Configuration Information

To view all predefined and custom Windows endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-windows-profile

To view the configuration information of the specified Windows endpoint item, in any mode, use the following command:

show ztna-endpoint-information-windows-profile *key-name*

- *key-name* - Specifies the Windows endpoint item name. Both the predefined and the custom ones are supported.

macOS Endpoint Item Management

The following table shows the types of predefined macOS endpoint items supported by the system.

Predefined macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the macOS endpoint.	is、is-not	10.13/10.14/10.15/11/12/13
fileVault	Checks whether the FileVault function is enabled in the macOS	is、is-not	enabled

Predefined macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	endpoint.		

The following table shows the types of custom macOS endpoint items supported by the system.

Custom macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
ad-domain	Checks the AD domain name of the macOS endpoint.	is、is-not	Alias of the specified AD domain name
process	Checks whether the specified process is running in the macOS endpoint.	exist、not-exist	Alias of the specified process
service-installed	Checks whether the specified service is installed in the macOS endpoint.	exist、not-exist	Alias of the specified service
service-running	Checks whether the specified ser-	exist、not-exist	Alias of the specified service

Custom macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	vice is running in the macOS end-point.		
file	Checks whether the specified file exists in the macOS endpoint.	exist、not-exist	Alias of the spe-cified file

Configuring a Custom macOS Endpoint Item

To configure custom macOS endpoint items, you need to enter the ztna-endpoint-information-macos-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-macos-profile

Defining AD Domain Name as Endpoint Item

You can configure the firewall to check whether the macOS endpoint is using the specified AD domain name.

To define the AD domain name item that needs to be checked, in the ztna-endpoint-information-macOS-profile configuration mode, use the following command:

ad-domain alias *alias-name* **value** *domain-name*

- **alias** *alias-name* - Specifies the AD domain name's alias. The length is 1 to 31 characters.
- **value** *domain-name* - Specifies the actual name of the AD domain name. The length is 1 to 255 characters.

Only one AD domain name can be defined as the endpoint item.

To delete the endpoint item configuration of the specified AD domain name, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

no registry-key alias*alias-name*

Defining Running Process as Endpoint Item

You can configure the firewall to check whether the specified process is running in the macOS endpoint.

To define the process item that needs to be checked, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

process alias *alias-name* **value** *process-name*

- **alias** *alias-name* - Specifies the process's alias. The length is 1 to 31 characters.
- **value** *process-name* - Specifies the actual name of the process. The length is 1 to 255 characters.

Repeat this command to add up to 5 running processes as endpoint items.

To delete the endpoint item configuration of the specified process, in the ztna-endpoint-information-windows-profile configuration mode, use the following command:

no process alias*alias-name*

Defining Running Service as Endpoint Item

You can configure the firewall to check whether the specified service is running in the macOS endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

service-running alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 running services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining Installed Service as Endpoint Item

You can configure the firewall to check whether the specified service is installed in the macOS endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

service-installed alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 installed services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

no service-installed alias *alias-name*

Defining File as Endpoint Item

You can configure the firewall to check whether the specified file exists in the macOS endpoint.

To define the file item that needs to be checked, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

file alias *alias-name* **value** *file-name*

- **alias** *alias-name* - Specifies the file's alias. The length is 1 to 31 characters.
- **value** *file-name* - Specifies the file's absolute path. The length is 1 to 255 characters.

Repeat this command to add up to 5 files as endpoint items.

To delete the endpoint item configuration of the specified file, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

no file alias *alias-name*

Viewing macOS Endpoint Item Configuration Information

To view all predefined and custom macOS endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-macos-profile

To view the configuration information of the specified macOS endpoint item, in any mode, use the following command:

show ztna-endpoint-information-macos-profile *key-name*

- *key-name* - Specifies the macOS endpoint item name. Both the predefined and the custom ones are supported.

Linux Endpoint Item Management

The following table shows the types of predefined Linux endpoint items supported by the system.

Predefined Linux Endpoint Items			
Endpoint Item Name (keyname)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the Linux endpoint.	is、isnot	CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5; Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04; Ubuntu Kylin 18.04/20.04

The following table shows the types of custom Linux endpoint items supported by the system.

Custom Linux Endpoint Items			
Endpoint Item Name (keyname)	**Description**	**Operator**	**Value**
process	Checks whether the specified process is running in the Linux endpoint.	exist、notexist	Alias of the specified process
serviceinstalled	Checks whether the specified service is installed in the Linux endpoint.	exist、notexist	Alias of the specified service

Custom Linux Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
service-running	Checks whether the specified service is running in the Linux endpoint.	exist、not-exist	Alias of the specified service
file	Checks whether the specified file exists in the Linux endpoint.	exist、not-exist	Alias of the specified file

Configuring a Custom Linux Endpoint Item

To configure custom Linux endpoint items, you need to enter the ztna-endpoint-information-macos-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-linux-profile

Defining Running Process as Endpoint Item

You can configure the firewall to check whether the specified process is running in the Linux endpoint.

To define the process item that needs to be checked, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

process alias *alias-name* **value** *process-name*

- **alias** *alias-name* - Specifies the process's alias. The length is 1 to 31 characters.
- **value** *process-name* - Specifies the actual name of the process. The length is 1 to 255 characters.

Repeat this command to add up to 5 running processes as endpoint items.

To delete the endpoint item configuration of the specified process, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

no process alias *alias-name*

Defining Running Service as Endpoint Item

You can configure the firewall to check whether the specified service is running in the Linux endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

service-running alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 running services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining Installed Service as Endpoint Item

You can configure the firewall to check whether the specified service is installed in the Linux endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

service-installed alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 installed services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

no service-installed alias *alias-name*

Defining File as Endpoint Item

You can configure the firewall to check whether the specified file exists in the Linux endpoint.

To define the file item that needs to be checked, in the ztna-endpoint-information-macos-profile configuration mode, use the following command:

file alias *alias-name* **value** *file-name*

- **alias** *alias-name* - Specifies the file's alias. The length is 1 to 31 characters.
- **value** *file-name* - Specifies the file's absolute path. The length is 1 to 255 characters.

Repeat this command to add up to 5 files as endpoint items.

To delete the endpoint item configuration of the specified file, in the ztna-endpoint-information-linux-profile configuration mode, use the following command:

no file alias *alias-name*

Viewing Linux Endpoint Item Configuration Information

To view all predefined and custom Linux endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-linux-profile

To view the configuration information of the specified Linux endpoint item, in any mode, use the following command:

show ztna-endpoint-information-linux-profile *key-name*

- *key-name* - Specifies the Linux endpoint item name. Both the predefined and the custom ones are supported.

iOS Endpoint Item Management

The following table shows the types of predefined iOS endpoint items supported by the system.

Predefined iOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the iOS endpoint.	is、is-not	iOS 12/13/14/15/16

The following table shows the types of custom iOS endpoint items supported by the system.

Custom iOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
device-model	Checks the device model of the iOS endpoint.	is、is-not	Alias of the specified device model
wifi-ssid	Checks the connected WiFi SSID of the iOS end-	is、is-not	Alias of the specified WiFi SSID

Custom iOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	point.		
client-version	Checks the ZTNA client version of the iOS endpoint.	is、 is-not	Alias of the specified ZTNA client version

Configuring a Custom iOS Endpoint Item

To configure custom iOS endpoint items, you need to enter the ztna-endpoint-information-ios-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-ios-profile

Defining Device Model as Endpoint Item

You can configure the firewall to check the device model of the iOS endpoint.

To define the device model that needs to be checked, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

device-model alias *alias-name* **value** *device-model-number*

- **alias** *alias-name* - Specifies the iOS device model number's alias. The length is 1 to 31 characters.
- **value** *device-model-number* - Specifies the iOS device model number. The length is 1 to 255 characters.

Repeat this command to add up to 5 iOS device model numbers as endpoint items.

To delete the endpoint item configuration of the specified device model number, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

no device-model alias *alias-name*

Defining WiFi SSID as Endpoint Item

You can configure the firewall to check the WiFi SSID that the iOS endpoint connects.

To define the WiFi SSID item that needs to be checked, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

wifi-ssid alias *alias-name* **value** *wifi-ssid*

- **alias** *alias-name* - Specifies the WiFi SSID's alias. The length is 1 to 31 characters.
- **value** *wifi-ssid* - Specifies the WiFi SSID. The length is 1 to 255 characters.

Repeat this command to add up to 5 WiFi SSIDs as endpoint items.

To delete the endpoint item configuration of the specified WiFi SSID, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining ZTNA Client Version as Endpoint Item

You can configure the firewall to check the ZTNA client version of the iOS endpoint.

To define the ZTNA client version item that needs to be checked, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

client-version *alias-name* **value** *client-version*

- **client-version** *alias-name* - Specifies the ZTNA client version's alias. The length is 1 to 31 characters.
- **value** *client-version* - Specifies the ZTNA client version. The length is 1 to 255 characters.

Repeat this command to add up to 5 ZTNA client versions as endpoint items.

To delete the endpoint item configuration of the specified ZTNA client version, in the ztna-endpoint-information-ios-profile configuration mode, use the following command:

no client-version *alias-name*

Viewing iOS Endpoint Item Configuration Information

To view all predefined and custom iOS endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-ios-profile

To view the configuration information of the specified iOS endpoint item, in any mode, use the following command:

show ztna-endpoint-information-ios-profile *key-name*

- *key-name* - Specifies the iOS endpoint item name. Both the predefined and the custom ones are supported.

Android Endpoint Item Management

The following table shows the types of predefined Android endpoint items supported by the system.

Predefined Android Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the Android endpoint.	is、is-not	Android 8/9/10/11/12/13

The following table shows the types of custom Android endpoint items supported by the system.

Custom Android Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
device-model	Checks the device	is、is-not	Alias of the spe-

Custom Android Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	model of the Android endpoint.		cified device model
wifi-ssid	Checks the connected WiFi SSID of the Android endpoint.	is、 is-not	Alias of the specified WiFi SSID
client-version	Checks the ZTNA client version of the Android endpoint.	is、 is-not	Alias of the specified ZTNA client version

Configuring a Custom Android Endpoint Item

To configure custom Android endpoint items, you need to enter the ztna-endpoint-information-android-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-android-profile

Defining Device Model as Endpoint Item

You can configure the firewall to check the device model of the Android endpoint.

To define the device model that needs to be checked, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

device-model alias *alias-name* **value** *device-model-number*

- **alias***alias-name* - Specifies the Android device model number's alias. The length is 1 to 31 characters.
- **value** *device-model-number* - Specifies the Android device model number. The length is 1 to 255 characters.

Repeat this command to add up to 5 Android device model numbers as endpoint items.

To delete the endpoint item configuration of the specified device model number, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

no device-model alias *alias-name*

Defining WiFi SSID as Endpoint Item

You can configure the firewall to check the WiFi SSID that the Android endpoint connects.

To define the WiFi SSID item that needs to be checked, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

wifi-ssid alias *alias-name* **value** *wifi-ssid*

- **alias***alias-name* - Specifies the WiFi SSID's alias. The length is 1 to 31 characters.
- **value** *wifi-ssid* - Specifies the WiFi SSID. The length is 1 to 255 characters.

Repeat this command to add up to 5 WiFi SSIDs as endpoint items.

To delete the endpoint item configuration of the specified WiFi SSID, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining ZTNA Client Version as Endpoint Item

You can configure the firewall to check the ZTNA client version of the Android endpoint.

To define the ZTNA client version item that needs to be checked, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

client-version *alias-name* **value** *client-version*

- **client-version** *alias-name* - Specifies the ZTNA client version's alias. The length is 1 to 31 characters.
- **value** *client-version* - Specifies the ZTNA client version. The length is 1 to 255 characters.

Repeat this command to add up to 5 ZTNA client versions as endpoint items.

To delete the endpoint item configuration of the specified ZTNA client version, in the ztna-endpoint-information-android-profile configuration mode, use the following command:

no client-version *alias-name*

Viewing Android Endpoint Item Configuration Information

To view all predefined and custom Android endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-android-profile

To view the configuration information of the specified Android endpoint item, in any mode, use the following command:

show ztna-endpoint-information-android-profile *key-name*

- *key-name* - Specifies the Android endpoint item name. Both the predefined and the custom ones are supported.

ChineseOS Endpoint Item Management

The following table shows the types of predefined ChineseOS endpoint items supported by the system.

Predefined ChineseOS Endpoint Items			
Endpoint Item Name	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the ChineseOS end-	is, is-not	KylinV10 ; UOS20

Predefined ChineseOS Endpoint Items			
Endpoint Item Name	Description	Operator	Value
	point.		

The following table shows the types of custom ChineseOS endpoint items supported by the system.

Custom ChineseOS Endpoint Items			
Endpoint Item Name	Description	Operator	Value
process	Checks whether the specified process is running in the ChineseOS endpoint.	exist, not-exist	Alias of the specified process
service-running	Checks whether the specified service is running in the ChineseOS endpoint.	exist, not-exist	Alias of the specified service
service-installed	Checks whether the specified service is installed in the ChineseOS endpoint.	exist, not-exist	Alias of the specified service
file	Checks whether the specified file	exist, not-exist	Alias of the specified file

Custom ChineseOS Endpoint Items			
Endpoint Item Name	Description	Operator	Value
	exists in the ChineseOS end-point.		

Configuring a Custom ChineseOS Endpoint Item

To configure custom ChineseOS endpoint items, you need to enter the ztna-endpoint-information-chineseos-profile configuration mode by using the following command in the global configuration mode:

ztna-endpoint-information-chineseos-profile

Defining Running Process as Endpoint Item

You can configure the firewall to check whether the specified process is running in the ChineseOS endpoint.

To define the process item that needs to be checked, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

process alias *alias-name* **value** *process-name*

- **alias** *alias-name* - Specifies the process's alias. The length is 1 to 31 characters.
- **value** *process-name* - Specifies the actual name of the process. The length is 1 to 255 characters.

Repeat this command to add up to 5 running processes as endpoint items.

To delete the endpoint item configuration of the specified process, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

no process alias *alias-name*

Defining Running Service as Endpoint Item

You can configure the firewall to check whether the specified service is running in the ChineseOS endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

service-running alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 running services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

no service-running alias *alias-name*

Defining Installed Service as Endpoint Item

You can configure the firewall to check whether the specified service is installed in the ChineseOS endpoint.

To define the service item that needs to be checked, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

service-installed alias *alias-name* **value** *service-name*

- **alias** *alias-name* - Specifies the service's alias. The length is 1 to 31 characters.
- **value** *service-name* - Specifies the actual name of the service. The length is 1 to 255 characters.

Repeat this command to add up to 5 installed services as endpoint items.

To delete the endpoint item configuration of the specified service, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

no service-installed alias *alias-name*

Defining File as Endpoint Item

You can configure the firewall to check whether the specified file exists in the ChineseOS endpoint.

To define the file item that needs to be checked, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

file alias *alias-name* **value** *file-name*

- **alias** *alias-name* - Specifies the file's alias. The length is 1 to 31 characters.
- **value** *file-name* - Specifies the file's absolute path. The length is 1 to 255 characters.

Repeat this command to add up to 5 files as endpoint items.

To delete the endpoint item configuration of the specified file, in the ztna-endpoint-information-chineseos-profile configuration mode, use the following command:

no file alias *alias-name*

Viewing ChineseOS Endpoint Item Configuration Information

To view all predefined and custom ChineseOS endpoint items the system supports, in any mode, use the following command:

show ztna-endpoint-information-chineseos-profile

To view the configuration information of the specified ChineseOS endpoint item, in any mode, use the following command:

show ztna-endpoint-information-chineseos-profile *key-name*

- *key-name* - Specifies the ChineseOS endpoint item name. Both the predefined and the custom ones are supported.

Example:

```
hostname(config)# show ztna-endpoint-information-chineseos-profile
Total ZTNA endpoint information key: 5
=====================================================
Key name ID Data type Support custom
-----------------------------------------------------
file 10 string Yes
os-version 1 string No
process 20 string Yes
service-installed 40 string Yes
service-running 30 string Yes
=====================================================
```

Configuring the Endpoint Monitoring Period

After a user logs in successfully, the system will continuously monitor the endpoint state and adaptively adjust the resource access range granted to the user. The system supports configuration of the endpoint monitoring period. If endpoint information collection fails within the specified monitoring period and the number of consecutive failures reaches the specified threshold, the system will clear the user's endpoint tag and rematch ZTNA policies.

To configure the endpoint monitoring period, in the global configuration mode, use the following command:

ztna-endpoint-information-monitor { [**interval***interval-value*] [**threshold** *threshold-value*] }

- **interval** *interval-value* - Specifies the report period. The value ranges from 60 to 65535 minutes. The default value is 60.
- **threshold** *threshold-value* - Specifies the threshold for the number of consecutive failures of endpoint information report. The value ranges from 2 to 65535. The default value is 2.

Viewing Endpoint Monitoring Configuration Information

To view endpoint monitoring configuration information, in any mode, use the following command:

show ztna-endpoint-information-monitor

Viewing Endpoint Information Database

To view endpoint information database, in any mode, use the following command:

show ztna-endpoint-information-database

Execution of this command will display the database version, supported endpoint OS and operators.

Configuring Application Resource/Application Resource Group

Application resource refers to the applications, contents, services, etc. that users want to access. You need to configure the address, protocol, port number and others to define an application resource entry. Each application resource can contain up to 16 application resource entries. Application resource group is a group of up to 16 application resources. The system supports a maximum of 256 application resources and 64 application resource groups.

The system supports the following ways to define an application resource entry:

- Based on IP address, protocol and port number
- Based on IP range, protocol and port number
- Based on domain name, protocol and port number

Creating an Application Resource

To create an application resource and enter the application resource configuration mode, in the global configuration mode, use the following command:

application-resource *application-resource-name* [**id** *id*]

- *application-resource-name* - Specifies the application resource's name, which is case-insensitive. The length is 1 to 95 characters. If the name already exists, you will enter the configuration mode of this application resource directly.
- **id** *id* - Specifies the application resource ID. The value ranges from 1 to 256. If the ID is not specified, the system will automatically assign one.

To delete the specified application resource, in the global configuration mode, use the following command:

no application-resource *application-resource-name*

Configuring an IP-Based Application Resource Entry

To configure an application resource entry based on the IP address, in the application resource configuration mode, use the following command:

ip *ip-address* **protocol** {**tcp** | **udp**} **port** *port-number*[*maximum-port-number*] [**timeout** *timeout-value* | **timeoutday** *timeout-value*]

- **ip** *ip-address* - Specifies the application resource's IP address. IPv4/IPv6 address, IPv4 address/netmask and IPv6 address/prefix length are supported. The value range for the prefix length of an IPv6 address is 0 to 128.
- **protocol** {**tcp** | **udp**} - Specifies the transmission-layer protocol type of the application resource, TCP or UDP.
- **port** *port-number*[*maximum-port-number*] - Specifies the port number or port range of the application resource. The value ranges from 1 to 65535.
  - If you specify a port number, you can specify only *port-number* .
  - If you specify a port range, the minimum port number *port-number* cannot be greater than the maximum port number *maximum-port-number*.

  Note: If the minimum port number *port-number* and the maximum port number *maximum-port-number* are the same, it indicates that a port number is specified.
- **timeout** *timeout-value* | **timeoutday** *timeout-value* - Specifies the timeout value of ZTNA sessions created when an application resource is accessed. When the ZTNA session times out, it will be ended. **timeout** *timeout-value* specifies the timeout value in seconds, which ranges from 1 to 65535. **timeoutday** *timeout-value* specifies the timeout value in days, which ranges from 1 to 1000. If the **timeout/timeoutday** parameter is not specified, the default lifetime of TCP type ZTNA sessions is 1800s; the default lifetime of UDP type ZTNA sessions is 60s.



Notes: When only the **timeout/timeoutday** parameter configuration of a new IP-based application resource entry is different with an existing one, the existing one will be overwritten.

To delete an IP-based application resource entry, in the application resource configuration mode, use the following command:

no ip*ip-address***protocol** {**tcp** | **udp**} **port***port-number* [*maximum-port-number*]

Configuring an IP Range-Based Application Resource Entry

To configure an application resource entry based on the IP range, in the application resource configuration mode, use the following command:

range *min-ip max-ip***protocol** {**tcp** | **udp**} **port***port-number*[*maximum-port-number*] [**timeout***timeout-value* | **timeoutday***timeout-value*]

- **range** *min-ip max-ip* - Specifies the application resource's IP range. *min-ip* and *max-ip* specify the start IP address and end IP address respectively. A maximum of 65535 IP addresses are allowed in an IP range.
- **protocol** {**tcp** | **udp**} - Specifies the transmission-layer protocol type of the application resource, TCP or UDP.
- **port***port-number*[*maximum-port-number*] - Specifies the port number or port range of the application resource. The value ranges from 1 to 65535.
    - If you specify a port number, you can specify only *port-number* .
    - If you specify a port range, the minimum port number *port-number* cannot be greater than the maximum port number *maximum-port-number*.

Note: If the minimum port number *port-number* and the maximum port number *maximum-port-number* are the same, it indicates that a port number is specified.

- **timeout** *timeout-value* | **timeoutday** *timeout-value* - Specifies the timeout value of ZTNA sessions created when an application resource is accessed. When the ZTNA session times out, it will be ended. **timeout** *timeout-value* specifies the timeout value in seconds, which ranges from 1 to 65535. **timeoutday** *timeout-value* specifies the timeout value in days, which ranges from 1 to 1000. If the **timeout/timeoutday** parameter is not specified, the default lifetime of TCP type ZTNA sessions is 1800s; the default lifetime of UDP type ZTNA sessions is 60s.



Notes: When only the **timeout/timeoutday** parameter configuration of a new IP range-based application resource entry is different with an existing one, the existing one will be overwritten.

To delete an IP range-based application resource entry, in the application resource configuration mode, use the following command:

no range*min-ip max-ip* **protocol** {**tcp** | **udp**} **port***port-number*[*maximum-port-number*]

Configuring a Domain Name-Based Application Resource Entry

To configure an application resource entry based on the domain name, in the application resource configuration mode, use the following command:

domain*string***protocol** {**http** | **https**} **port***port-number*[*maximum-port-number*] [**timeout***timeout-value* | **timeoutday***timeout-value*]

- **domain** *string*- Specifies the domain name of the application resource. The length is 1 to 255 characters, and the length between two periods (.) cannot exceed 63 characters. You can set an exact domain name or a wildcard domain name beginning with "*".
- **protocol** {**http** | **https**} - Specifies the application-layer protocol type of the application resource, HTTP or HTTPS.
- **port***port-number*[*maximum-port-number*] - Specifies the port number or port range of the application resource. The value ranges from 1 to 65535.

- If you specify a port number, you can specify only *port-number* .
- If you specify a port range, the minimum port number *port-number* cannot be greater than the maximum port number *maximum-port-number*.

Note: If the minimum port number *port-number* and the maximum port number *maximum-port-number* are the same, it indicates that a port number is specified.

- **timeout** *timeout-value* | **timeoutday** *timeout-value* - Specifies the timeout value of ZTNA sessions created when an application resource is accessed. When the ZTNA session times out, it will be ended. **timeout***timeout-value* specifies the timeout value in seconds, which ranges from 1 to 65535. **timeoutday** *timeout-value* specifies the timeout value in days, which ranges from 1 to 1000. If the **timeout/timeoutday** parameter is not specified, the default lifetime of TCP type ZTNA sessions is 1800s; the default lifetime of UDP type ZTNA sessions is 60s.



Notes: When only the **timeout/timeoutday** parameter configuration of a new domain name-based application resource entry is different with an existing one, the existing one will be overwritten.

To delete a domain name-based application resource entry, in the application resource configuration mode, use the following command:

no domain*string***protocol** {**http** | **https**} **port***port-number*[*maximum-port-number*]

Configuring Hyperlink for an Application Resource

On the ZTNA portal displayed after a user logs in, the user can copy the hyperlink to access an application resource in a browser if the application resource is configured with an hyperlink; or, the user can directly click the application resource icon to access it (make sure the link work). An application resource without a hyperlink configured will not be displayed on the ZTNA portal.

The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing

any application resources, the portal page displays a message indicating that no Web resources are available to the user. After the portal page is closed, the user can click the "Application Resource List" option in the Secure Connect client menu to display the latest ZTNA portal page.

To configure a hyperlink, in the application resource configuration mode, use the following command:

hyperlink *hyperlink*

- *hyperlink* - Specifies the hyperlink. The length is 1 to 2047 characters. If the specified hyperlink does not contain a protocol type, the default HTTP protocol will be used.

To delete the hyperlink, in the application resource configuration mode, use the following command:

no hyperlink

Configuring Description for an Application Resource

To add description to an application resource, in the application resource configuration mode, use the following command:

description *description*

- *description* - Specifies the application resource description. The length is 1 to 255 characters. When the application resource is already configured with description, it will be overwritten by the new description.

To delete the application resource description, in the application resource configuration mode, use the following command:

no description

Renaming an Application Resource

To change the application resource name, in the application resource configuration mode, use the following command:

rename *application-resource-name*

- *application-resource-name* - Specifies the new name of the application resource, which is case-insensitive. The length is 1 to 95 characters.

Or, you can use the following command in the global configuration mode to rename an application resource:

rename application-resource *original-application-resource-name new-application-resource-name*

- *original-application-resource-name* - Specifies the original name of the application resource.
- *new-application-resource-name* - Specifies the new name of the application resource, which is case-insensitive. The length is 1 to 95 characters.

Viewing Application Resource Configuration Information

To view the configuration information of the specified application resource, in any mode, use the following command:

show application-resource {**name** *application-resource-name* | **id** *id*}

- **name** *application-resource-name* | **id** *id* - Specifies the application resource name or ID.

To view the configuration information of all application resources, in any mode, use the following command:

show application-resource

Viewing Application Resource Configuration Information According to Filter Conditions

To view application resource configuration information that matches the specified filter conditions, in any mode, use the following command:

show application-resource filter { [**name** *application-resource-name*] [**ip** *ip-address*] [**domain** *string*] [**protocol** {**udp** | **tcp** | **http** | **https**}] [**port** *port-number*] [**description** *description*] [**hyperlink** *hyperlink*] }

- **name** *application-resource-name* - Shows the application resource configuration information matching the specified application resource name. Partial match and full match are supported.
- **ip** *ip-address* - Shows the application resource configuration information matching the specified IP address. IPv4/IPv6 address, IPv4 address/netmask and IPv6 address/prefix length are supported.
- **domain** *string* - Shows application resource configuration information matching the specified domain name. Partial match and full match are supported.
- **protocol** {**udp** | **tcp** | **http** | **https**} - Shows the application resource configuration information matching the specified protocol. When you filter for application resources defined based on IP address, the supported protocol types are UDP and TCP; When you you filter for application resources defined based on domain name, the supported protocol types are HTTP and HTTPS.
- **port** *port-number* - Shows the application resource configuration information matching the specified port number.
- **description** *description* - Shows the application resource configuration information matching the specified description. Partial match and full match are supported.
- **hyperlink** *hyperlink* - Shows the application resource configuration information matching the specified hyperlink. Partial match and full match are supported.

Viewing Reference Information of an Application Resource

User traffic hitting a ZTNA policy will be or not be granted access to the application resource referenced by the policy.

To view the reference information of the specified application resource, in any mode, use the following command:

show reference application-resource *application-resource-name*

- *application-resource-name* - Specifies the application resource name.

Creating an Application Resource Group

An application resource group is composed of one or multiple application resource members. To create an application resource group and enter the application resource group configuration mode , in the global configuration mode, use the following command:

application-resource-group *application-resource-group-name* [**id** *id*]

- *application-resource-group-name* - Specifies the application resource group name, which is case-insensitive. The length is 1 to 95 characters. If the specified name exists, you will enter the configuration mode of this application resource group.
- **id** *id* - Specifies the application resource group ID. The value ranges from 1 to 64. If the ID is not specified, the system will automatically assign one.

To delete the specified application resource group, in the global configuration mode, use the following command:

no application-resource-group *group-name*

Adding Members to an Application Resource Group

A maximum of 16 application resources can be added to a group.

To configure a member for the specified application resource group, in the application resource group configuration mode, use the following command:

application-resource *application-resource-name*

- *application-resource-name* - Specifies the name of an existing application resource.

To delete the specified member from the application resource group, in the application resource group configuration mode, use the following command:

no application-resource *application-resource-name*

Configuring Description for an Application Resource Group

To configure description for an application resource group, in the application resource group configuration mode, use the following command:

description *description*

- *description* - Specifies the application resource group description. The length is 1 to 255 characters. When the application resource group is already configured with description, it will be overwritten by the new description.

To delete the application resource group description, in the application resource group configuration mode, use the following command:

no description

Renaming an Application Resource Group

To change the application resource group name, in the application resource group configuration mode, use the following command:

rename *application-resource-group-name*

- *application-resource-group-name* - Specifies the new name of the application resource group, which is case-insensitive. The length is 1 to 95 characters.

Or, you can use the following command in the global configuration mode to rename an application resource group:

rename application-resource-group *original-application-resource-group-name new-application-resource-group-name*

- *original-application-resource-group-name* - Specifies the original name of the application resource group.
- *new-application-resource-group-name* - Specifies the new name of the application resource group, which is case-insensitive. The length is 1 to 95 characters.

Viewing Application Resource Group Configuration Information

To view the configuration information of the specified application resource group, in any mode, use the following command:

show application-resource-group {**name** *application-resource-group-name* | **id** *id*}

- **name** *group-name* | **id** *id* - Specifies the application resource group name or ID.

To view the configuration information of all application resource groups, in the global configuration mode, use the following command:

show application-resource-group

Viewing Reference Information of an Application Resource Group

User traffic hitting a ZTNA policy will be or not be granted access to the application resource group referenced by the policy.

To view the reference information of the specified application resource group, in any mode, use the following command:

show reference application-resource-group *group-name*

- *group-name* - Specifies the application resource group name.

Configuring ZTNA Policy

Each ZTNA policy is labeled with a unique ID. When traffic flows into the ZTNA server, the device will query for ZTNA polices by turn, and processes the traffic according to the first matched policy. However, the ZTNA policy ID is not related to the matching sequence during the query. The policy sequence displayed by the command **show ztna-policy** is the actual sequence for the policy matching (the system will match the policies from the top to the bottom). You can specify the location of a ZTNA policy when creating the policy or moving its position in the global ZTNA policy configuration mode. The positions of a ZTNA policy can be either an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after a specific policy ID or name.

ZTNA grants access to users based on ZTNA policies. The system supports up to 2000 ZTNA policies. A ZTNA policy functions based on the matching condition and action. It supports the following dimensions as matching conditions:

- User/User group: When a user/user group matches the one configured in the ZTNA policy, this user/user group is considered to meet the matching condition.
- Application resource/Application resource group: When a requested application resource/application resource group matches the one configured in the ZTNA policy, this application resource/application resource group is considered to meet the matching condition.
- Endpoint tag: When the endpoint tag carried with an authenticated user matches the one configured in the ZTNA policy, this endpoint tag is considered to meet the matching condition.
- Schedule: When the user access time matches the one configured in the ZTNA policy, the access time is considered to meet the matching condition.

Each ZTNA policy can be configured with one or multiple matching conditions. For a ZTNA policy configured with multiple matching conditions, the policy is considered to be hit and the traffic will be processed based on the action specified in the policy only when all matching conditions are met. When a matching condition is not configured in a ZTNA policy, all objects are considered to meet this matching condition. The policy action includes two types (at least one must be configured):

- permit: User traffic hitting a specified ZTNA policy will be granted access to resources configured in the policy.
- deny: User traffic hitting a specified ZTNA policy will be denied access to resources configured in the policy.

User traffic that does not hit any ZTNA policies will hit the ZTNA default policy and be processed based on the default action.

This section describes the following ZTNA policy configurations:

- Creating a ZTNA Policy
- Configuring the ZTNA Policy Name
- Binding an Application Resource/Application Resource Group
- Binding an Endpoint Tag
- Binding a User/User Group
- Configuring a Schedule
- Specifying the Action
- Enabling/Disabling a ZTNA Policy
- Configuring Description for a ZTNA Policy
- Log Management of ZTNA Policies
- Entering Global ZTNA Policy Configuration Mode
- Binding Anti-Virus Profile
- Binding Sandbox Profile
- Binding IPS Profile

- Binding File Filter Profile
- Binding File Content Filter Profile
- Clearing ZTNA Policy Statistics Information

Creating a ZTNA Policy

To create a ZTNA policy and enter the ZTNA policy configuration mode, in the global configuration mode, use the following command:

ztna-rule [**name** *rule-name* | **id** *id*] [**top** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*}]

- **name** *rule-name* - Specifies the ZTNA policy name. The length is 1 to 95 characters.
- **id** *id* - Specifies the ZTNA policy ID. The value ranges from 1 to 2000. If the specified ID exists, you will enter the configuration mode of this ZTNA policy directly. If the ID is not specified for a new ZTNA policy, the system all automatically assign one.
- **top** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} - Specifies the position of the ZTNA policy. By default, the newly-created ZTNA policy is located at the end of all the ZTNA polices.
- **top** - Specifies the location of the policy to the top of all policies.
- **before** {**name** *rule-name* | *id*} - Specifies the location of the policy before the specified policy ID or name.
- **after** {**name** *rule-name* | *id*} - Specifies the location of the policy after the specified policy ID or name.

To delete the specified ZTNA policy, in the global configuration mode, use the following command:

no ztna-rule {**name** *rule-name* | **id** *id*}

Configuring the ZTNA Policy Name

For an existing ZTNA policy, to specify or modify its name, in the ZTNA policy configuration mode, use the following command:

name *name*

- *name* - Specifies the ZTNA policy name. The length is 1 to 95 characters.

To delete the ZTNA policy name, in the ZTNA policy configuration mode, use the following command:

no name

Binding an Application Resource/Application Resource Group

Each ZTNA policy can be bound with up to 10 application resources and 10 application resource groups. The logical relationship among multiple application resources/application resource groups is "Or". When a user accesses any of these application resources, the application resource dimension of the policy is considered to be hit. If a policy does not bind any application resources, all application resources can be matched.

To bind the specified application resource with the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

application-resource *application-resource-name*

- *application-resource-name* - Specifies the name of an existing application resource.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no application-resource *application-resource-name*

To bind the specified application resource group with the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

application-resource-group *group-name*

- *group-name* - Specifies the name of an existing application resource group.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no application-resource-group *group-name*

Binding an Endpoint Tag

Each ZTNA policy can be bound with up to 10 endpoint tags. The logical relationship among multiple endpoint tags is "Or". When a user matches any of these endpoint tags, the endpoint tag dimension of the policy is considered to be hit. If a policy does not bind any endpoint tags, all endpoint tags can be matched.

To bind the specified endpoint tag with the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

endpoint-tag *tag-name*

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no endpoint-tag *tag-name*

Binding a User/User Group

Each ZTNA policy can be bound with up to 8 users and 8 user groups. The logical relationship among multiple user/user groups is "Or". When any of the users attempts to access, the user dimension of the policy is considered to be hit. If a policy does not bind any users, all users can be matched.

To bind the specified user with the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

user *aaa-server-name user-name*

- *aaa-server-name* - Specifies the name of the AAA server that the user belongs to.
- *user-name* - Specifies the user name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no user *aaa-server-name user-name*

To bind the specified user group with the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

user-group *aaa-server-name user-group-name*

- *aaa-server-name* - Specifies the name of the AAA server that the user group belongs to.
- *user-group-name* - Specifies the user group name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no user-group *aaa-server-name user-group-name*

Configuring a Schedule

By default, the configured ZTNA policy will take effect immediately. If you apply a schedule to the ZTNA policy, it will only take effect in the specified time defined in the schedule. You can configure up to 10 schedules for a ZTNA policy, and the effective time of the policy is the sum of all time configured in the schedules. The logical relationship among multiple schedules is "Or". When any of these schedules is matched, the schedule dimension of the policy is considered to be hit. If a policy does not bind any schedules, all time can be matched. For information about how to configure a schedule, refer to System Management > Configuring Schedule.

To configure the specified schedule for the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* - Specifies the schedule name. To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To delete the specified schedule, in the ZTNA policy configuration mode, use the following command:

no schedule *schedule-name*

Specifying the Action

To specify the action to be performed on user traffic that hits the ZTNA policy, in the ZTNA policy configuration mode, use the following command:

action {**permit** | **deny**}

- **permit** | **deny** - Specifies the action that will be performed on user traffic that hits the ZTNA policy, i.e. permitting or denying access to the bound application resources/application resource groups.

Enabling/Disabling a ZTNA Policy

By default, the configured ZTNA policy will take effect immediately. You can disable a ZTNA policy to terminate its control over traffic. To enable or disable a ZTNA policy, in the ZTNA policy configuration mode, use the following command:

- Disable: **disable**
- Enable: **enable**

Configuring Description for a ZTNA Policy

To configure description for ZTNA policy, in the ZTNA policy configuration mode, use the following command:

description *description*

- *description* - Specifies the description of the ZTNA policy. The length is 1 to 255 characters. When the policy is already configured with description, it will be overwritten by the new description.

To delete the policy description, in the ZTNA policy configuration mode, use the following command:

no description

Log Management of ZTNA Policies

The system supports log management of ZTNA policies. By default, it is disabled.

- For the ZTNA policies of action Permit, logs will be generated when the matched traffic session starts and ends.
- For the ZTNA policies of action Deny, logs will be generated when the matched traffic is denied.

Before using this function, make sure the log function for the traffic is enabled. In the global configuration mode, use the command **logging traffic session on**. To configure the log management of ZTNA policies, in the ZTNA policy configuration mode, use the following command:

log {**policy-deny** | **session-start** | **session-end**}

- **policy-deny** – Generates logs when the matched traffic is denied. This parameter is applicable to the ZTNA policies of action Deny.
- **session-start** – Generates logs when the matched traffic starts its session. This parameter is applicable to the ZTNA policies of action Permit.
- **session-end** – Generates logs when the matched traffic ends its session. This parameter is applicable to the ZTNA policies of action Permit.

To cancel the log management configuration, in the ZTNA policy configuration mode, use the following command:

no log {**policy-deny** | **session-start** | **session-end**}

Binding Anti-Virus Profile

When the system is installed with the anti-virus license, you can bind an anti-virus profile to a ZTNA policy to achieve virus detection on traffic matching the ZTNA policy and process the detected viruses based on the Anti-Virus Profile. For information about anti-virus, please refer to Anti-Virus.

To bind an anti-virus profile, in the ZTNA policy configuration mode, use the following command:

av *profile-name*

- *profile-name* - Specifies the anti-virus profile name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no av

Binding Sandbox Profile

When the system is installed with the sandbox license, you can bind a sandbox profiles to a ZTNA policy to achieve sandbox detection on traffic matching the ZTNA policy. By using the cloud sandbox and the local sandbox technology, the system analyzes the suspicious file and collects the actions of the suspicious file, verifies the legality of the file, gives the analysis result to the system and deals with the malicious file based on the actions set by system. For information about sandbox, please refer to Sandbox.

To bind a sandbox profile, in the ZTNA policy configuration mode, use the following command:

sandbox *profile-name*

- *profile-name* - Specifies the sandbox profile name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no sandbox

Binding IPS Profile

When the system is installed with the IPS license, you can bind an IPS profile to a ZTNA policy to detect network attacks in traffic matching the ZTNA policy and perform actions such as blocking on the attacks based on the IPS Profile. For information about IPS, please refer to IPS.

To bind an IPS profile, in the ZTNA policy configuration mode, use the following command:

ips *profile-name*

- *profile-name* - Specifies the IPS profile name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no ips

Binding File Filter Profile

After the ZTNA policy is bound with a file filter profile, the system will perform file detection on traffic matching the ZTNA policy and perform control actions on the file matching the filter conditions based on the file filter profile. For information about file filter, please refer to File Filter.

To bind a file filter profile, in the ZTNA policy configuration mode, use the following command:

dlp *profile-name*

- *profile-name* - Specifies the file filter profile name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no dlp

Binding File Content Filter Profile

After the ZTNA policy is bound with a file content filter profile, the system will perform file content detection on traffic matching the ZTNA policy and perform control actions such as blocking or logging based on the file content filter profile. For information about file content filter, please refer to File Content Filter.

To bind a file filter profile, in the ZTNA policy configuration mode, use the following command:

file-contentfilter *profile-name*

- *profile-name* - Specifies the file content filter profile name.

To cancel the binding, in the ZTNA policy configuration mode, use the following command:

no file-contentfilter

Entering Global ZTNA Policy Configuration Mode

Some global configurations for the ZTNA policy should be completed in the global ZTNA policy configuration mode. To enter the global ZTNA policy configuration mode, in the system global configuration mode, use the following command:

ztna-policy-global

This section describes the following global ZTNA configurations:

- Specifying the Default Action
- Enabling/Disabling ZTNA Session Rematch
- Log Management of ZTNA Default Policy
- Moving a ZTNA Policy

Specifying the Default Action

You can specify the default action for the traffic that is not matched to any configured ZTNA policy. The system will process the traffic according to the specified default action. By default, the system will deny such traffic.

To configure the default action, in the global ZTNA policy configuration mode, use the following command:

default-action {**permit** | **deny**}

- **permit** | **deny** - Specifies the default action, i.e. permitting or denying access to resources.

Enabling/Disabling ZTNA Session Rematch

By default, ZTNA session rematch is enabled. When you add, modify or delete a ZTNA policy, the matched ZTNA policies for existing ZTNA sessions might change. The system will dispose sessions as follows:

- If ZTNA session rematch is enabled, the system will rematch ZTNA policies for existing sessions and delete the sessions for which the matched policy has changed.
- If ZTNA session rematch is disabled, the system will not rematch ZTNA policies for existing sessions. Related sessions will be kept until they time out.

Use the following command in the global ZTNA policy configuration mode to disable and enable ZTNA session rematch:

- Disable: **session-rematch off**
- Enable: **no session-rematch off**

Log Management of ZTNA Default Policy

For traffic hitting the ZTNA default policy, you can specify whether to generate logs. By default, the system does not generate log for such kind of traffic. To generate log for such traffic, in the global ZTNA policy configuration mode, use the following command:

log ztna-policy-default

To restore to the default value, in the global ZTNA policy configuration mode, use the following command:

no log ztna-policy-default

Moving a ZTNA Policy

To move a ZTNA policy, in the global ZTNA policy configuration mode, use the following command:

move {**name** *rule-name* | *id*} {**top** | **bottom** | **before** {**name** *rule-name* | *id*} | **after** {**name** *rule-name* | *id*} }

- **name** *rule-name* | **id** *id* – Specifies the ZTNA policy ID or name that you want to move.
- **top** – Moves the ZTNA policy to the top of all policies.
- **bottom** - Moves the ZTNA policy to the end of all policies.
- **before** {**name** *rule-name* | **id** *id*} – Moves the ZTNA policy before the specified policy ID or name.
- **after** {**name** *rule-name* | **id** *id*} – Moves the ZTNA policy after the specified policy ID or name.

Viewing ZTNA Policy Configuration Information

To view the configuration information of the specified ZTNA policy, in any mode, use the following command:

show ztna-policy {**name** *rule-name* | **id** *id*}

- **name** *rule-name* - Specifies the ZTNA policy name.
- **id** *id* - Specifies the ZTNA policy ID.

To view the ZTNA policy configuration information that matches the specified filter conditions, in any mode, use the following command:

show ztna-policy filter { [**application-resource** *application-resource-name*] [**application-resource-group** *application-resource-group-name*] [**description** *description*] [**endpoint-tag** *tag-name*] [**name***rule-name*] [**user** *user-name*] [**user-group** *user-group-name*] }

- **application-resource** *application-resource-name* - Shows ZTNA policy configuration information that matches the specified application resource name.
- **application-resource-group** *application-resource-group-name* - Shows ZTNA policy configuration information that matches the specified application resource group name.
- **description** *description* - Shows ZTNA policy configuration information that matches the specified description.
- **endpoint-tag** *tag-name* - Shows ZTNA policy configuration information that matches the specified endpoint tag.
- **name***rule-name* - Shows ZTNA policy configuration information that matches the specified ZTNA policy name.
- **user** *user-name* - Shows ZTNA policy configuration information that matches the specified user name.
- **user-group** *user-group-name* - Shows ZTNA policy configuration information that matches the specified user group name.

To view the configuration information of all ZTNA policies, in any mode, use the following command:

show ztna-policy

Viewing ZTNA Policy Statistics Information

To view the statistics information of ZTNA policies ranked in the top 10, top 20 and top 50 hit counts, in any mode, use the following command:

show ztna-policy statistics-information top {10 | 20 | 50 | **all**}

- **top** {10 | 20 | 50 | **all**} - Shows the statistics information of ZTNA policies ranked in the top 10, top 20 and top 50 hit counts. **all** means the statistics information of all ZTNA policies will be shown in descending order of hit counts.

To view all ZTNA policy statistics, use the following command:

show ztna-policy statistics-information

Clearing ZTNA Policy Statistics Information

To clear the statistics information of the specified ZTNA policy, in any mode, use the following command:

clear ztna-policy statistics-information {**name** *rule-name* | **id** *id*}

- **name** *rule-name* - Specifies the ZTNA policy name.
- **id** *id* - Specifies the ZTNA policy ID.

To clear the statistics information of all ZTNA policies, use the following command:

clear ztna-policy statistics-information all

To clear the statistics information of the ZTNA default policy, use the following command:

clear ztna-policy statistics-information default-action

Configuring Access Address Pool

ZTNA supports IPv4 and IPv6 type address pools. For information about address pool configuration.

Configuring an IPv4 Access Address Pool

Address pool is used to store IPv4 addresses allocated to clients. When a client connects to its server, the server will take an IPv4 address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

access-address-pool *pool-name*

- *pool-name* – Specifies a name for the address pool. The length is 1 to 31 characters.

This command creates a new address pool and leads you into the address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete an address pool, in the global configuration mode, use the following command:

no access-address-pool *pool-name*

The following sections explain how to configure address pools, including:

- Configuring an address range and network mask of a pool
- Configuring excluded addresses
- Configuring an IP binding rule
- Configuring a DNS server
- Configuring a WINS server

Configuring an IP Range of the Address Pool

To configure the start ip, end ip and network mask of an address pool, in the IPv4 address pool configuration mode, use the following command:

address *start-ip end-ip* **netmask** *A.B.C.D*

- *start-ip* – Specifies the start IPv4 address.
- *end-ip* – Specifies the end IPv4 address.
- **netmask** *A.B.C.D* – Specifies the network mask for this IPv4 address range.

To delete the IP range setting of an address pool, in the IPv4 address pool configuration mode, use the following command:

no address

Configuring Reserved Addresses

Some addresses in the address pool need to be reserved for other devices, like gateways, FTP servers, etc. These reserved IPv4 addresses are not allowed to allocate to clients.

To configure the start IP and end IP of reserved IP range, in the IPv4 address pool configuration mode, use the following command:

exclude address *start-ip end-ip*

- *start-ip* – Specifies the start IP for reserved IP range.
- *end-ip* – Specifies the end IP for reserved IP range.

To delete the reserved address range, in the IPv4 address pool configuration mode, use the following command:

no exclude

Configuring IP Binding Rules

If an IPv4 client needs static IPv4 address, IP-user binding rule can be applied to meet this requirement. Binding the user of IPv4 client to an IPv4 address in the address pool can guarantee that this IPv4 address is allocated to the client when it reaches the server. In addition, IPv4 address for an client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IPv4 addresses bound to this role.

When an IPv4 server allocates IPv4 addresses, it follows the rules below:

1. Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
2. Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.



Notes: IPv4 addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

Binding an IP to a User

To bind an IP address to a user, in the IPv4 address pool configuration mode, use the following command:

ip-binding user *user-name***ip** *ip-address*

- **user** *user-name* – Specifies the username.
- **ip** *ip-address* – Specifies an available IPv4 address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the IPv4 address pool configuration mode, use the following command:

no ip-binding user*user-name*

Binding an IP to a Role

To bind an IP address to a role, in the IPv4 address pool configuration mode, use the following command:

ip-binding role *role-name* **ip_range** *start-ip end-ip*

- **role** *role -name* – Specifies the role name.
- **ip_range** *start-ip end-ip* – Specifies the available IP range (start IPv4 address and end IPv4 address) in the address pool.

To cancel a binding between an IP range and a role, in the IPv4 address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IPv4 addresses, the system searches for the first rule which matches the user and applies the IPv4 address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the IPv4 address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after***role-name2*| **top** | **bottom**}

- *role-name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a DNS Server

To specify a DNS server, in the IPv4 address pool configuration mode, use the following command:

dns *address1* [*address2*] [*address3*] [*address4*]

- *address1* – Specifies the IPv4 address of DNS servers. You can specify up to four addresses.

To cancel the DNS setting, in the IPv4 address pool configuration mode, use the following command:

no dns

Configuring a WINS Server

To specify a WINS server, in the IPv4 address pool configuration mode, use the following command:

wins *address1* [*address2*]

- *address1* – Specifies the IPv4 address of WINS server. You can specify up to two WINS servers.

To cancel the WINS server setting, in the IPv4 address pool configuration mode, use the following command:

no wins

Viewing IPv4 Address Pool

To view information about an IPv4 address pool, in any mode, use the following command:

show access-address-pool [*pool-name*]

- *pool-name* – Specifies the name of IPv4 address pool to be shown. If this parameter is not specified, you can view all IPv4 address pools.

Here is an example of viewing IPv4 address pool:

```
hostname(config)# show access-address-pool pool_test1
Name: pool_test1
Address range: 3.3.3.1 - 3.3.3.10 (start IP and end IP)
Exclude range: 3.3.3.1 - 3.3.3.2 (reserved IP addresses)
Netmask: 255.255.255.0 (network mask of the address pool)
Wins server: (WINS server setting)
wins1: 10.1.1.1
```

```
Dns server:  (DNS server setting)
dns1: 10.10.209.1
IP Binding User: (IP-user binding)
test 3.3.3.8
IP Binding Role: (IP-role binding)
role1 3.3.3.3 3.3.3.7
```

To view statistical information about an IPv4 address pool, in any mode, use the following command:

show access-address-pool *pool-name* **statistics**

- *pool-name* – Specifies the name of IPv4 address pool whose statistics you want to view.

Here is an example of viewing statistics of an IPv4 address pool:

```
hostname(config)# show access-address-pool pool_test1 statistics
Total Ip Num 10 (total IP count in the address pool)
Exclude Ip Num 2 (reserved IP count)
Fixed Ip Num 6 (bound IP count)
Used Ip Num 2 (assigned IP count)
Fixed Used Ip Num 0 (assigned IP among the bound IP addresses)
Free Ip Num 6 (available IP count in the address pool)
```

Configuring an IPv6 Access Address Pool

IPv6 address pool is used to store IPv6 addresses allocated to clients. When a client connects to its server, the server will take an IPv6 address from the address pool according to the client propriety (like DNS server address or WIN server address) and give it to the client.

To creat an IPv6 address pool, in the global configuration mode, use the following command:

access-address-pool-ipv6 *pool-name*

- *pool-name* – Specifies a name for the address pool. The length is 1 to 31 characters.

This command creates a new address pool and leads you into the IPv6 address pool configuration mode; if the pool with this name exists, you will enter its configuration mode directly.

To delete an IPv6 address pool, in the global configuration mode, use the following command:

no access-address-pool-ipv6*pool-name*

The following sections explain how to configure IPv6 address pool, including:

- Configuring an address range and prefix of a pool
- Configuring excluded addresses
- Configuring an IP binding rule
- Configuring a DNS server

Configuring an IP Range of the Address Pool

To configure the start ip, end ip and network mask of an IPv6 address pool, in the IPv6 address pool configuration mode, use the following command:

address *start-ipv6-address end-ipv6-address* **prefix-len** *prefix-length*

- *start-ipv6-address* – Specifies the start IPv6 address.
- *end-ipv6-address* – Specifies the end IPv6 address.
- **prefix-len** *prefix-length* – Specifies the prefix for this IPv6 address range. The range is 111 to 128.

To delete the IP range setting of an address pool, in the IPv6 address pool configuration mode, use the following command:

no address

Configuring Reserved Addresses

Some addresses in the address pool need to be reserved for other devices, like gateways, FTP servers, etc. These reserved IPv6 addresses are not allowed to allocate to clients.

To configure the start IP and end IP of reserved IP range, in the IPv6 address pool configuration mode, use the following command:

exclude address *start-ipv6-address end-ipv6-address*

- *start-ipv6-address* – Specifies the start IP for reserved IP range.
- *end-ipv6-address* – Specifies the end IP for reserved IP range.

To delete the reserved address range, in the IPv6 address pool configuration mode, use the following command:

no exclude

Configuring IP Binding Rules

If an IPv6 client needs static IPv6 address, IP-user binding rule can be applied to meet this requirement. Binding the user of IPv6 client to an IPv6 address in the address pool can guarantee that this IPv6 address is allocated to the client when it reaches the server. In addition, IPv6 address for an client can be defined to an address range by using IP-role binding which defines an IP range for this role. When a client with the role connects to the server, it gets one address from the IPv6 addresses bound to this role.

When an IPv6 server allocates IPv6 addresses, it follows the rules below:

1. Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
2. Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.



Notes: IPv6 addresses in the IP-user binding rules and those in the IP-role binding rules should not conflict with each other.

Binding an IP to a User

To bind an IP address to a user, in the IPv6 address pool configuration mode, use the following command:

ip-binding user *user-name***ip** *ipv6-address*

- **user** *user-name* – Specifies the username.
- **ip** *ipv6-address* – Specifies an available IPv6 address in the address pool which will be bound to the user.

To cancel an IP-user binding, in the IPv6 address pool configuration mode, use the following command:

no ip-binding user*user-name*

Binding an IP to a Role

To bind an IP address to a role, in the IPv6 address pool configuration mode, use the following command:

ip-binding role *role-name* **ip-range** *start-ipv6-address end-ipv6-address*

- **role** *role -name* – Specifies the role name.
- **ip-range** *start-ipv6-address end-ipv6-address* – Specifies the available IP range (start IPv6 address and end IPv6 address) in the address pool.

To cancel a binding between an IP range and a role, in the IPv6 address pool configuration mode, use the following command:

no ip-binding role *role-name*

Changing the Sequence of IP-Role Binding

Normally, if a user belongs to multiple roles which bind to different IPv6 addresses, the system searches for the first rule which matches the user and applies the IPv6 address under this rule to the user. By default, new rule is at the bottom of the rule list.

To move the position of an IP-role binding rule in the rule list, in the IPv6 address pool configuration mode, use the following command:

move *role-name1* {**before** *role-name2* | **after** *role-name2*| **top** | **bottom**}

- *role –name1* – Specifies the role whose binding you want to move.
- **before** *role-name2* – Moves the binding rule before the IP-role binding specified here.
- **after** *role-name2* – Moves the binding rule after the IP-role binding specified here.
- **top** – Moves the binding rule to the top of the IP-role binding rule list.
- **bottom** – Moves the binding rule to the bottom of the IP-role binding rule list.

Configuring a DNS Server

To specify a DNS server, in the IPv6 address pool configuration mode, use the following command:

dns *ipv6-address1* [*ipv6-address2*] [*ipv6-address3*] [*ipv6-address4*]

- *ipv6-address1* – Specifies the IPv6 address of DNS servers. You can specify up to four addresses.

To cancel the DNS setting, in the IPv6 address pool configuration mode, use the following command:

no dns

Viewing IPv6 Address Pool

To view information about an IPv6 address pool, in any mode, use the following command:

show access-address-pool-ipv6 [*pool-name*]

- *pool-name* – Specifies the name of IPv6 address pool to be shown. If this parameter is not specified, you can view all IPv6 address pools.

Here is an example of viewing IPv6 address pool:

```
hostname(config)# show access-address-pool-ipv6
```

```
==================================================

Name Address range Prefix length

--------------------------------------------------

1-ipv6-pool 1000:5678:2222~ - 1000:5678:2222~112

2-ipv6-pool 1001:5678:2222~ - 1001:5678:2222~112

3-ipv6-pool 1002:5678:2222~ - 1002:5678:2222~112

4-ipv6-pool 1003:5678:2222~ - 1003:5678:2222~112

5-ipv6-pool 1004:5678:2222~ - 1004:5678:2222~112

6-ipv6-pool 1005:5678:2222~ - 1005:5678:2222~112

==================================================-
=========

hostname(config)# show access-address-pool-ipv6 2-ipv6-pool

Name: 2-ipv6-pool

Address range: 1001:5678:2222:3333:5555:ABCD:EFAB:1000 -
1001:5678:2222:3333:5555:ABCD:EFAB:3000 (start IP and end IP)

Exclude range: 1001:5678:2222:3333:5555:ABCD:EFAB:1000 -
1001:5678:2222:3333:5555:ABCD:EFAB:2000 (reserved IPv6 addresses)

prefix length: 112(prefix length of the address pool)

Dns server:  (DNS server setting)

dns1: AAAA:BBBB::1

dns2: 3333:2222::1
```

To view statistical information about an IPv6 address pool, in any mode, use the following command:

show access-address-pool-ipv6 *pool-name* **statistics**

- *pool-name* – Specifies the name of IPv6 address pool whose statistics you want to view.

Here is an example of viewing statistics of an IPv6 address pool:

```
hostname(config)# show access-address-pool-ipv6 2-ipv6-pool statistics
```

Total Ip Num 10 (total IP count in the address pool)

Exclude Ip Num 2 (reserved IP count)

Fixed Ip Num 6 (bound IP count)

Used Ip Num 2 (assigned IP count)

Fixed Used Ip Num 0 (assigned IP among the bound IPv6 addresses)

Free Ip Num 6 (available IP count in the address pool)

Configuring ZTNA Instance

To create a ZTNA instance, in the global configuration mode, use the following command:

tunnel ztna*instance-name* [**intranet** | **remote**]

- *instance-name* - Specifies a name for the ZTNA instance. The length is 1 to 31 characters.
- **intranet** | **remote** - Specifies the ZTNA instance type, which can be **intranet** or **remote**. By default, **remote** is selected.

This command creates a ZTNA instance with the specified name and leads you into the corresponding ZTNA instance configuration mode, including intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode; if the instance exists, you will enter this ZTNA instance configuration mode directly.

To delete a ZTNA instance, in the ZTNA instance configuration mode, use the following command:

no tunnel ztna *instance-name* {**intranet** | **remote**}



Notes: The system allows you to create at most 8 ZTNA gateways. Only one ZTNA gateway can be created in each VSYS, and ZTNA gateway of intranet access cannot be created in non-root VSYS.

In intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, you can configure the following:

- Specifying the Service Type
- Specifying an Access Address Pool (applicable only to remote access ZTNA instance)
- Specifying a Server Interface
- Specifying an SSL Protocol Version
- Specifying a PKI Trust Domain
- Specifying an Encryption Trust Domain

- Specifying the Tunnel Cipher Suite (applicable only to remote access ZTNA instance)
- Specifying an AAA Server
- Specifying an SSL Port Number
- Specifying the Transport Protocol (applicable only to remote access ZTNA instance)
- Configuring a ZTNA Tunnel Route (applicable only to remote access ZTNA instance)
- Configuring Anti-Replay (applicable only to remote access ZTNA instance)
- Configuring Packet Fragmentation (applicable only to remote access ZTNA instance)
- Configuring Forced Timeout (applicable only to intranet access ZTNA instance)
- Configuring Idle Time (applicable only to remote access ZTNA instance)
- Configuring forced logoff schedule
- Configuring Multi-logon
- Configuring Multi-Gateway Address
- Configuring URL Redirection
- Enabling/Disabling the Browser Download Function
- Binding Remote Access ZTNA Instance to a Tunnel Interface (applicable only to remote access ZTNA instance)
- Authentication with USB Key Certificate

Specifying the Service Type

This command can only be configured when the version is IPv6. By default, the service type of ZTNA instance is IPv4. To specify the service type of the ZTNA instance, including IPv4 or IPv6, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

service-type {**ipv4** | **ipv6**}

- **ipv4** | **ipv6** – Specifies the service type of the ZTNA instance, including IPv4 or IPv6.

Specifying an Access Address Pool

This configuration is applicable only to remote access ZTNA instance.

To specify an IPv4 address pool for the IPv4 ZTNA instance, in the ZTNA instance configuration mode, use the following command:

access-address-pool *pool-name*

- *pool-name* – Specifies the name of IPv4 address pool.

To cancel the IPv4 address pool, in remote access ZTNA instance configuration mode, use the following command:

no access-address-pool

To specify an IPv6 address pool for the IPv6 ZTNA instance, in remote access ZTNA instance configuration mode, use the following command:

access-address-pool-ipv6 *pool-name*

- *pool-name* – Specifies the name of IPv6 address pool.

To cancel the IPv6 ZTNA address pool, in remote access ZTNA instance configuration mode, use the following command:

no access-address-pool-ipv6

Specifying a Server Interface

The client uses HTTPS protocol to access the device. Each ZTNA instance can be configured with 8 interfaces. To specify the ZTNA interface of the device, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the interface for the ZTNA client to connect.

To cancel the ZTNA interface, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no interface *interface-name*

Specifying an SSL Protocol Version

To specify the SSL protocol version of the ZTNA instance, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

ssl-protocol { **tlsv1** | **tlsv1.2** | **gmssl** | **any**}

- **tlsv1** – Uses TLSv1 protocol.
- **tlsv1.2** – Uses TLSv1.2 protocol. This is the default option.
- **gmssl** – Uses GMSSLv1.0 protocol. After selecting this option, you're recommended to select the trust domain that contains SM2 type key for the PKI trust domain and the encrypted trust domain. The SM4 is preferred for encryption algorithm and the SM3 is preferred for hash algorithm.
- **any** – Uses any of the following protocols: TLSv1, TLSv1.1 and TLSv1.2.

To restore to the default value, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no ssl-protocol

If tlsv1.2 or any is specified to the SSL protocol in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate.

We will take the certificate file named oldcert.pfx as an example, the procedure is as follows:

1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format: openssl pkcs12 –in oldcert.pfx –out cert.pem
2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports tlsv1.2 protocol: openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"
3. Import the newly generated .pfx format certificate into your browser or USB Key.

Specifying a PKI Trust Domain

PKI trust domain in ZTNA is used in HTTPS authentication.

To specify a PKI trust domain for the ZTNA instance, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the name of PKI trust domain. The default domain is trust_domain_default.

To restore to the default value, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no trust-domain



Tips: For information on how to create a PKI trust domain, see PKI in User Authentication.

Specifying an Encryption Trust Domain

To specify the encryption trust domain which is used for the GMSSL negotiation for ZTNA, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

trust-domain-enc *trust-domain-name*

- *enc-cert* – Specifies the predefined encryption trust domain for GMSSL negotiation.

To delete the configured encryption trust domain, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no trust-domain-enc

Specifying a Tunnel Cipher Suite

This configuration is applicable only to remote access ZTNA instance. Tunnel cipher suite includes encryption algorithm, authentication algorithm and compression algorithm.

To specify a cipher suite for the tunnel, in remote access ZTNA instance configuration mode, use the following command:

tunnel-cipher encryption {**null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4**} **hash** {**null** | **md5** | **sha** | **sha256** | **sha384** | **sha512** | **sm3**} [**compression defl**]

- **null** | **des** | **3des** | **aes** | **aes192** | **aes256** | **sm4** – Specifies an encryption algorithm. The default value is AES. Null means no encryption is specified. For more information about encryption algorithms, see Encryption Algorithm in VPN.
- **null** | **md5** | **sha** | **sha256** | **sha384** | **sha512**| **sm3** – Specifies an authentication algorithm. The default value is MD5. Null means no authentication is specified. For more information about authentication algorithms, see Hash Algorithm in VPN.
- **compression defl** – Specifies the compression algorithm DEFALTE. The default setting is no compression. For more information on compression algorithms, see Compression Algorithm in VPN.

To restore to the default cipher suite setting, in remote access ZTNA instance configuration mode, use the following command:

no tunnel-cipher

Specifying an AAA Server

AAA server in ZTNA is used for user authentication. To specify an AAA server, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

aaa-server *aaa-server-name* [**domain** *domain-name*] [**keep-domain-name**]

- *aaa-server-name* – Specifies the name of AAA server you want to use for authentication.
- **domain** *domain-name* – Specifies the domain for the AAA server so that it can be distinguished from other servers. The length is 1 to 31 characters.
- **keep-domain-name** – After specifying this parameter, the AAA server uses the full name of the user, including the user name and the domain name, to perform the authentication.



Notes: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication. The OAuth2 server does not support user domain name verification (**keep-domain-name**).

To cancel the AAA server in an ZTNA, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no aaa-server *aaa-server-name* [**domain** *domain-name*]

Specifying an SSL Port Number

SSL port is used for the clients to access the device.

To specify an SSL port number, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

ssl-port *port-number*

- *port-number* – Specifies the SSL port number. The range is 1 to 65535. If multiple ZTNA instances use the same interface, their SSL port numbers cannot be the same and should be different from other services' SSL port numbers.

To restore to the default value, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no ssl-port

Configuring the Transport Protocol

This configuration is applicable only to remote access ZTNA instance. The system supports ZTNA data transmission over TCP or UDP. The default protocol is UDP, and the default port is 4433. To configure the transport protocol and port number, in remote access ZTNA instance configuration mode, use the following command:

transport-service {**tcp** | **udp**} *port-number*

- **tcp** | **udp** - Specifies TCP or UDP for data transmission.
- *port-number* – Specifies the port number for data transmission. The range is 1 to 65535.

To delete the transport protocol and port number, in remote access ZTNA instance configuration mode, use the following command:

no transport-service {**tcp** | **udp**}

Configuring a ZTNA Tunnel Route

This configuration is applicable only to remote access ZTNA instance. To reach the destination IPv4/IPv6 network segment or destination domain name through the ZTNA tunnel, you need to specify them by configuring the IPv4/IPv6 ZTNA tunnel route.

- The specified destination network segment will be distributed to the ZTNA client, then the client uses it to generate the route to the specified destination.

- The specified destination domain name will be distributed to the ZTNA client, and the client will generate the route to the specified destination according to the resolving results from DNS.

Configuring a ZTNA Tunnel Route to the Specified IPv4 Network Segment

You can only specify the IPv4 ZTNA tunnel route for the IPv4 ZTNA instance. To reach the destination IPv4 network segment through a ZTNA tunnel, in remote access ZTNA instance configuration mode, use the following command:

split-tunnel-route *ip-address/netmask* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

You can add multiple IPv4 tunnel routes as required.

To delete an IPv4 tunnel route, in remote access ZTNA instance configuration mode, use the following command:

no split-tunnel-route *ip-address/netmask* [**metric** *metric-number*]

Configuring a ZTNA Tunnel Route to the Specified IPv6 Network Segment

You can only specify the IPv6 ZTNA tunnel route for the IPv6 ZTNA instance. To reach the destination IPv6 network segment through a ZTNA tunnel, in remote access ZTNA instance configuration mode, use the following command:

split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ipv6-address/prefix* – Specifies the IPv6 address and prefix length of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

You can add multiple IPv6 tunnel routes as required.

To delete an IPv6 tunnel route, in remote access ZTNA instance configuration mode, use the following command:

no split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*]

Configuring a ZTNA Tunnel Route to the Specified Domain Name

After specifying a ZTNA tunnel route to a domain name, the system will distribute the domain name to the client. The client will generate the route to the specified destination according to the

resolving results from DNS. To configure a ZTNA tunnel route to the specified domain name, in remote access ZTNA instance configuration mode, use the following command:

domain-route {**disable** | **enable** | **max-entries** *value* | *url*}

- **disable** – Does not distribute the specified domain name to the client. This is the default option.
- **enable** – Distributes the specified domain name to the client.
- **max-entries** *value* – Specifies the maximum number of routes that can be generated after obtaining the resolved IP addresses of the domain name. The default value is 1000. The value ranges from 1 to 10000.
- *url* – Specifies the URL of the domain name. You can add one each time and you can add up to 64 domain names. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. **com** and **.com** are not supported.

To delete the specified domain name, use the following command in remote access ZTNA instance configuration mode:

no domain-route *url*



Notes: The domain route function cannot be used together with the dedicated ZTNA tunnel function. For more information about how to configure the dedicated ZTNA tunnel function, see Enabling Dedicated ZTNA Tunnel.

Enabling Dedicated ZTNA Tunnel

The system supports the Dedicated ZTNA Tunnel function. By default, this function is disabled. After you enable this function, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to ZTNA.

Notes:

- The client versions that support the dedicated ZTNA tunnel function include: the latest version of the ZTNA client for Windows, the latest version of the ZTNA client for macOS, and the latest version of the ZTNA client for Linux.
- The dedicated ZTNA tunnel function cannot be used together with the domain route function. For more information about how to configure the domain route function, see Configuring a ZTNA Tunnel Route to the Specified Domain Name.
- After you enable the dedicated ZTNA tunnel function, we recommend that you do not configure a default route in the tunnel routing.

To enable/disable the dedicated ZTNA tunnel function, in remote access ZTNA configuration mode, use the following command:

dedicated-tunnel {**enable** | **disable**}

- **enable** - Enable the dedicated ZTNA tunnel function.
- **disable** -Disable the dedicated ZTNA tunnel function.

Configuring Anti-Replay

This configuration is applicable only to remote access ZTNA instance. Anti-Replay is used to prevent hackers from injecting the captured packets repeatedly by rejecting the packets.

To enable Anti-Replay, in remote access ZTNA instance configuration mode, use the following command:

anti-replay {32 | 64 | 128 | 256 | 512}

- **32** – Specifies that the Anti-Replay window size is 32. This is the default value.
- **64** – Specifies that the Anti-Replay window size is 64.
- **128** – Specifies that the Anti-Replay window size is 128.
- **256** – Specifies that the Anti-Replay window size is 256.
- **512** – Specifies that the Anti-Replay window size is 512.

Bigger window size suits more in bad network conditions, such as serious packets disorder.

To restore the Anti-Replay window size to the default value, in remote access ZTNA instance configuration mode, use the following command:

no anti-replay

Configuring Forced Timeout

This configuration is applicable only to intranet access ZTNA instance. After the client accesses the intranet successfully, when the online duration of the user reaches the configured forced timeout period, the system kicks out the user and forces the user offline. To configure forced timeout, in intranet access ZTNA instance configuration mode, use the following command:

force-timeout*time-value*

- *time-value* – Specifies the forced timeout period. Valid values: 10 to 10080. Default value: 10080. Unit: minutes.

To restore the forced timeout to the default value, in intranet access ZTNA instance configuration mode, use the following command:

no force-timeout

Configuring Packet Fragmentation

You can specify if packet fragmentation is permitted in the device.

To configure packet fragmentation, in the ZTNA instance configuration mode, use the following command:

df-bit {**copy** | **clear** | **set**}

- **copy** – Copies the DF value from the destination of the packet. This is the default value.
- **clear** – Permits packet fragmentation.
- **set** – Forbids packet fragmentation.

To restore to the default value, in the ZTNA configuration mode, use the following command:

no df-bit

Configuring Idle Time

This configuration is applicable only to remote access ZTNA instance. Idle time defines the time length a client is allowed to connect to the device without any operation. When a client takes no action for the time period of idle time specified here, it is forced to log out the device.

To specify the idle time, in remote access ZTNA instance configuration mode, use the following command:

idle-time *time-value*

- *time-value* – Specifies the idle time value. The value range is 1 to 1500 minutes. The default value is 30.

To restore to the default value, in remote access ZTNA instance configuration mode, use the following command:

no idle-time

Configuring Forced Logoff Schedule

When forced logoff schedule is configured for an ZTNA Instance, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. To configure the forced logoff schedule, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

kickout-all-user schedule *schedule-name*

- *schedule-name* - Specified the name of the schedule. The system forces users to log out at the start time of the timeframe.



Notes:

- The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect.
- SSL VPN users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.

Configuring Multi-Logon

To allow multiple users to log in at multiple places with the same user name simultaneously, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

allow-multi-logon

This command enables the function and does not limit the login number. If you want to specify the number of users logging in with the same user name simultaneously, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

allow-multi-logon number *number*

- *number* – Specifies the number of users who are allowed to log in with one user name. The value range is 1 to 99999999.

To disable multi-logon, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no allow-multi-logon

Configuring Multi-Gateway Address

ZTNA supports configuration of multiple backup gateways for clients to select which to connect. When the ZTNA device is configured with backup gateways, ZTNA users can enable gateway detection on clients to select the connected ZTNA gateway.

After gateway detection is enabled, ZTNA client will attempt to obtain the backup gateway list from the gateway that the user is logging in, detect the link quality of all backup gateways and then establish the ZTNA connection with the one that has the best link quality. After the connection is established, ZTNA client will detect and update the link quality every 30 minutes. When a connection or login failure occurs, ZTNA client will switch to connect the backup gateway that has the best link quality.

To configure a backup gateway, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

gateway *gateway-name* {**ipv4** *ip-address* | **domain** *string*}

- *gateway-name* - Specifies the backup gateway name. The range is 1 to 31 characters.
- *ip-address* - Specifies the IPv4 address of the backup gateway.
- *string* - Specifies the domain name of the backup gateway. The range is 1 to 255 characters, and the length between two dots (.) cannot exceed 63 characters.

Repeat this command to configure multiple backup gateways.

To delete the specified backup gateway, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no gateway *gateway-name*



Notes: ZTNA configurations on the backup gateways need to be consistent with those on the master backup gateway.

Configuring URL Redirection

URL redirection function in ZTNA server displays a specified URL page to the authenticated client user. By default, this function is disabled.

To enable URL redirection, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

redirect-url *url* **title** *name*

- *url* – Specifies the URL address of the page shown for the new authenticated client. The value range is 1 to 255 characters. It can be an HTTP (http://) or an HTTPS (https://) address.
- **title** *name* – Specifies a description for the redirect page. The value range is 1 to 31 characters.

To cancel URL redirection, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no redirect-url

URL Format

- For pages of UTF-8 encoding, type URL + username=$USER&password=$PWD, for example, type the address http://www.-abc.com/oa/login.do?username=$USER&password=$PWD.
- For pages of GB2312 encoding, type URL + username=$GBUSER&password=$PWD, for example, type the address http://www.-abc.com/oa/login.do?username=$GBUSER&password=$PWD.
- For other pages, type http://www.abc.com.

Enabling/Disabling the Browser Download Function

With the browser download function, you're allowed to download the ZTNA client via the browser WebUI. By default, the function is enabled. When this function is disabled, you can only download the ZTNA client from www.hillstonenet.com.cn.

To enable the function, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

client-download-page enable

To disable the function, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

client-download-page disable

Binding Remote Access ZTNA Instance to a Tunnel Interface

This configuration is applicable only to remote access ZTNA instance. Only when a remote access ZTNA instance binds to a tunnel interface can it take effect.

To bind a remote access ZTNA instance to a tunnel interface, in the tunnel interface configuration mode, use the following command:

tunnel ztna *instance-name*

- *instance-name* – Specifies the name of the remote access ZTNA instance you want to bind.

  A tunnel interface can be bound to only one remote access ZTNA instance.

To cancel the binding of a remote access ZTNA instance, in the tunnel interface configuration mode, use the following command:

no tunnel ztna *instance-name*

Authentication with USB Key Certificate

The client is allowed to use a USB flash disk that stores a certificate to authenticate. A USB disk which supports Windows SDK (Certificate Store Functions) and has a legal UKey certificate can pass the authentication and connect to the server.

The following sections describe how to configure USB Key certificate authentication, including:

- Enabling USB Key certificate authentication
- Importing a CA certificate to a trust domain
- Configuring a trust domain

Enabling USB Key Certificate Authentication

By default, this function is disabled. To enable the USB Key certificate authentication, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

client-cert-authentication [**usbkey-only**]

- **usbkey-only** – Specifies the USB Key authentication as USB Key only. If this parameter is not specified, the authentication of Username/Password + USB Key will be used.

To disable the function, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no client-cert-authentication [**usbkey-only**]

Importing a USB Key Certificate to a Trust Domain

CA certificates can be imported through various methods, including downloading from an FTP or TFTP server and from USB disk. To import a certificate, in the execution mode, use the following command:

import pki trust-domain *trust-domain-name* **cacert from** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- *trust-domain-name* – Specifies the name of PKI trust domain.
- **ftp server** *ip-address* [**user** *user-name* **password** *password*] – Specifies the IP address of FTP server, user name and password to log in. If the server supports anonymous login, skip the user name and password.
- **tftp server** *ip-address* – Specifies the IP address of TFTP server.

- **usb0** | **usb1** – Specifies the port to which the USB disk is plugged.
- *file-name* – Specifies the file name of CA certificate.

Specifying a Trust Domain for the CA Certificate

USB Key certificate authentication requires a trust domain for the CA certificate. When the certificate provided from client matches one of the trust domain certificates, it passes authentication.

To specify a trust domain, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

client-auth-trust-domain *trust-domain*

- *trust-domain* – Specifies a configured PKI trust domain for the CA certificate.

Repeat this command to add more trust domains. The system supports up to 10 domains.

To cancel a PKI trust domain for a certificate, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no client-auth-trust-domain *trust-domain*



Tips: For information on how to create PKI trust domain, see PKI in User Authentication.

Configuring Two-Step Verification

Two-Step Verification means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS Authentication, Token Authentication or Email Authentication after the user name and password is entered. The user must enter the random verification code received in order to log in the ZTNA server and access intranet resources.

Enabling/Disabling Two-Step Verification

The two-step verification function is disabled by default. To enable or disable the two-step verification function, in the ZTNA instance configuration mode, use the following command:

- Enable: **two-step verification enable**
- Disable: **two-step verification disable**

Specifying the Type of Two-Step Verification

To specify the type of two-step verification, in the ZTNA instance configuration mode, use the following command:

two-step verification type {**token** | **sms modem** | **sms service-provider** | **email**}

- **token** - Specifies to use the token authentication for two-step verification.
- **sms modem** - Specifies to send a short message through an SMS modem for two-step verification.
- **sms service-provider** - Specifies to send a short message through an SMS gateway for two-step verification.
- **email** - Specifies to use Email authentication for two-step verification.

Token Authentication

The system supports for authentication through the token password when logging in, and user-defined prompt information for token authentication.

Configuring Prompt Message

To configure the prompt message of the token authentication, in the ZTNA instance configuration mode, use the following command:

token-auth prompt-message *message*

- **prompt-message** *message*- Specifies the prompt message. The range is 1 to 255 characters.

SMS Authentication

SMS authentication means that when a ZTNA user logs in by providing a user name and password, the Hillstone device, through an SMS modem or an SMS gateway, sends a dynamically generated random password to the mobile phone number of the user in SMS after the use rname and password is entered. The user must enter the random password received in the mobile phone in order to log in the ZTNA server and access intranet resources. This section describes how to configure the global parameters for the SMS authentication function.



Notes: Not all platforms support SMS authentication.

Modem Authentication

Hillstone device adopts an external GSM modem. Before configuring the SMS authentication function, you need to prepare a SIM card and a GSM modem, and then connect the modem to the device properly. To connect the modem to the device, first, you should insert the SIM card into the GSM modem properly; then, connect the modem to the USB port of the device via a USB cable.

The following models of SMS modem are recommended:

Model	Type	Chip	Interface
GSM MODEM (M1206B, M1206B-FT and M1806-NC5)	GSM	WAVECOM	USB interface

The following sections introduce how to configure SMS authentication, including:

- Configuring a mobile phone number for SMS authentication
- Configuring expiration time of SMS authentication code
- Configuring the SMS authentication code length
- Configuring the SMS authentication code content
- Configuring a maximum SMS number
- Sending a test message

Configuring a Mobile Phone Number for SMS Authentication

ZTNA local users and AD users, when assigned with a mobile phone number by the administrator, can use SMS password sent by the system to authenticate.

To configure the phone number for a local user, in the user configuration mode, use the following command:

phone *phone-number*

- *phone-number* – Specifies the mobile phone number.

To cancel a number, in the user configuration mode, use the following command:

no phone

For an AD user, configure the mobile phone number in the mobile propriety of AD server.

Configuring Expiration Time of SMS Authentication Code

Each SMS authentication code has a period of validity. If the user neither types the authentication code within the period nor applies for a new code, ZTNA server will disconnect the connection.

To configure the SMS authentication code validity period, in the ZTNA instance configuration mode, use the following command:

sms-auth expiration *expiration*

- *expiration* – Specifies the validity period. The range is 1 to 10 minutes. The default value is 10.

To restore the validity period to the default value, in the ZTNA instance configuration mode, use the following command:

no sms-auth expiration

Configuring the SMS Authentication Code Length

To specify the length of the SMS authentication code, in the ZTNA instance configuration mode, use the following command:

sms-auth verification-code-length *length*

- *length* – Specifies the length of the SMS authentication code. The range is 4 to 8 characters. The default value is 8.

In the ZTNA. instance configuration mode, use the following command to restore the code length to the default value.

no sms-auth verification-code-length

Configuring the SMS Authentication Code Content

To specify the SMS authentication code content, in the ZTNA instance configuration mode, use the following command:

sms-auth message-content *content*

- *content* – Specifies the SMS authentication code content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 9 to 500 characters.

In the ZTNA instance configuration mode, use the following command to restore the code content to the default value.

no sms-auth message-content

Configuring a Maximum SMS Number

You can specify the maximum number of SMS messages sent by the SMS modem per hour or per day. If the modem is required to send more messages than the maximum number, it will reject and record a log.

To configure the maximum SMS number, in the global configuration mode, use the following command:

sms modem {**num-per-hour** | **num-per-day**} *number*

- {**num-per-hour** | **num-per-day**} *number* – Specifies the maximum number of SMS messages per hour or per day. The value range is 1 to 1000.

If you do not limit the maximum number of SMS messages sent by the SMS modem per hour or per day, in the global configuration mode, use the following command:

no sms modem {**num-per-hour** | **num-per-day**}

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number.

To send a test message, in any mode, use the following command:

exec sms send test-message to *phone-number*

- *phone-number* – Specifies the phone number which receives the test message. The length is 6 to 16 characters.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

Viewing SMS Modem Settings

To view the configuration information of an SMS modem, in any mode, use the following command:

show sms modem

SMS Gateway Authentication

Hillstone device, through SMS gateway or other proxy server, can send a short message to users in SMS after the user name and password is entered. Before configuring the function, you need to ask the supplier to provide the necessary information, such as the gateway address, device ID which sends the short messages.

SMS gateway authentication configuration includes:

1. Create a Service Provider (SP) instance.
2. Bind the SP instance to a configured ZTNA instance, and enable the SMS gateway authentication function.

Specifying the Default Protocol Type of SMS Gateway

The types of SMS gateway protocol supported by the device include SGIP, UMS, ACC, ALIYUNSMS, XUANWU, CAS, BEIKE and HTTP(S). SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. HTTP(S) indicates HTTP/HTTP(S) protocol. To specify the default protocol type of SMS gateway, in the global configuration mode, use the following command:

sms service-provider default-protocol {**sgip** | **ums** | **acc** | **aliyunsms**| **xuanwu** | **cas** | **beike** | **http(s)**}

- **sgip** | **ums** | **acc** | **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)**- Specifies the default protocol type of SMS gateway that the SP instance is running. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates the BEIKE SMS gateway. http(s) indicates HTTP/HTTPS protocol.

In the global configuration mode, use the command **no sms service-provider default-protocol**to cancel the specified default protocol type.

Creating an SP Instance

To create an SP instance, use the following command in the global configuration mode:

sms service-provider *sp-name* [**protocol** {**sgip** | **ums** | **acc** | **aliyunsms**| **xuanwu** | **cas** | **beike** | **http(s)**}]

- *sp-name* - Specifies the SP instance name. The value range is 1 to 31.
- **protocol** {**sgip** | **ums** | **acc** | **aliyunsms** | **xuanwu** | **cas** | **beike** | **http(s)**} - Specifies the protocol of SMS gateway that the SP instance is running. System only supports SGIP of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Telecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates the BEIKE SMS gateway. http(s) indicates HTTP/HTTPS protocol.

This command creates an SP instance and leads you into the SP instance configuration mode; if the instance exists, you will enter the SP instance configuration mode directly. The system supports at most eight SP instances now.

In the global configuration mode, use the following command to delete the specified SP instance:

no sms service-provider *sp-name*

You can perform the following configurations in the SP instance configuration mode:

- Specifying the VRouter
- Specifying the Request Method
- Specifying the Charset
- Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol
- Specifying the URL
- Specifying the Success Code
- Specifying the Attributes
- Specifying the Gateway Address and Port Number
- Specifying the Number to Send Auth-message
- Specifying the Device ID
- Specifying the User Name and Password
- Specifying the Template Parameter
- Specifying a Maximum SMS Number
- Specifying the Company Code
- Specifying the AccessKeyId
- Specifying the AccessKeySecret
- Specifying Instance of SMS Gateway
- Specifying the Sender Name or Sign Name
- Specifying the Template Code

- Specifying the Request Type
- Specifying the Organization Code
- Specifying the SMS Service Type
- Specifying the Trading Code
- Specifying the Channel
- Sending a Test Message
- Enabling/Disabling the Sending Sign Code Function

Specifying the VRouter

The system supports multi-Vrouter, and the default VRouter is trust-vr. To specify the VRouter which SP belongs to, use the following command in the SP instance configuration mode:

vrouter {**trust-vr** | *vr-name*}

- **trust-vr** - Specifies the VRouter as trust-vr.
- *vr-name* – Specifies a created VRouter.

In the SP instance configuration mode, use the following command to restore the default VRouter:

no vrouter

Specifying the Request Method

When the HTTP (S) protocol type is specified for the SP instance, you can specify the request method of HTTP(S). The default request method is POST. To specify the request method, in the SP instance configuration mode, use the following command:

request-type [**get** | **post**]

- **get** – Specifies the request method of HTTP(S) as GET.

- **post** – Specifies the request method of HTTP(S) as POST.

To restore the default request type, use the command **no request-type**.

Specifying the Charset

When the HTTP (S) protocol type is specified for the SP instance, you can specify the charset of HTTP(S). The default charset is UTF-8. To specify the charset, in the SP instance configuration mode, use the following command:

charset [**utf-8** | **gbk**]

- **utf-8** – Specifies to use UTF-8 to encode the content of the authentication message.
- **gbk** – Specifies to use GBK to encode the content of the authentication message.

To restore the default charset, use the command **no charset** .

Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol

To specify the protocol of UMS, ACC , ALIYUNSMS, BEIKE or CAS, in the SP instance configuration mode, use the following command:

protocol {**http** | **https**}

- **http** | **https** – Specifies the protocol type as HTTP or HTTPS. The default protocol of UMS and BEIKE is HTTPS. The default protocol of UMS and CAS is HTTPS. The default protocol of ACC and ALIYUNSMS is HTTP.

In the SP instance configuration mode, use the following command to restore the default protocol type:

no protocol

Specifying the URL

When the HTTP (S) protocol type is specified for the SP instance, you can specify the URL of HTTP(S). You need to enter a complete access path. The system requests to communicate with

the SMS gateway based on the specified URL address. To specify the URL address, in the SP instance configuration mode, use the following command:

url *url string*

- *url string* – Specifies the URL address of the SMS gateway, such as "http(s)://1.1.1.1". The range is 1 to 255 characters.

To delete the specified URL address, use the command **no url**.

Specifying the Success Code

When the HTTP (S) protocol type is specified for the SP instance, you can specify the success code of HTTP(S). Success code is used to determine whether the SMS gateway successfully sent an authentication message. The SMS gateway sends an authentication message to the mobile phone, and when completed, it will send a message containing the status code to the system. If the message contains the specified success code, the system will judge that the authentication message has been sent successfully. For example, if an SMS gateway sent an authentication message successfully, the status code returned is "OK: 325689", and if failed, the status number returned is "ERROR: eUser". In this instance, you can specify the success code as "OK". When the system receives a message sent by the SMS gateway, it determines whether the message contains "OK". If the message contains the specified success code, it means that the SMS gateway has sent message successfully. To specify the success code, in the SP instance configuration mode, use the following command:

success-code *string*

- *string* – Specifies the success code. The range is 1 to 50 characters. Different SMS gateways return different status code. Refer to the status code in the SMS gateway manual.

To delete the specified success code, use the command **no success-code**.

Specifying the Attributes

When the HTTP (S) protocol type is specified for the SP instance , you can configure attributes to communicate with the SMS gateway. Attributes including the parameter name of the mobile number field, the parameter name of the message content field, the password filed, and the username filed, etc. You can configure up to 32 attributes. The parameter name of the mobile number

field and the parameter name of the message content field are default attributes and must be specified.

To specify the parameter name of the mobile number field and the parameter name of the message content field, in SP instance configuration mode, use the following command:

default-attribute {**phone-attr-name** *phone-attr-name* | **msg-content-attr-name** *msg-content-name*}

- **phone-attr-name** *phone-attr-name* – Specifies the parameter name of the mobile number field, such as phone. This is the default attribute and the range is 1 to 400 characters.
- **msg-content-attr-name** *msg-content-name* – Specifies the parameter name of the message content field, such as msg. This is the default attribute and the range is 1 to 400 characters.

The system will obtain the parameter values of the mobile number field and the parameter values of the message content field when SMS gateway and the system is communicating.

When the SMS gateway and the system communicate, the SMS gateway can obtain the parameter values of the mobile number field and the parameter values of the message content field from the system. To delete the parameter name of the specified mobile number field and the parameter name of the message content field, use the command **no default-attribute** {**phone-attr-name** | **msg-content-attr-name**}.

To specify the parameters of password to log in SMS gateway, which is an optional attribute, in SP instance configuration mode, use the following command:

password-attribute *password-name password-value*

- *password-name* – Specifies the parameter name of the password, such as password. The range is 1 to 20 characters.
- *password-value* – Specifies the parameter value of the password, such as 123456. The range is 2 to 255 characters.

To delete the specified parameters of password, use the command **no password-attribute**.

To specify the parameters of username to log in SMS gateway, which is an optional attribute, in SP instance configuration mode, use the following command:

user-attribute *user-name user-value*

- *user-name* – Specifies the parameter name of the username, such as username. The range is 1 to 20 characters.
- *user-value* – Specifies the parameter value of the username, such as user1. The range is 2 to 255 characters.

To delete the specified parameters of username, use the command **no user-attribute**.

Specifying the Gateway Address and Port Number

To specify the gateway address and port number, in the SP instance configuration mode, use the following command:

gateway {**host** *hostname* | **ip** *ip-address*} [**port** *port-number*]

- **host** *hostname* - Specifies the host name of the gateway. The range is 1 to 31 characters.
- **ip** *ip-address* - Specifies the IP address of the gateway.
- **port** *port-number* - Specifies the port number of the gateway. When the protocol type is specified as "SGIP", the default port number is 8801; When the protocol type is specified as "ACC", the default port number is 80. When the protocol type is specified as "UMS", the default port number is 9600. When the protocol type is specified as "XUANWU" or "CAS", the default port number is 8080.

Execute this command for many times and the latest configuration takes effect.

In the SP instance configuration mode, use the following command to delete the gateway address and restore to the default port number:

no gateway {**host** | **ip**}

Specifying the Template Parameter

To specify the template parameter of BEIKE SMS gateway, in the SP instance configuration mode, use the following command:

template *value*

- *value* – Specifies the template parameter of BEIKE SMS gateway. The length is 1 to 64 characters.

In SP instance configuration mode, use the following command to delete the template parameter of BEIKE SMS gateway:

no template

Enabling/Disabling the Sending Sign Code Function

When this function is enabled, the ACC SMS gateway will add a sign code field when sending a request to the ACC server, which will prevent the content of the SMS from being tampered with. In the SP instance configuration mode, use the following command to enable the sending sign code function:

sign enable

In the SP instance configuration mode, use the following command to disable the sending sign code function:

no sign enable

Specifying the Number to Send Auth-message

When the SP instance uses the SGIP type SMS gateway, after enabling the SMS Authentication function, the system will send an Auth-message to the mobile phone number. In the SP instance configuration mode, use the following command to set the number:

source-number *phone-number*

- *phone-number* – Specifies the user's phone number. The range is 1 to 21 characters.

In the SP instance configuration mode, use the following command to cancel the specification of user's phone number:

no source-number

Specifying the Device ID

When the SP instance uses the SGIP type SMS gateway, you have to ask your supplier to provide the device ID of SP, which sends the SMS messages. In the SP instance configuration mode, use the following command to specify the device ID:

device-code *code-number*

- *code-number* - Specifies the device ID. The range is 1 to 4294967295.

In the SP instance configuration mode, use the following command to cancel the device ID specification:

no device-code

Specifying the User Name/User ID and Password

To specify the user name/user ID and password, in the SP instance configuration mode, use the following command:

user {*username* | *userid*} **password** *password*

- *username* | *userid* – Specifies the user name or user ID to log in SMS gateway. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1 to 64 characters. When the protocol type is specified as "XUANWU", the range is 1 to 6 characters.
- *password* – Specifies the password for the user. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1 to 64 characters. When the protocol type is specified as "XUANWU", the range is 1 to 6 characters.

In SP instance configuration mode, use the following command to cancel the specification of user name/user ID and password:

no user

Specifying a Maximum SMS Number

When the SP instance uses the SGIP or UMS type SMS gateway, you can specify the maximum number of SMS messages sent by the SMS gateway per hour or per day. To configure the maximum SMS number, in the SP instance configuration mode, use the following command:

{**num-per-hour** | **num-per-day**} *number*

- *number* – Specifies the maximum number of SMS messages per hour or per day. The value range is 0 to 65535.

In the SP instance configuration mode, use the following command to cancel the maximum number:

no {**num-per-hour** | **num-per-day**}

Specifying the Company Code

When the SP instance uses the UMS protocol type, users can specify the enterprise code registered on the UMS platform, in the SP instance configuration mode, use the following command:

spcode*spcode-number*

- *spcode-number* - Specifies the company code. The range is 1 to 31 digits.

In the SP instance configuration mode, use the following command to cancel the company code:

no spcode

Specifying the AccessKeyId

If the protocol of SMS gateway that the SP instance is running is ALIYUNSMS, users must specify the AccessKeyId which will be used as the user name for authentication between the device and the SMS gateway of Alibaba Cloud . To specify the AccessKeyId, in the SP instance configuration mode, use the following command:

accesskeyid*word*

- *word* - Specifies the AccessKeyId. The range is 1 to 63 characters. This parameter should be the same with the template AccessKeyId applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the **no accesskeyid** command to cancel the specified AccessKeyId.

Specifying the AccessKeySecret

If the protocol of SMS gateway that the SP instance is running is ALIYUNSMS, users must specify the AccessKeySecret which will be used as the password for authentication between the device and the SMS gateway of Alibaba Cloud. To specify the AccessKeySecret, in the SP instance configuration mode, use the following command:

accesskeysecret *word*

- *word* - Specifies the AccessKeySecret. The range is 1 to 31 characters. This parameter should be the same with the template AccessKeySecret applied in the SMS of Alibaba Cloud.

In the SP instance configuration mode, use the **no accesskeysecret** command to cancel the specified AccessKeySecret.

Specifying Instance of SMS Gateway

The SP instance needs to be bound to the ZTNA tunnel to take effect. To specify the SMS gateway instance, in the ZTNA instance configuration mode, use the following command:

sms-auth service-provider *sp-name*

- *sp-name* – Specifies the name of the SP instance, which must be the created SP instance. The value range is 1 to 31 characters.

Specifying the Sender Name or Sign Name

If the protocol of the SP instance bound to ZTNA tunnel is SGIP, USM or ACC, users can specify a message sender name to display in the message content. If the protocol of the SP instance bound to ZTNA tunnel is ALIYUNSMS, users must specify the sign name applied in the SMS of

Alibaba Cloud to display in the message content. To specify the sender name or sign name, in the ZTNA instance configuration mode, use the following command:

sms-auth sms-sender-name *sender-name*

- *sender-name* – Specifies the sender name. The range is 1 to 63 characters. The sign name should be the same with the sign name applied in the SMS of Alibaba Cloud.

In the ZTNA instance configuration mode, use the following command to cancel the specified sender name or sign name:

no sms-auth sms-sender-name



Notes: Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.

Specifying the Template Code

If the protocol of the SP instance bound to ZTNA tunnel is ALIYUNSMS, users must specify the code of the SMS template applied in the SMS of Alibaba Cloud. To specify the template code, in the ZTNA instance configuration mode, use the following command:

sms-auth sms-msg-templatecode *word*

- *word* – Specifies the template code. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.

In the ZTNA instance configuration mode, use the following command to cancel the specified template code:

no sms-auth sms-msg-templatecode

Specifying the Request Type

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the request type. To specify the request type, in the SP instance configuration mode, use the following common:

post-type *post_type*

- *post_type* – Specifies the request type. The range is 1 to 6 characters.

In the SP instance configuration mode, use the following command to cancel the request type:

no post-type

Specifying the Organization Code

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the organization code. To specify the organization code, in the SP instance configuration mode, use the following common:

orgcode *orgcode*

- *orgcode* – Specifies the organization code. The range is 1 to 31 characters.

In the SP instance configuration mode, use the following command to cancel the organization code:

no orgcode

Specifying the SMS Service Type

If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the SMS service type. To specify the SMS service type, in the SP instance configuration mode, use the following common:

smstype *smstype*

- *smstype* – Specifies the SMS service type. The range is 1 to 31 characters.

In the SP instance configuration mode, use the following command to cancel the SMS service type:

no smstype

Specifying the Trading Code

If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the trading code. To specify the trading code, in the SP instance configuration mode, use the following common:

trading-code *trading-code*

- *trading-code* – Specifies the trading code. The range is 1-7.

In the SP instance configuration mode, use the following command to cancel the trading code:

no trading-code

Specifying the Channel

If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the channel. To specify the channel, in the SP instance configuration mode, use the following common:

channel *channel-value*

- *channel-value* – Specifies the channel. The range is a-z.

In the SP instance configuration mode, use the following command to cancel the channel:

no channel

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number. To send a test message, in any mode, use the following command:

exec sms sp *sp-name* **send test-message to** *phone-number* [**test-msg-content** *content*]

- *sp-name* – Specifies the SP name.
- *phone-number* – Specifies the phone number. The range is 6 to 16 characters.

- *content* – Specifies the content of the test message. The default value is "This is a test message, please don't feedback!". The range is 1 to 64 characters.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

Viewing SMS Gateway Settings

To view the SMS gateway configurations, use the following command in any mode:

show sms service-provider [*sp-name*]

- *sp-name* – Specifies the SP instance name. If not specified, the system will show all the SP instance configurations that have already created.

Viewing SMS Statistic Information

To view the statistic information that indicates the SMS message is failed or succeed, use the following command in any mode:

show tunnel ztna *ztna-name* **smsp-statistice** [**clear**]

- *ztna-name* – Specifies an existing ZTNA instance name.
- **clear** – Clear all the statistic information.

Email Authentication

Email Authentication means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", Hillstone device, through a mail server, can automatically send a Email containing random verification code to the user after the user name and password is entered. The user must enter the random verification code received in order to log in the ZTNA server and access intranet resources.

Configurations of Email authentication on ZTNA server include:

- Configuring the Email Address
- Specifying the Email Server
- Configuring the Verification Code Length
- Configuring the Lifetime of Email Verification Code
- Configuring the Sender Name
- Configuring the Email Verification Content

Configuring the Email Address

Users can receive the verification code via Email address configured on a local server or a Radius server.

When receiving the verification code via Email address configured on a local server, to configure the Email address, in the user configuration mode, use the following command:

email *email-address*

- *email-address* - Specifies the Email address used to receive the verification code. The range is 1 to 127 characters.

In the user configuration mode, use the **no email** command to cancel the specified Email address.

When receiving the verification code via Email address configured on a Radius server, users need to configure the Email address on the Radius server. Take FreeRadius as an example:

```
"test1" Cleartext-Password: ="123456"
Login-LAT-Group="radiusgroup1",
Hillstone-user-type=16,
Hillstone-user-vsys-id=0,
Hillstone-user-login-type=63,
Hillstone-user-admin-privilege=4294967295,
Hillstone-user-email=user-test@hillstonenet.com ( Add the
```

```
attribute value of Hillstone-user-email in "etc/-
freeradius/users".)
```

Specifying the Email Server

To specify the existing Email server which the Email address that used to send the verification code is configured on, in the ZTNA instance configuration mode, use the following command:

email-auth smtp-server *smtp-server-name*

- *smtp-server--name* - Specifies the existing Email server. The range is 1 to 31 characters.

In the ZTNA instance configuration mode, use the **no email-auth smtp-server** command to cancel the specified Email server.

Configuring the Verification Code Length

To specify the length of the Email verification code, in the ZTNA instance configuration mode, use the following command:

email-auth verification-code-length*length*

- *length* - Specifies the length of the Email verification code. The range is 4 to 8 characters. The default value is 8.

In the ZTNA instance configuration mode, use the **no email-auth verification-code-length** command to restore the default value.

Configuring the Lifetime of Email Verification Code

Each Email verification code has a period of validity. If the user neither types the code within the period nor applies for a new code, ZTNA server will disconnect the connection.

To configure the lifetime of the Email verification code, in the ZTNA instance configuration mode, use the following command:

email-auth expiration*value*

- *value* – Specifies the lifetime of the Email verification code. The range is 1 to 10 minutes. The default value is 10.

In the ZTNA instance configuration mode, use the **no sms-auth expiration** command to restore the default value.

Configuring the Sender Name

To specify a verification code sender name to display in the Email content, in the ZTNA instance configuration mode, use the following command:

email-auth sender-name*name*

- *name* - Specifies a verification code sender name to display in the Email content. The range is 1 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended to configure the sender name.

In the ZTNA instance configuration mode, use the **no email-auth sender-name** command to restore the default value.

Configuring the Email Verification Content

To specify the Email verification content, in the ZTNA instance configuration mode, use the following command:

email-auth message-content*content*

- *content* - Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the user name) and " $ VRFYCODE" (This parameter is used to get the verification code). The range is 18 to 128 characters. The default content is "ZTNA user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".

In the ZTNA instance configuration mode, use the **no email-auth message-content** command to restore the default content.

Configuring Single Packet Authorization (SPA)

Single Packet Authorization (SPA) is a universal access technology concept. Its main purpose is to hide the host's port number and therefore the service running on it will be hidden. The system will open the port only for packets carrying expected information.

The ZTNA device supports enabling the SPA function and hiding the ZTNA service IP address and port number. ZTNA client also needs to enable the SPA function and pass the authorization before establishing a connection to the ZTNA device. After SPA is configured, the SPA process for ZTNA users logging in through the ZTNA client is as follows:

1. ZTNA client sends knock packets to ZTNA device with the knock port number being the destination port number.
2. ZTNA device checks the destination IP address of the knock packets. If the destination IP address is not a configured hidden IP address, it will be discarded. If it is a configured hidden IP address, ZTNA device will verify it and generate a permit entry with the destination IP address, destination port number and source IP address.
3. ZTNA client sends ZTNA connection requests.
4. ZTNA device checks the requested IP address and port number. If they are hidden IP address and port number, ZTNA device will search for the matched permit entry. If a matched permit entry is found, the connection request is accepted. Otherwise, the request will be discarded.

Enabling/Disabling SPA

By default, the SPA function is disabled.

To enable or disable the SPA function, in the global configuration mode, use the following command:

- Enabling: **spa enable**
- Disabling: **no spa enable**

Configuring Local Knock Port

Local knock port is where the ZTNA device listens for knock packets. The default knock port is 60001.

To configure the local knock port number, in the global configuration mode, use the following command:

spa knock-port *port-number*

- *port-number* - Specifies the local knock port number. The value range is 1025 to 65535. The default value is 600001.

In the global configuration mode, use the following command to restore the local knock port number.

no spa knock-port

Configuring the Hidden IP and Port Number

The SPA function takes effect when it is enabled and configured with the hidden IP address and port number. When SPA is disabled or enabled but no configured with a hidden IP and port number, the ZTNA device will not perform single packet authorization on clients no matter whether the clients have SPA enabled.

To configure the hidden IP address and port number, in the global configuration mode, use the following command:

spa hide service-ip *ip-address* **port** *port-number* **vrouter** *vrouter-name* [**description** *description*]

- *ip-address* - Specifies the IPv4 address to be hidden.
- *port-number* - Specifies the port number to be hidden. The range is 1 to 65535.

- *vrouter-name* - Specifies the virtual router that the interface of the hidden IP address belongs to.
- *description* - Specifies the description. The range is 1 to 63 characters.

Repeat this command to add more pieces of hidden IP addresses and port numbers.

To delete the specified hidden IP address and port number, in the global configuration mode, use the following command:

no spa hide service-ip *ip-address* **port** *port-number* **vrouter** *vrouter-name*

Viewing SPA Configuration Information

To view SPA configuration information, in any mode, use the following command:

show spa

Viewing SPA Permit Entries

To view SPA permit entries, in any mode, use the following command:

show spa-entry

Managing Endpoint Tag Logs

The system support management of endpoint tag logs by using the endpoint tag log function.

Enabling/Disabling Endpoint Tag Log

By default, the endpoint tag log function is enabled.

To enable or disable the endpoint tag log function, in the global configuration mode, use the following command:

- Enable: **logging endpoint-tag on**
- Disable: **no logging endpoint-tag on**

Clearing Endpoint Tag Logs

To clear endpoint tags, in the global configuration mode, used the following command:

clear logging endpoint-tag

Sending Endpoint Tag Logs

After the endpoint tag logging function is enabled, the system will send the endpoint tag logs to the memory buffer by default. You can configure the system to send them to other destinations as required. You can configure multiple destinations.

To configure the system to send endpoint tag logs to the specified destination, in the global configuration mode, use the following command:

logging endpoint-tag to {**console** | **syslog** | **localdb** | **buffer** [**size** *buffer-size*] }

- **console** - Sends the endpoint tag logs to the console.
- **syslog** - Sends the endpoint tag logs to the syslog server. For configuration information about the syslog server, refer to Configuring a Syslog Server.

- **localdb** - Sends the endpoint tag logs to the local database. Only A series (except A2200, A1800, and A1600) with hard-disk card installed and SCMs of X8180 and X25812 with hard-disk card installed support this parameter.
- **buffer** - Sends the endpoint tag logs to the memory buffer.
- **size** *buffer-size* - Specifies the memory buffer size for storing the endpoint tag logs, in bytes. The range is 4096 to 2097152. The default value is 2097152.

To disable the system from sending endpoint tag logs to the specified destination, in the global configuration mode, use the following command:

no logging endpoint-tag to {**console** | **syslog** | **localdb** | **buffer**}

Configuring Disk Storage Space Threshold

When configuring the system to send endpoint tag logs to the hard disk, you can configure a threshold for the space size occupied by the sent logs. In the global configuration mode, use the following command:

storage threshold log endpoint-tag *percent*

- *percent* - Specifies the threshold for the disk space size occupied by the sent logs. The range is 0.01 to 90, in percent. The default value is 1. When the disk space occupied by endpoint tag logs exceeds the specified threshold, the system will override the earliest logs or stopping sending new logs to the disk based on the configuration of the **storage threshold percent**command.

Configuring the Quota of Endpoint Tag Log Buffer

After configuring to send endpoint tag logs to the memory buffer, you can specify the reserved buffer quota and maximum buffer quota for endpoint tag logs in a VSYS by creating a VSYS profile. Reserved quota refers to the memory buffer value reserved for the endpoint logs; maximum quota refers to the maximum memory buffer value available to the endpoint tag logs. The root

administrator has the permission to create VSYS profiles. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.

To configure the quota of buffer for endpoint tag logs, in the VSYS profile configuration mode, use the following command:

log endpoint-tagbuffer-size max *max-num* **reserve** *reserve-num*

- **max** *max-num* **reserve** *reserve-num* – Specifies the maximum quota (**max** *max-num*) and reserved quota (**reserve** *reserve-num*) of endpoint tag logs in a VSYS.The range of reserved quota or maximum quota varies from different platforms. The reserved quota should not exceed the maximum quota.

For information about VSYS profile configuration information, refer to Creating a VSYS Profile.

Viewing Endpoint Tag Logs

To view endpoint tag logs, in any mode, use the following command:

show logging endpoint-tag

ZTNA Portal

After a ZTNA user logs in, the user terminal will be prompted with the ZTNA portal page via the default browser, displaying the applications resources to which the user is granted access and not granted access.

- When the user's authentication information and endpoint tag match the ZTNA policy whose action is Permit, the user is granted access to the application resources bound with this policy.
- When the user's authentication information matches teh ZTNA policy but the endpoint tag does not match the ZTNA policy, the user is not granted access to the application resource bound with this policy.

For an application resource to which a user is granted access, the user can click the application resource icon on the ZTNA Portal page to switch to the desired URL address. Or, the user can copy the URL address to a browser to access the application resource. For an application resource to which a user is not granted access, the user can view the reason.

The ZTNA portal page does not display the following application resources:

- Application resources that the user is not allowed to access
- Application resources that the user is allowed to access, but no hyperlink is specified when the application resource is defined

After the ZTNA Portal page is closed, the user can select "Application Resource List" from the ZTNA client menu to obtain the ZTNA Portal page again.

Other Configurations

Force Disconnecting a ZTNA User

The ZTNA server can force to disconnect with a user.

To kick out a ZTNA user, in any mode, use the following command:

exec ztna *instance-name* **kickout** *user-name*

- *instance-name* – Specifies the name of ZTNA instance.
- *user-name* – Specifies the name of user to be kicked out of the server.

To kick out all ZTNA users, in any mode, use the following command:

exec ztna *instance-name* **kickout-all-user**

- *instance-name* - Specifies the name of ZTNA instance.

Configuring the Allowed Client Types

By default, when the ZTNA instance type of the device is remote access, you are allowed to access the system with six types of ZTNA clients, which are ZTNA client for Windows, ZTNA client for Android, ZTNA client for iOS, ZTNA client for macOS, ZTNA client for Linux, and ZTNA client for ChineseOS; when the ZTNA instance type of the device is intranet access, you are allowed to access the system with three types of ZTNA clients, which are ZTNA client for Windows, ZTNA client for Linux, ZTNA client for macOS. You can configure to access the system only via the specified types of ZTNA clients as needed.

When **the ZTNA instance type of the device is remote access**, to configure client type with which you are allowed to access the system, in remote access ZTNA instance configuration mode, use the following command:

allowed-client-type {**Android** | **iOS** | **Linux** | **macOS** | **Windows** | **ChineseOS**}

- **Android** | **iOS** | **Linux** | **macOS** | **Windows**| **ChineseOS** - Specifies the allowed type of ZTNA client. The type can be ZTNA client for Windows (**Windows**), ZTNA client for Android (**Android**), ZTNA client for iOS (**iOS**), ZTNA client for macOS (**macOS**), ZTNA client for Linux (**Linux**), and ZTNA client for ChineseOS (**ChineseOS**).

To allow more types, execute the above command multiple times.

In remote access ZTNA instance configuration mode, use the command **no allowed-client-type** {**Android** | **iOS** | **Linux** | **macOS** | **Windows** | **ChineseOS**} to forbid the specified type of ZTNA client to access the system.

When **the ZTNA instance type of the device is intranet access**, to configure client type with which you are allowed to access the system, in intranet access ZTNA instance configuration mode, use the following command:

allowed-client-type {**Linux** | **macOS** | **Windows**}

- **Linux** | **macOS** | **Windows** - Specifies the allowed type of ZTNA client. The type can be ZTNA client for Windows (**Windows**), ZTNA client for macOS (**macOS**), and ZTNA client for Linux (**Linux**).

To allow more types, execute the above command multiple times.

In intranet access ZTNA instance configuration mode, use the command **no allowed-client-type** {**Linux** | **macOS** | **Windows**} to forbid the specified type of ZTNA client to access the system.

Configuring Change Password URL of the Client

The system supports to redirect to the specified page to modify the password through the configured URL on the client .

To configure the change password URL, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

change-password-url *url*

- *url* – Specifies the URL address that needs to be redirected to modify the password. The ranges is 1 to 255 characters.

To cancel the configuration, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no change-password-url

Configuring Forgot Password URL of the Client

The system supports to redirect to the specified page through the configured URL to reset the password.

To configure the forgot password URL, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

forgot-password-url *url*

- *url* – Specifies the URL address that needs to be redirected to reset the password. The ranges is 1 to 255 characters.

To cancel the configuration, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no forgot-password-url

Configuring Client Auto-Connection

The system supports to configure the client to automatically reconnect when the connection terminates.

To configure client auto-connection, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

client-auto-connect count {**number** | **unlimited**}

- **number** | **unlimited** - Specifies the number of reconnection times. **number** specifies a value in the range 0 to 1024. **unlimited** means the client does not automatically reconnect. The default value is "unlimited".

To restore to the default value, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no client-auto-connect

General Configuration

The following configurations are shared by ZTNA and SSL VPN. The configurations take effect on both ZTNA and SSL VPN.

- Configuring SSL Cipher Suite
- Allowing Password Change by Local Users
- Customizing Client Download Source
- Customizing the Background Picture of Client Download Page
- Configuring Upgrade URL for Windows Type Client
- Customizing the Page Title

Configuring SSL Cipher Suite

To configure the SSL cipher suite, in the global configuration mode, use the following command:

secure-connect ssl-cipher-list *string*

- string - Specifies the SSL cipher suite list. The default is "ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2:!RC4".

To restore to the default SSL cipher suite list, in the global configuration mode, use the following command:

no secure-connect ssl-cipher-list

Allowing Password Change by Local Users

By default, the local user is not allowed to change its password, but you can configure the device to enable password changing right for local users if they pass SSL VPN or ZTNA authentication.

To enable/disable the right for local users to change the login password, in the password control mode, use the following command:

- Enable: **allow-pwd-change**
- Disable: **no allow-pwd-change**

> **Tip:** Secure Connect client of version 1.2.0.1106 and later allows the local users to change password. Therefore, it's advised to use the latest Secure Connect client.

When the server allows the client user to change password, the user can change login password after passing SSL VPN or ZTNA authentication by the following steps:

1. Right-click the client icon in notification area of the task bar on the right-bottom corner and a menu appears.



2. Click **Changing Password** and type current password and new password into the corresponding boxes.



3. Click **OK** to save the changes.

Customizing Client Download Source

End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.

By default, the client download source on the device is the same with that on Hillstone Networks Official Website. In the application scenario where you want end users to download and use specific Secure Connect clients, such as a client of the specified version or a customized client, you can import the client into the system to overwrite the default download source on the device. You can import Windows, macOS and Linux type clients.

To import the client file from a server, in the execution configuration mode, use the following command:

import secure-connect client {**windows** | **linux** | **macos**} **from** { {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies that the client file is imported from an FTP/FTPS/SFTP server. Type the IP address of the FTP/FTPS/SFTP server, virtual router name, username and password (skip if the server can be logged in anonymously).
- **tftp server** *ip-address* - Specifies that the client file is imported from a TFTP server and specifies the TFTP server address.
- **usb0** | **usb1** - Specifies that the client file is imported from the USB disk plugged to USB0 or USB1 port.
- *file-name* – Specifies the client file. The system will check the imported file. It is recommended to import a client file downloaded from Hillstone Networks Official Website and keep the file name unchanged. Otherwise, the import might fail.

You can delete the imported client file. After deletion, the download source will be restored to the default source. In the execution configuration mode, use the following command to delete the imported client file:

exec secure-connect client {**windows** | **linux** | **macos**} **delete**

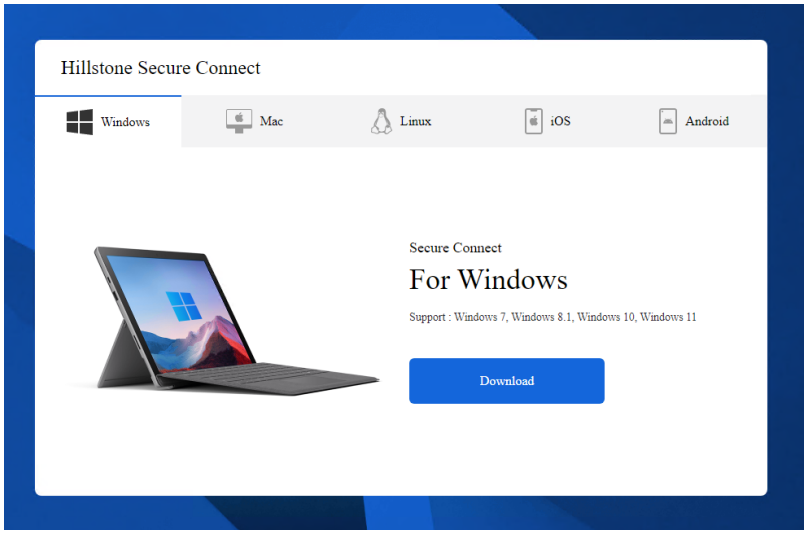
Viewing Secure Connect Client Information

In any mode, use the following command to view the information of Secure Connect clients saved in the system:

show secure-connect client-info [**windows** | **linux** | **macos**]

Customizing the Background Picture of Client Download Page

You can customize the title and background of the download address on the device. The default download page is shown as below:



To import the background picture from a server, in the execution configuration mode, use the following command:

import customize secure-connect download-webpage-background-picture from { {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name*

- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies that the background picture is imported from an FTP/FTPS/SFTP server. Type the IP address of the FTP/FTPS/SFTP server, virtual router name, username and password (skip if the server can be logged in anonymously).
- **tftp server** *ip-address* - Specifies that background picture is imported from a TFTP server and specifies the TFTP server address.
- **usb0** | **usb1** - Specifies that the background picture is imported from the USB disk plugged to USB0 or USB1 port.
- *file-name* – Specifies the picture name and picture format. The picture must be in PNG format, the resolution is recommended at 1920x *1080x, and the picture size must be less than 2MB.

To restore to the default background picture, in any mode, use the following command:

exec customize secure-connect download-webpage-background-picture default

Configuring Upgrade URL for Windows Type Client

The Windows type client checks and downloads the new version by using the configured upgrade URL. The system has a default URL that links to the official upgrade server and this URL cannot be deleted. To configure the upgrade URL, use the following command in the global configuration mode:

no secure-connect update-url

- *ip-address* – To use the intranet server to check and download the new version, enter the URL of the intranet server. You need to deploy the new version in this intranet server.

To use the default URL that links to the official upgrade server, use the following command in the global configuration mode:

no secure-connect update-url

To view the default URL that links to the official upgrade server, use the following command in any mode:

show secure-connect update-url



Notes:

- When the client version is 1.4.4.1199 or below and the StoneOS version is 5.5R1 or above, it is recommended to uninstall the previous client and login the Web page to re-install it.
- If you want the end users to download the Windows type client carried in the system image, configure this command **secure-connect update-url localhost**.
- After you import a Windows type client file using the **import secure-connect client** command, the **secure-connect update-url** configuration will not take effect.

Customizing the Page Title

By default, the title of client download page is "Hilllstone Secure Connect". To customize the title of client download page, in the global configuration mode, use the following command:

secure-connect download-web-page-title *title*

- *title* - Specifies the title of client download page. The length is 1 to 63 characters.

To delete the customized title of client download page, use the following command in the global configuration mode. After the customized title is deleted, no title will be displayed on the client download page.

no secure-connect download-web-page-title

To view the customized title of client download page, use the following command in any mode:

show secure-connect download-web-page-title

Viewing ZTNA Information

You can use the following commands to view ZTNA information:

- Show ZTNA instance information:

  show tunnel ztna [*ztna-instance-name*]

- Show ZTNA authenticated user information:

  show auth-user ztna [**interface** *interface-name* | **groupname** *group-name* | **vrouter** *vrouter-name* | **endpoint-tag** *endpoint-tag-name*]

- Show client information:

  show secure-connect client-info

- Show ZTNA user information:

  show ztna-user *instance-name* [**user** *user-name*]

- Show the license capacity of ZTNA authorized user:

  show secure-connect user capacity

- Show client upgrade URL:

  show secure-connect update-url

- Show the customized client download page title:

  show secure-connect download-web-page-title

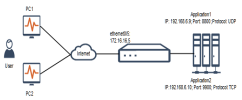
Example of Configuring ZTNA

User user1 on the external network requests to access the server on the internal network through Hillstone ZTNA.

- Endpoint state of PC1: Windows10 OS with firewall and anti-virus software installed
- Endoint state of PC2: WindowsXP OS without firewall and anti-virus software installed
- Applcation resources on Server: Application1 and Application2

Networking and Requirement

The following figure shows the networking:



Requirements:

- User user1 is allowed to access Application1 and Application 2 via PC1.
- User user1 is not granted access to Application1 and Application2 via PC2 because the terminal device state does not meet requirements.

Configuration Steps

Step 1: Create a local user

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
hostname(config-user)# exit
hostname(config)#exit
```

Step 2: Configure an access address pool

```
hostname(config)# access-address-pool pool1
hostname(config-address-pool)# address 172.18.100.10 172.18.100.200 netmask 255.255.255.0
hostname(config-address-pool)# exit
hostname(config)#
```

Step 3: Configure a ZTNA instance

```
hostname(config)# tunnel ztna ztna-access
hostname(config-tunnel-ztna-remote)# access-address-pool pool1
hostname(config-tunnel-ztna-remote)# aaa-server local
hostname(config-tunnel-ztna-remote)# interface ethernet0/5
hostname(config-tunnel-ztna-remote)# ssl-port 5588
hostname(config-tunnel-ztna-remote)# split-tunnel-route 192.168.6.0/24
hostname(config-tunnel-ztna-remote)# exit
hostname(config)#
```

Step 4: Create a tunnel interface and bind the ZTNA instance to it (the tunnel interface and address pool should be in the same IP address segment)

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# ip address 172.18.100.1/24
hostname(config-if-tun1)# tunnel ztna ztna-access
hostname(config-if-tun1)# exit
hostname(config)#
```

Step 5: Configure endpoint tags

```
hostname(config)# endpoint-tag tag1
hostname(config-endpoint-tag)# criteria-set 1
hostname(config-endpoint-tag-criteria-set)# criteria os-type windows key os-version is windows-10
```

```
hostname(config-endpoint-tag-criteria-set)# criteria os-type windows key anti-virus is installed
hostname(config-endpoint-tag-criteria-set)# criteria os-type windows key firewall is installed
hostname(config-endpoint-tag-criteria-set)# exit
hostname(config-endpoint-tag)# exit
hostname(config)#
```

Step 6: Configure application resources

```
hostname(config)# application-resource application1
hostname(config-app-res)# ip 192.168.6.9 protocol udp port 8800hostname(config-app-res)# hyperlinl http://a1a1.com
hostname(config)# application-resource application2
hostname(config-app-res)# ip 192.168.6.10 protocol tcp port 9900hostname(config-app-res)# hyperlinl http://a2a2.com
```

Step 7: Configure ZTNA policy

```
hostname(config)# ztna-rule rule1
hostname(config-ztna-policy-rule)# application-resource application1
hostname(config-ztna-policy-rule)# application-resource application2
hostname(config-ztna-policy-rule)# endpoint-tag tag1
hostname(config-ztna-policy-rule)# user local user1
hostname(config-ztna-policy-rule)# action permit
hostname(config-ztna-policy-rule)# enable
hostname(config-ztna-policy-rule)# exit
hostname(config)#
```

Step 8: User user1 accesses https://172.16.16.5:5588 in the browser of PC1 and PC2 and then downloads and installs the client for Windows on the displayed page.

Step 9: User user1 logs in the ZTNA server through the client installed on PC1 and PC2. The server address is "172.16.16.5", the port number is 5588, the user name and password are "user1" and "123456".

Step 10: On the displayed ZTNA portal page after the user logs in on PC1, Application1 and Application2 are in the accessible state. The user can click the icon to directly access the resource. On the displayed ZTNA portal page after the user logs in on PC2, Application1 and Application2 are grayed out. Clicking the icon will be prompted with a message indicating that user is not granted access to them.

Chapter 11 Traffic Management

This chapter introduces the following topics:

- iQoS
- QoS
- Load Balancing
- Session Limit

QoS /iQoS

This chapter contains iQoS(intelegent quality of service) and QoS(quality of service). The upgrading descriptions of iQoS/QoS for different versions are listed in the table below.

Product version	Description
Before version 5.5, and QoS function is not configured	After upgrading, the system uses the iQoS function by default.
Before version 5.5, and QoS function has already been configured	After upgrading, the QoS function is still enabled. But iQoS is recommended to use. For switching to iQoS, see Swichting iQoS/QoS.
Version 5.5 and above	Use the iQoS function by default.

Swichting iQoS/QoS

If you have not configured the QoS function before upgrading to version 5.5, the system will enable the iQoS function by default. You can configure iQoS function via WebUI or CLI and the QoS function will not take effect.

If you have configured QoS before upgrading the system to verion 5.5, the QoS function will still take effect. You can configure QoS function only via CLI. We recommend you to use iQoS function to control bandwidth. To switch from QoS to iQoS, in any mode, use the following command:

exec iqos enable

To switch from iQoS to QoS, in any mode, use the following command:

exec iqos disable

iQoS

The system provides intelligent quality of service (iQoS) which guarantees the customer's network performance, manages and optimizes the key bandwidth for critical business traffic, and helps the customer greatly in fully utilizing their bandwidth resources.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.

iQoS is controlled by license. To use iQoS, apply and install the iQoS license.

iQoS Implement

The packets are classified and marked after entering the system from the ingress interface. For the classified and marked traffic, the system will smoothly forward the traffic through shaping mechanism, or drop the traffic through policing mechanism. If selecting shaping mechanism to forward the traffic, the congestion management and congestion avoidance mechanisms give different priorities to different types of packets so that the packets of higher priority can pass the gateway earlier to avoid network congestion.

In general, implementing iQoS includes:

- Classification and marking mechanism: Classification and marking is the process of identifying the priority of each packet. This is the first step of iQos.
- Policing and shaping mechanisms: Policing and shaping mechanisms are used to identify traffic violation and make responses. The policing mechanism checks traffic in real time, and takes immediate actions according to the settings when it discovers violation. The shaping mechanism works together with queuing mechanism. It makes sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly.
- Congestion management mechanism: Congestion management mechanism uses queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work.
- Congestion avoidance mechanism: Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic.

Function Overview

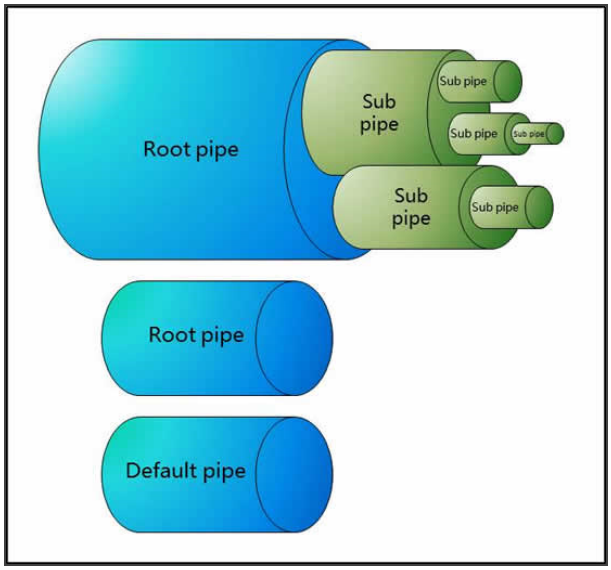
By configuring pipes, the devices implement iQos. Pipe, which is a virtual concept, represents the bandwidth of transmission path. The system classifies the traffic by using the pipe as the unit, and control the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe pre-defined by the system.

Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- Traffic matching conditions: Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. The system will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe.
- Traffic management actions: Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. Forward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

Multiple-level Pipes

To provide flexible configurations, the system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:

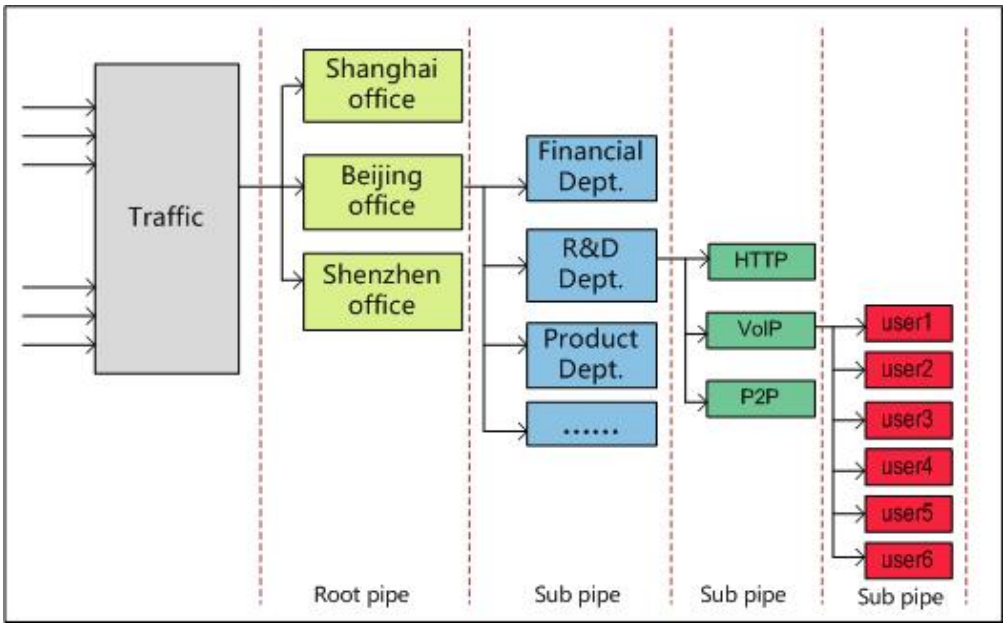


- You can create multiple root pipes that are independent individually. At most three levels of sub pipes can be nested to the root pipe.
- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.
- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belongs to this root pipe will inherit the configurations of the traffic direction set on the root pipe.
- The root pipe that is only configured the backward traffic management actions cannot work.

The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

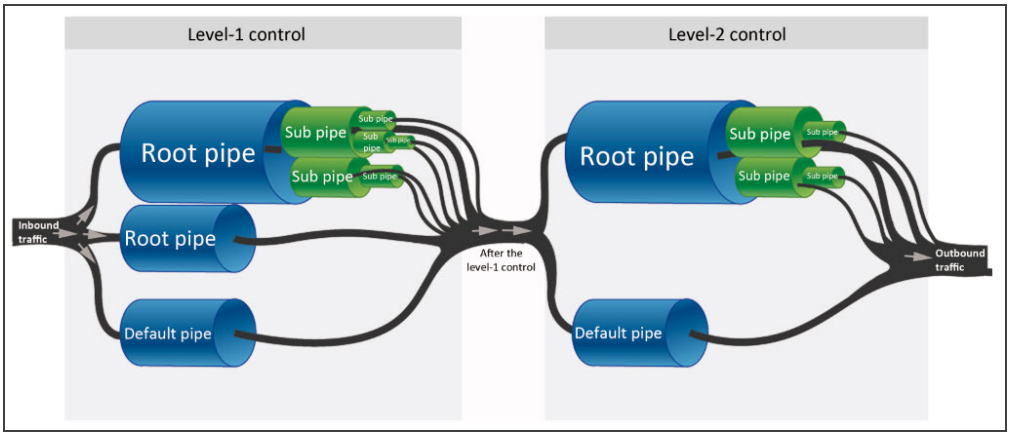
1. Create a root pipe to limit the traffic of the office located in Beijing.
2. Create a sub pipe to limit the traffic of its R&D department.
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.

4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Process of iQos

The system supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then the system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flows into the device, the process of iQos is shown as below:



According to the chart above, the process of traffic control is described below:

1. The traffic first flows into the level-1 control, and then the system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list. After the traffic flows into the root pipe, the system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.
2. According to the traffic management actions configured for the pipes, the system manages and controls the traffic that matches the traffic matching conditions.
3. The traffic dealt with by level-1 control flows into the level-2 control. The system manages and controls the traffic in level-2 control. The principle of traffic matching, management and control are the same as the one of the level-1 control.
4. Complete the process of iQos.

Configuring iQoS

By using pipes, devices implement QoS. Using pipes includes the following sections:

1. Create the traffic matching conditions, which are used to control the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.
2. Create a white list according to your requirements. The system will not control the traffic in the white list. Only root pipe and the default pipe support the white list.
3. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.



Notes:

- For SG-6000-X20812, SG-6000-X20803 and SG-6000-X8180, the QSM module is not supported, you can install the SIOM to process QoS (make sure that the device has installed iQoS license).
- For SG-6000-X9180 and SG-6000-X10800, when there is no QSM installed, you can install the IOM/SIOM to process QoS (make sure that the device has installed iQoS license). If you install the IOM to process QoS, the QoS doesn't support the shaping mode. If you install the SIOM to process QoS, the QoS is the same as the QoS function by installing the QSM module.
- For SG-6000-X9180 and SG-6000-X10800, when the device is installed with both QSM and IOM, QSM will take effect first for QoS.

Specifying Traffic Control Level

Specify which traffic control level you want to enter, first-leve traffic control or second-level traffic control and enter the traffic control mode. You can create pipes to manage the traffic. In the global configuration mode, use the following command:

qos-engine {**first** | **second**}

- **first** – Enter the traffic control mode of the first-level traffic control.
- **second** – Enter the traffic control mode of the second-level traffic control.

Enabling/Disabling Traffic Control Level/Root Pipe/Sub Pipe

To enable/disable the traffic control level, in the traffic control mode of the specified level, use the following command:

- Disable the traffic control level: **disable**
- Enable the traffic control level: **no disable**

To enable/disable the root pipe, in the root pipe configuration mode of the specified root pipe, use the following command:

- Disable the root pipe: **disable**
- Enable the root pipe: **no disable**

To enable/disable the sub pipe, in the sub pipe configuration mode of the specified sub pipe, use the following command:

- Disable the sub pipe: **disable**
- Enable the sub pipe: **no disable**



Notes: The disabled levels or pipes will not take effect during the iQoS process. The unavailable pipes will not take effect as well.

Enabling/Disabling NAT IP Matching

You can enable the NAT IP matching function in the traffic control mode of the specified level as needed.After it is enabled, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is successful, system will limit the speed of these IP addresses. To enable the NAT IP matching, in the traffic control mode of the specified level, use the following command:

match-nat-ip enable

To disable the NAT IP matching, in the traffic control mode of the specified level, use the command **no match-nat-ip enable**.



Notes: Before enabling NAT IP matching, you must config the NAT rules. Otherwise, the configuration will not take effect.

Creaing a Root Pipe

In the traffic control mode, use the following command to create a root pipe and enter the root pipe configuration mode. If the name of the root pipe already exists, the system will enter the root

pipe configuration mode directly.

root-pipe {pipe-name | default}

- **pipe-name** – Enter the name of the newly created root pipe.
- **default** – Enter the default pipe.

In the traffic control mode, use the following command to delete a root pipe:

no root-pipe pipe-name



Notes:

- The name of the root pipe cannot exceed 63 characters.
- A root pipe can nest up to 3 level sub pipes.
- The default pipe cannot be deleted.

After entering the root pipe configuration mode, you can configure the following configurations:

- Enable/Disable the root pipe
- Configure the traffic matching conditions of the root pipe
- Create a traffic whit list of the root pipe
- Configure the traffic management action of the root pipe
- Configure the traffic control mode of the root pipe
- Specify a schedule for the root pipe
- Create a sub pipe

Creating a Sub Pipe

To create a sub pipe and enter the sub pipe configuration mode, use the following command in the pipe configuration mode. If the sub pipe name already exists, the system will enter the sub

pipe configuration mode directly.

pipe *pipe-name*

- *pipe-name* – *Enter the name of the newly created sub pipe.*

In the pipe configuration mode, use the following command to delete the created sub pipe:

no pipe *pipe-name*



Notes:

- The name of the pipe cannot exceed 63 characters.
- To delete the sub pipe, you need to execute the command **no pipe** *pipe-name* in the pipe configuration mode of its parent pipe.

In the sub pipe configuration mode, you can configure the following options:

- Enable/Disable the sub pipe
- Configure the traffic matching conditions of the sub pipe
- Create a sub pipe

Configuring a Traffic Matching Condition

Before configuring a traffic matching condition, you need to first create a traffic matching condition and then enter the traffic maching condition configuration mode. If the ID already exists, the system will enter the traffic matching condition configuration mode directly. Without the ID specified, the system will create a traffic matching condition and enter its configuration mode. To create a traffic matching condition and enter its configuration mode, use the following command in the pipe configuration mode:

pipe-map [*id*]

- *id* – Enter the ID of the traffic matching condition.

Use the **no pipe-map** [*id*] command to delete the specified traffic matching condition.

After entering the traffic matching condition configuration mode, use the following command to configure the traffic matching condition:

- Specify the source zone name of the traffic: **src-zone***src-zone*
- Delete the source zone name of the traffic: **no src-zone**
- Specify the destination zone name of the traffic: **dst-zone***dst-zone*
- Delete the destination zone name of the traffic: **no dst-zone**
- Specify the source host name of the traffic: **src-host***host-name*
- Delete the source host name of the traffic: **no src-host***host-name*
- Specify the destination host name of the traffic: **dst-host***host-name*
- Delete the destination host name of the traffic: **no dst-host***host-name*
- Specify the source IP address (IPv4 or IPv6) of the traffic: **src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- Delete the source IP address (IPv4 or IPv6) of the traffic: **no src-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- Specify the destination IP address (IPv4 or IPv6) of the traffic: **dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- Delete the destination IP address (IPv4 or IPv6) of the traffic: **no dst-ip** {*ip/netmask* | *ip-address netmask* | *ipv6-address/prefix* }
- Specify the source IP address range (IPv4 or IPv6)of the traffic: **src-range***min-ip*[*max-ip*]
- Delete the source IP address range (IPv4 or IPv6)of the traffic: **no src-range***min-ip* [*max-ip*]
- Specify the destination IP address range (IPv4 or IPv6)of the traffic: **dst-range***min-ip* [*max-ip*]

- Delete the destination IP address range (IPv4 or IPv6)of the traffic: **no dst-range***min-ip* [*max-ip*]
- Specify the ingress interface name of the traffic: **ingress-if** *interface-name*
- Delete the ingress interface name of the traffic: **no ingress-if***interface-name*
- Specify the egress interface name of the traffic: **egress-if***interface-name*
- Delete the egress interface name of the traffic: **no egress-if***interface-name*
- Specify the source address entry (IPv4 or IPv6)of the traffic: **src-addr***address-book*
- Delete the source address entry (IPv4 or IPv6)of the traffic: **no src-addr***address-book*
- Specify the destination address entry (IPv4 or IPv6)of the traffic: **dst-addr***address-book*
- Delete the destination address entry (IPv4 or IPv6)of the traffic: **no dst-addr***address-book*
- Specify the user and its AAA server: **user***AAA-server user-name*
- Delete the users and its AAA server: **no user***AAA-server user-name*
- Specify the user group and its AAA server: **user-group***AAA-server usergroup-name*
- Delete the users group and its AAA server: **no user-group***AAA-serverusergroup-name*
- Specify the application or application group, including pre-defined application and user-defined application: **application***app-name*
- Delete the application or application group, including pre-defined application and user-defined application: **no application***app-name*
- Specify the name of the service or service group: **service***service-name*
- Delete the name of the service or service group: **no service***service-name*
- Specify the ToS field: **tos***tos-value*

- Delete the ToS field: **no tos***tos-value*
- Specify the VLAN information: **vlan***vlan-id*
- Delete the VLAN information: **no vlan***vlan-id*
- Specify the URL category: **url-category***category-name*
- Delete the URL category: **no url-category***category-name*
- Specify the TrafficClass field: **traffic-class***traffic-class-value*
- Delete the TrafficClass field: **no traffic-class***traffic-class-value*



Notes: iQoS does not support to configure a tunnel interface. To limit the speed of tunnel traffic, use the method of policy-based IPSec VPN. For more information, see "Configuring an IPsec VPN" on Page 1403。

Configuring a Traffic White List

After configuring a traffic white list, the system will not manage the traffic in the white list. You can specify a whit list for the root pipe or the default pipe.

Before configuring a white list, you need to first create a whilte list and then enter the white list configuration mode. If the specified ID already exists, the system will directly enter the white list configuration mode. If you do not specify an ID, the system wil create a white list and enter its configuration mode. To create a white list and enter the white list configuration mode, in the pipe configuration mode, use the following command:

exception-map [*id*]

- *id* – Enter the ID of the white list.

Use the **no exception-map** [*id*] command to delete the specified white list.

After entering the white list configuration mode, use the following command to configure the white list:

- Specify the source zone name of the traffic: **src-zone***src-zone*
- Delete the source zone name of the traffic: **no src-zone**
- Specify the destination zone name of the traffic: **dst-zone***dst-zone*
- Delete the destination zone name of the traffic: **no dst-zone**
- Specify the ingress interface name of the traffic: **ingress-if** *interface-name*
- Delete the ingress interface name of the traffic: **no ingress-if** *interface-name*
- Specify the egress interface name of the traffic: **egress-if** *interface-name*
- Delete the egress interface name of the traffic: **no egress-if** *interface-name*
- Specify the source IP address of the traffic: **src-ip** {*ip/netmask | ip-address netmask*}
- Delete the source IP address of the traffic: **no src-ip** {*ip/netmask | ip-address netmask*}
- Specify the destination IP address of the traffic: **dst-ip** {*ip/netmask | ip-address netmask*}
- Delete the destination IP address of the traffic: **no dst-ip** {*ip/netmask | ip-address netmask*}
- Specify the user and its AAA server: **user** *AAA-server user-name*
- Delete the users and its AAA server: **no user** *AAA-server user-name*
- Specify the user group and its AAA server: **user-group** *AAA-server usergroup-name*
- Delete the users group and its AAA server: **no user-group** *AAA-server usergroup-name*
- Specify the application or application group, including pre-defined application and user-defined application: **application** *app-name*
- Delete the application or application group, including pre-defined application and user-defined application: **no application** *app-name*
- Specify the name of the service or service group: **service** *service-name*

- Delete the name of the service or service group: **no service** *service-name*
- Specify the ToS field: **tos** *tos-value*
- Delete the ToS field: **no tos** *tos-value*
- Specify the VLAN information: **vlan** *vlan-id*
- Delete the VLAN information: **no vlan** *vlan-id*
- Specify the URL category: **url-category** *category-name*
- Delete the URL category: **no url-category** *category-name*

Configuring the trigger threshold for the maximum floating bandwidth

Configure the upper and lower thresholds of the bandwidth utilization for a root pipe. When a root pipe's bandwidth utilization is lower than the lower threshold, the maximum bandwidth of sub pipes is the configured maximum floating bandwidth. If a root pipe's bandwidth utilization is higher than the upper threshold, sub pipes apply the configured maximum bandwidth of each IP/user. To configure the trigger threshold for the maximum floating bandwidth, in the root pipe configuration mode, use the following command:

flex-qos low-water-mark *value* **high-water-mark** *value*

- **low-water-mark** *value* – Specifies the lower threshold of the bandwidth utilization for a root pipe. The range is 20%-75%. The default lower threshold is 40%.
- **high-water-mark** *value* – Specifies the upper threshold of the bandwidth utilization for a root pipe. The range is 76%-90%. The default upper threshold is 80%.

In the root pipe configuration mode, use **no flex-qos** command to restore to the default value.

Configuring Traffic Management Actions for a Root Pipe

To configure traffic management actions for a root pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* **[per-ip-min** *min-value***] [per-ip-max** *max-value* **[delay** *delay-time***] [flex-per-max {Kbps | Mbps}**

value]] [per-ip-using {src-ip | dst-ip}] [tos-marking *tos-value*] [traffic-marking *traffic-class-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* [per-user-min *min-value*] [per-user-max *max-value* [delay *delay-time*] [flex-per-max {Kbps | Mbps} *value*]] [tos-marking *tos-value*] [traffic-marking *traffic-class-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* average-using {src-ip | dst-ip | user} [tos-marking *tos-value*] [traffic-marking *traffic-class-value*] [mode aggressive [strength-level *level-value*]] [priority *value*]

- forward – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- backward -Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.
- bandwidth {Kbps | Mbps | Gbps} - Specify the minimum bandwidth of the pipe. When selecting Kbps, the bandwidth ranges from 32 to 100,000,000. When selecting Mbps, the bandwidth ranges from 1 to 100,000. When selecting Gbps, the bandwidth ranges from 1 to 100.
- per-ip-min *min-value* - Specify the minimum bandwidth of each IP. The value ranges from 32Kbps to 1,000,000Kbps.
- per-ip-max *max-value* - Specify the maximum bandwidth of each IP. The value ranges from 32Kbps to 1,000,000Kbps.
- per-ip-using {src-ip|dst-ip} - Limit the bandwidth to each source IP address or destination IP address. This configuration can take effect after you have configured the per-ip-min min-value and per-ip-max max-value parameters.

- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 10,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 10,000Mbps.
- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 10,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 10,000Mbps.
- **delay** *delay-time* – Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
- **flex-per-max** {**Kbps** | **Mbps**} – Specifies the maximum floating bandwidth, which should be larger than the maximum bandwidth of each IP/user. The maximum floating bandwidth is triggered when a root pipe's bandwidth utilization is lower than the lower threshold. If Kbps is selected, the value range is from 32Kbps to 1000,000Kbps. If Mbps is selected, the value range is from 1Mbps to 1000Mbps.
- **tos-marking** *tos-value* - Specify the TOS filed.
- **traffic-marking** *traffic-class-value*] - Specifies the value of the TrafficClass field for IPv6 traffic, ranging from 0-255. The TrafficClass field value of IPv6 traffic matched is set to the specified value.
- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device.When the peer quench function is enabled,the default value of strength-level is 1,whose value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.

- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.
- **average-using** {**src-ip** | **dst-ip** | **user**} - Allocate the bandwidth equally to each source IP address or each destination IP address in the pipe.

Use the no form of the above command to delete the traffic management actions of a specified direction.



Notes:

- You cannot limit the bandwidth to each user and each IP address at the same time.
- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

Configuring Traffic Management Actions for a Sub Pipe

To configure traffic management actions for a sub pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *value* **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* [**per-ip-min** *min-value*] [**per-ip-max** *max-value* [**delay** *delay-time*]] [**flex-per-max** {**Kbps** | **Mbps**} *value*] [**per-ip-using** {**src-ip** | **dst-ip**}] [**tos-marking** *tos-value*] [**traffic-marking** *traffic-class-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *min-value* **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* [**per-user-min** *min-value*] [**per-user-max** *max-value* [**delay** *delay-time*]] [**flex-per-max** {**Kbps** | **Mbps**} *value*] [**tos-**

marking *tos-value*] [**traffic-marking** *traffic-class-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

- **forward** – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- **backward** - Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.
- {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**} *value* - Specify the minimum bandwidth of the pipe, or set the reserved bandwidth of the pipe. `min` represents the minimum bandwidth and **reserve-bandwidth** represents the reserved bandwidth. When configuring the minimum bandwidth or the reserved bandwidth, **percent**represents that the minimum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**, the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps** the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.
- **max** {**percent** | **Kbps** | **Mbps** | **Gbps**} *max-value* - Specify the maximum bandwidth of the pipe or the maximum percentage of its parent pipe. **percent**represents that the maximum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**, the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.
- **per-ip-min** *min-value* - Specify the minimum bandwidth of each IP address. When selecting Kbps, the values ranges from 32Kbps to 10,000,000Kbps. When selecting Mbps, the value ranges from 1Mbps to 10,000Mbps.
- **per-ip-max** *max-value* - Specify the maximum bandwidth of each IP address. When selecting Kbps, the values ranges from 32Kbps to 10,000,000Kbps. When selecting Mbps, the value ranges from 1Mbps to 10,000Mbps.
- **per-ip-using** {**src-ip**|**dst-ip**} - Specify which kind of IP addresses will be controlled by the bandwidth limit you configured by the per-ip-max max-value and per-ip-min min-value

commands. src-ip represents the source IP address, and dst-ip represents the destination IP address.

- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. The values ranges from 32Kbps to 1,000,000Kbps.
- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. The values ranges from 32Kbps to 1,000,000Kbps.
- **delay** *delay-time* – Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
- **flex-per-max** {**Kbps** | **Mbps**} – Specifies the maximum floating bandwidth, which should be larger than the maximum bandwidth of each IP/user. The maximum floating bandwidth is triggered when a root pipe's bandwidth utilization is lower than the lower threshold. If Kbps is selected, the value range is from 32Kbps to 1000,000Kbps. If Mbps is selected, the value range is from 1Mbps to 1000Mbps.
- **tos-marking** *tos-value* - Specify the TOS filed.
- **traffic-marking** *traffic-class-value*] - Specifies the value of the TrafficClass field for IPv6 traffic, ranging from 0-255. The TrafficClass field value of IPv6 traffic matched is set to the specified value.
- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device. When the peer quench function is enabled,the default value of strength-level is 1,which value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.

- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.



Notes:

- You cannot limit the bandwidth to each user and each IP address at the same time.
- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

Configuring a Traffic Control Mode for a Root Pipe

A root pipe has the following three traffic control modes:

- Shape mode: After configuring this mode, the system can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority schedule for the traffic within the root pipe.
- Police mode: After configuring this mode, the system will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority schedule, and cannot guarantee the minimum bandwidth.
- Stat mode: After configuring this mode, the system will monitor the matched traffic, generate the statistics, and will not control the traffic.

Bandwidth borrowing: All sub pipes in a root pipe can lend the idle bandwidth to the pipes that are lack of bandwidth. The prerequisite is the bandwidth of themselves are enough to forward their traffic.

Priority schedule: When there is traffic congestion, the system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and the system will deal with the traffic in order of precedence.

By default, a root pipe uses the policing mode. To configure the traffic control mode of a root pipe, use the following command in the root pipe configuration mode:

qos-mode {**police** | **shape** | **stat**}

- **police** – Use the policing mode.
- **shape** – Use the shping mode.
- **stat** – Use the monitoring mode.

Configuring a Schedule for a Root Pipe

You can specify a schedule entry for a root pipe and this root pipe will take effect within the specified time. To specify a schedule for a root pipe, in the root pipe configuration mode, use the following command:

schedule *schedule-name*

- schedule-name – Specify the name of the schedule entry.

Use the **no schedule** *schedule-name* command to cancel the schedule configuration.



Tip: For more information on creating a schedule, see "Configuring Schedule" in the the "System Management".

Configuring a Schedule for a Sub Pipe

You can specify a schedule entry for a sub pipe and this sub pipe will take effect within the specified time. To specify a schedule for a sub pipe, in the sub pipe configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* – Specify the name of the schedule entry.

Use the **no schedule** *schedule-name* command to cancel the schedule configuration.



Tip: For more information on creating a schedule, see "Configuring Schedule" in the "System Management".

Binding a Root Pipe to the QSM Moduel

When configuring iQos for SG-6000-X10800, you can bind the root pipe to the specified QSM model, which can improve the accuracy of traffic limit. To bind a root pipe to the QSM module, use the following command in the root pipe configuration mode:

bind slot {*number*}

- *number* – Specify the slot number where the QSM module locates.

Viewing Configurations of Traffic Control Levels and Pipes

To view the configurations of traffic control levels and pipes, use the following command in any mode:

show qos-engine {**first** | **second**} [**root-pipe** *pipe-name*]

- **first** – View the configurations of the first-leve traffic control.
- **second** - View the configurations of the second-leve traffic control.
- **root-pipe** *pipe-name* - View the configurations of the specified root pipe.

Configuring Threshold Alarm

The system supports to configure threshold alarm of the pipeline utilization. After the function is enabled and the alarm threshold is specified, when the pipeline usage reaches or exceeds the specified alarm threshold, the system will record a warning level event log. For the same pipeline, the system records the event log at an interval of 10 seconds.

Enabling/Disabling Threshold Alarm

By default, threshold alarm is enabled. To enabling/disabling threshold alarm, in the global configuration mode, use the following commands:

qos-threshold-switch {**on** | **off**}

- **on** - Enable threshold alarm.
- **off** - Disable threshold alarm.

Specifying the Alarm Threshold

To specify the alarm threshold, n the global configuration mode, use the following command:

qos-threshold *threshold*

- *threshold* - Specify the alarm threshold. The unit is percent. The range is from 50 to 100. The default value is 80.

Show the Status of Threshold Alarm

To show the status of threshold alarm, in any mode, use the following command:

show qos-threshold

QoS

Overview

QoS (Quality of Service) is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. QoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.

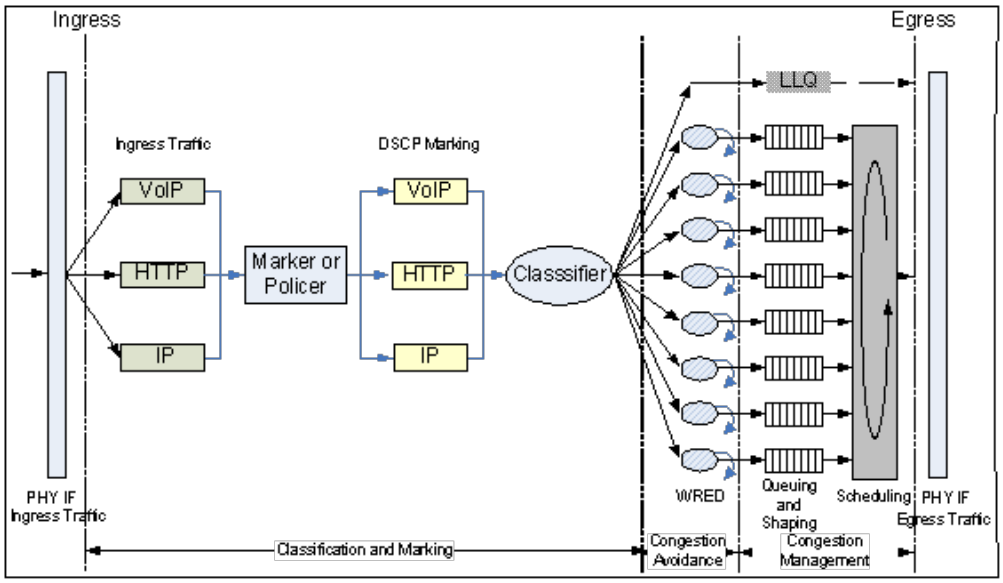
QoS is an assembly of techniques for controlling bandwidth, delay, flapping, and packet loss in a network. All QoS mechanisms are designed to affect at least one or even all the above features.

QoS Implementation

In general, QoS includes:

- Classification and marking mechanisms
- Policing and shaping mechanisms
- Congestion management mechanism
- Congestion avoidance mechanism

The QoS system structure is shown in the figure below.



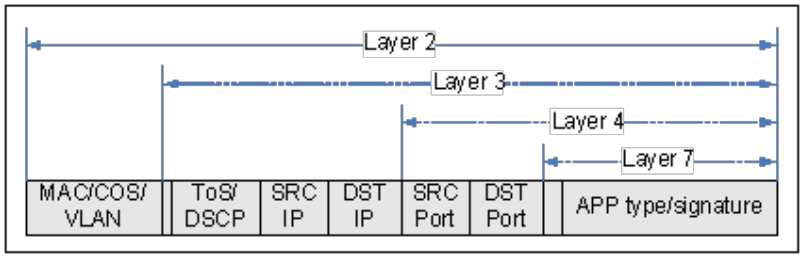
As shown in the figure above, the packets are classified and marked after entering the system from the ingress interface. During the process, the policing mechanism will drop some of the packets. Then, the packets will be categorized again according to their marks. The congestion management and congestion avoidance mechanisms give different priorities to different types of packets so that the packets of higher priority can pass the gateway earlier to avoid network congestion. Finally, the system will send packets which have been processed by QoS mechanisms out from the egress interfaces.

Classification and Marking

Classification and marking is the process of identifying the priority of each packet. This is the first step of QoS control, and should be done near the source hosts.

Classification

The packets are generally classified by their packet headers. The packet headers are examined closely by the rules specified in the figure below. The figure below shows the classification fields, and the table below lists the criteria of classification:



Layer	Description
Layer 1	Physical interface and sub-interface
Layer 2	MAC address, 802.1Q/p classification of service (CoS) bit string and VLAN mark
Layer 3	IP Precedence, DiffServ code point (DSCP) and source/destination IP address group
Layer 4	Port number (TCP or UDP)
Layer 7	Application type or application signature

Marking

The fields that can carry marks include:

- Layer 2 marking field: 802.1Q/p
- Layer 3 marking field: IP precedence and DSCP

802.1Q/p

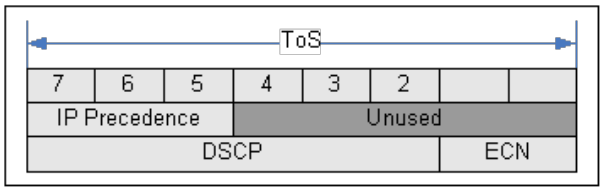
Ethernet frames are marked with 802.1p user priority (CoS) of 802.1Q header. The Layer 2 Ethernet frame has only 8 types of services (from 0 to 7), as shown in the table below:

CoS value/IP precedence	Application
7	Reserved
6	Reserved
5	Voice
4	Video Conference
3	Call Signaling
2	High-priority Data
1	Medium-priority Data
0	Best-effort Data

IP Precedence and DSCP

Similar to CoS, IP precedence can be marked with 8 types of services (0 to 7). See the table above.

DSCP (DiffServ Code Point) provides a 6-bit field for QoS marking, among which 3 bits are the same as IP precedence, and the other 3 bits are ToS fields. Thus, the DSCP value range is 0 to 63. The figure below shows the DSCP and IP precedence bits:



A DSCP value can be represented in two forms: digital and keyword. The keyword form of DSCP value is also known as Per-Hop Behavior (PHB). At the time of writing there are 3 types of defined PHBs: Best-Effort (BE or DSCP 0), Assured Forwarding (AF) and Expedited Forwarding (EF). For more information, see RFC2547, 2597 and 3246. The DSCP value plays a significant role in the subsequent QoS processing.

Policing and Shaping

QoS policing and shaping mechanisms are used to identify traffic violation and make responses. Policing and shaping adopts the same algorithms for identifying traffic violation, but they make different responses.

The policing mechanism checks traffic in real time, and takes immediate actions according to the settings when it discovers violation. For example, the policing mechanism can identify if the traffic payload exceeds the defined traffic flow rate, and then decide to re-mark or drop the excessive parts. It can control the traffic of both inbound and outbound directions.

The shaping mechanism works together with queuing mechanism. It sends all traffic to one interface and make sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly. The shaping mechanism is typically applied to the outbound direction.

The differences between policing and shaping are listed in the table below.

Policing	Shaping
TCP re-connection due to packets being dropped	Typically traffic delay, but seldom TCP re-connection
Inflexible and unadaptable	The queuing mechanism can reduce network congestion
Ingress interface and egress interface control	Egress interface control

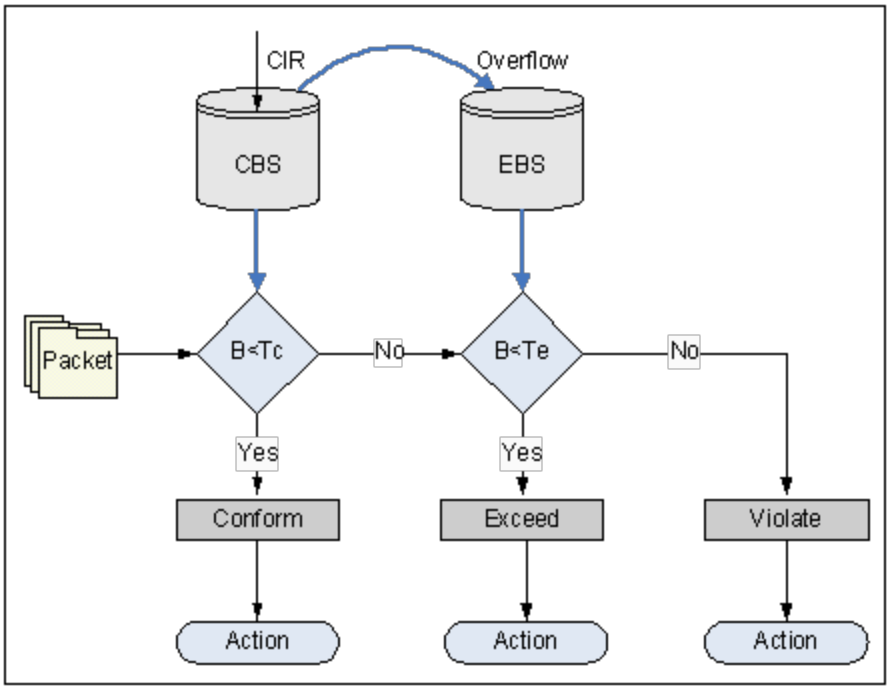
Policing	Shaping
No cache or rate limit	Cache and rate limit

Token Bucket Algorithm

Hillstone devices use token bucket algorithm to determine if the network traffic has violated rules. Token bucket is an abstract container that holds tokens. The system puts tokens into the bucket at a defined rate. When the bucket is full, the tokens will overflow it and the number of tokens in the bucket will not change. The token bucket uses its tokens to transmit packets. When the bucket has enough tokens to transmit the packets, the bucket is known as conforming to the rule, otherwise it excesses the rule. The parameters in traffic evaluation include:

- CIR (Committed Information Rate): The rate of placing tokens, i.e. the average rate of data transmission.
- CBS (Committed Burst Size): The size of the first token bucket, i.e. the maximum traffic volume allowed in each burst. This value must be larger than the length of the largest packet. This token bucket is abbreviated as C-bucket.
- EBS (Excess Burst Size): The size of the second token bucket, i.e. the maximum value of exceeded traffic allowed. This token bucket is abbreviated as E-bucket.

When evaluating traffic, the control operations may vary from different situations which include: 1) C-bucket has enough tokens; 2) C-bucket tokens are insufficient but E-bucket is sufficient; 3) both C-bucket and E-bucket do not have enough tokens. The figure below illustrates the double token buckets algorithm:



As shown above, B is the size of packet; Tc is the number of CBS tokens; Te is the number of EBS tokens.

When the CBS is larger than the packet size, the packet conforms and will be processed according to system settings; when the CBS is smaller than the packet size, the system will check EBS; if the EBS is larger than the packet size, the packet exceeds and will be processed according to system settings; but if the EBS is smaller than the packet size, the packet violates the rule and will be processed according to other settings.

Congestion Management

Congestion management mechanism is one of the most important tools in QoS control. It uses queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work. Hillstone devices support class-based weighted fair queuing (CBWFQ) and low latency queuing (LLQ).

- CBWFQ: Allows users to configure the minimum bandwidth of a certain type of traffic.
- LLQ: The algorithm combination of PQ, CQ and WFQ. LLQ is usually used in voice and interactive video. During configuration, all the applications of LLQ type can occupy no more than 33% of the total bandwidth.

Congestion Avoidance

Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic. On Hillstone devices, the congestion avoidance mechanism is implemented by the WRED algorithm.

Configuring QoS

To implement QoS on the Hillstone device, first you need to configure a QoS profile, and then apply the QoS profile to an interface. You can apply multiple QoS profiles to a single interface. To configure QoS, take the following steps:

1. Configure a class. The process of identifying and classifying traffic. The class defines the traffic that will be matched on the device, so that the device can classify the traffic.
2. Configure a QoS profile. The QoS profile defined actions for the matched traffic, including policing, shaping, congestion management, and congestion avoidance.
3. Binding the QoS profile to an interface. Only after the configured QoS profile is bound to an interface can QoS functions on the device.

Configuring a Class

Hillstone devices support the following types of matching conditions:

- Applicaion
- DSCP

- CoS
- IP range
- Address entry
- QoS tag
- IP precedence
- Ingress interface
- Role

The traffic matching conditions can only be configured in the class configuration mode. To enter the class configuration mode, in the global configuration mode, use the following command:

class-map *class-name*

- *class-name* – Specifies the name of class. After executing the command, the system will create a class and enter the class configuration mode; if the specified name exists, the system will directly enter the class configuration mode.

The system provides a default class named class-default. During QoS, all the unmatched traffic will be diverted to class-default. The minimum bandwidth of class-default is the interface bandwidth minus all the reserved bandwidth. You are recommended to reserve 25% bandwidth for class-default. This proportion has proven to be the best reservation. You can configure up to 10 matching conditions for each class.

To cancel the specified class, in the global configuration mode, use the command **no class-map** *clas-name*.

Configuring an Application Matching Condition

Hillstone devices support over 100 applications, such as FTP, SMTP, OSPF, etc. To configure an application matching condition, in the class configuration mode, use the following command:

match application *app-name*

- *app-name* – Specifies the name of the application. It can be the name of predefined application or application group, or the name of user-defined application or application group.

Repeat the command to configure more application matching conditions.

To delete the specified application matching condition, in the class configuration mode, use the command **no match application** *app-name*.

If multiple classes in a QoS Profile contain the same Application ID, the system will process the packets based on the first matched rule. You can use the show application list command to view Application ID.



Tip: For detailed information about service, see "Service and Application" in the "Firewall".

Configuring a DSCP Matching Condition

To configure a DSCP matching condition, in the class configuration mode, use the following command:

match dscp *dscp-value1* [*dscp-value2*] [*dscp-value3*] [*dscp-value4*]

- *dscp-value* – Specifies the DSCP as the matching condition. The DSCP can be either an integer (0 to 63) or a keyword (such as af11, cs2). You can specify up to 4 DSCP values in one command, and the logical relationship among them is OR.

Repeat the command to configure more DSCP matching conditions. To delete the specified DSCP matching condition, in the class configuration mode, use the command:

no match dscp *dscp-value1* [*dscp-value2*] [*dscp-value3*] [*dscp-value4*]

Configuring a CoS Matching Condition

To configure a CoS matching condition, in the class configuration mode, use the following command:

match cos *cos-value1* [*cos-value2*] [*cos-value3*] [*cos-value4*]

- *cos-value* – Specifies the CoS value of 802.1Q as the matching condition. The value range is 0 to 7. You can specify up to 4 CoS values in one command, and the logical relationship among them is OR.

Repeat the command to configure more CoS matching conditions.

To delete the specified CoS matching condition, in the class configuration mode, use the command **no match cos** *cos-value1* [*cos-value2*] [*cos-value3*] [*cos-value4*].

Configuring an IP Range Matching Condition

The IP range matching condition is used to configure IP QoS. To configure an IP range matching condition, in the class configuration mode, use the following command:

match ip-range *start-ip end-ip*

- *start-ip* – Specifies the start IP of the IP range.
- *end-ip* – Specifies the end IP of the IP range.

The ip-range should not exceed the range of Class B addresses.

Repeat the command to configure more IP range matching conditions.

To delete the specified IP range matching condition, in the class configuration mode, use the command **no match ip-range** *start-ip end-ip*.

Configuring an Address Entry Matching Condition

To configure an address entry matching condition, in the class configuration mode, use the following command:

match address *address-entry*

- *address-entry* – Specifies an address entry defined in the address book.

Repeat the command to configure more address entry matching conditions.

To delete the specified address entry matching condition, in the class configuration mode, use the command **no match address** *address-entry*.

Configuring a QoS Tag Matching Condition

To configure a QoS tag matching condition, in the class configuration mode, use the following command:

match policy-qos-tag *tag-value*

- *tag-value* – Specifies the value of QoS tag. The value range is 1 to 1024. You can configure a QoS tag when creating a policy rule or P2P Profile.

Repeat the command to configure more QoS tag matching conditions.

To delete the specified QoS tag matching condition, in the class configuration mode, use the command **no match policy-qos-tag** *tag-value*.



Tip: For more information about how to create a policy rule and how to configure a QoS tag, see the "Policy".

Configuring an IP Precedence Matching Condition

To configure an IP precedence matching condition, in the class configuration mode, use the following command:

match precedence *precedence-value1* [*precedence-value2*] [*precedence-value3*] [*precedence-value4*]

- *precedence-value* – Specifies the value of IP precedence. The value range is 0 to 7. You can specify up to 4 IP precedence values in one command, and the logical relationship among them is OR.

Repeat the command to configure more IP precedence matching conditions.

To delete the specified IP precedence matching condition, in the class configuration mode, use the command **no match precedence** *precedence-value1* [*precedence-value2*] [*precedence-value3*] [*precedence-value4*].

Configuring an Ingress Interface Matching Condition

To configure an ingress interface matching condition, in the class configuration mode, use the following command:

match input-interface *interface-name*

- *interface-name* – Specifies the ingress interface.

Repeat the command to configure more ingress interface matching conditions.

To delete the specified ingress interface matching condition, in the class configuration mode, use the command **no match input-interface** *interface-name*.

Configuring a Role/User/User Group Matching Condition

To configure a role/user/user group matching condition, in the class configuration mode, use the following command:

match {**role** *role-name*| **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*}

- *role-name* – Specifies the name of the role.
- *aaa-server-name* – Specifies the name of the AAA server.
- *user-name* - Specifies the username.
- *user-group-name* - Specifies the name of the user group.

Repeat the command to configure more role matching conditions.

To delete the specified role matching condition, in the class configuration mode, use the command **no match** {**role** *role-name*| **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*}.

Viewing the Class Information

To view the class information, in any mode, use the following command:

show class-map [*class-name*]

- *class-name* – Shows the information of the specified class. If this parameter is not specified, the system will show the information of all the classes.

Configuring a QoS Profile

QoS profile is used to implement QoS on the matched traffic. Besides, you can also control the valid time of QoS profile via a schedule. Hillstone devices support application QoS, IP QoS and role QoS. You need to configure the profile for them as needed.

The QoS profile needs to be configured in the QoS profile configuration mode. To enter the QoS profile configuration mode, in the global configuration mode, use the following command:

qos-profile *qos-profile-name*

- *qos-profile-name* – Specifies the name of the QoS profile. After executing the command, the system will create a QoS profile with the specified name, and enter the QoS profile configuration mode; if the specified name exists, the system will directly enter the QoS profile configuration mode.

To delete the specified QoS Profile, in the global configuration mode, use the command **no qos-profile** qos-profile-name.

To specify a schedule for the QoS profile, in the QoS profile configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* – Specifies the name of the schedule defined in the system.

Repeat the command to specify more schedules for the QoS profile. You can specify up to 10 schedules for each QoS profile. To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified schedule, in the QoS profile configuration mode, use the following command:

no schedule *schedule-name*



Tip: For more information on creating a schedule, see "Configuring Schedule" in the "System Management".

To implement QoS on the matched traffic, you need to specify a class for the QoS profile in the QoS profile configuration mode, and then specify an action for the traffic that matches the class. You can specify up to 64 classes (including the default class class-default) for each QoS profile. The application QoS supports all the matching conditions, while IP QoS only supports the IP range (start IP, end IP and address entry) matching condition, and role QoS only supports the role matching condition.

To specify a class for the QoS profile, in the QoS profile configuration mode, use the following command:

class *class-name*

- *class-name* – Specifies the name of the class. After executing the command, the system will enter the QoS profile class configuration mode.

To delete the specified class, in the QoS profile configuration mode, use the command **no class** *class-name*.

You can specify the QoS options for the matched traffic in the QoS profile class configuration mode, including:

- Specifying the minimum bandwidth
- Configuring policing
- Configuring shaping
- Configuring IP-based QoS (IP QoS)
- Configuring an IP QoS Priority
- Configuring LLQ
- Configuring congestion avoidance

- Configuring DSCP
- Configuring CoS
- Configuring IP precedence
- Configuring a matching priority
- Configuring role-based QoS (role QoS)

Specifying the Minimum Bandwidth

To specify the minimum bandwidth for the class of QoS profile, in the QoS profile class configuration mode, use the following command:

bandwidth {*bandwidth-value* | **percent** *percentage*} [**schedule** *schedule-name*]

- *bandwidth-value* – Specifies the minimum bandwidth for the class. This value is also the weight for CBWFQ calculation. The value range is 32 to 1000000 kbps.
- *percent percentage* – Specifies the minimum bandwidth percentage of class in the interface's total bandwidth. The value range is 1 to 100.
- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified minimum bandwidth, in the QoS profile class configuration mode, use the command *no bandwidth*.

Configuring Policing

Traffic policing is used to control the traffic and apply the specified actions to conform and exceed traffic. To configure policing for a class, in the QoS profile class configuration mode, use the following command:

police *cir-value* [*cbs-value*] [*ebs-value*] **conform-action** {**drop** | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**} **exceed-action** {**drop** | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**} [**violate-action** { **drop**| **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *precedence-value* | **transmit**}] [**schedule** *schedule-name*]

- *cir-value* – Specifies the committed information rate (for putting tokens into the token bucket), i.e., the average rate of the permitted traffic, and also the maximum bandwidth of the class. The value must be smaller than the actual bandwidth value of the interface. The value range is 32 to 1000000 Kbps.
- *cbs-value* – Specifies the committed burst size (the size of the first token bucket), i.e. the maximum traffic for each burst. The value must be larger than the size of the longest packet, and smaller than the actual bandwidth value of the interface. The value range is 2048 to 51200000 bytes.
- *ebs-value* – Specifies the excess burst size (the size of the second token bucket), i.e., the maximum traffic for the excess burst. The value must be smaller than the actual bandwidth value of the interface. The value range is 2048 to 51200000 bytes.
- **conform-action** – Specifies the action for the packets that conform with the specifications. Select one of the actions below:
  - **drop**: Drops the packets.
  - **set-dscp-transmit** *dscp-value*: Sets a DSCP for the packets and transmits.
  - **set-prec-transmit** *precedence-value*: Sets an IP precedence for the packets and transmits.
  - **transmit**: Keeps the packets intact and transmits.
- **exceed-action** - Specifies the action for the packets that exceed the excess burst size. The options are the same with those of the above conform-action.

- **violate-action** - Specifies the action for the packets that violate the specification. The only available option is Drop, i.e., dropping the packet.
- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified policing, in the QoS profile class configuration mode, use the command **no police**.

Configuirng Shaping

Traffic shaping working on egress interfaces is used to smooth the egress traffic according to the rate configuration. To configure shaping for a class, in the QoS profile class configuration mode, use the following command:

shape cir-value [*cbs-value*] [*ebs-value*] [**schedule** *schedule-name*]

- *cir-value* – Specifies the committed information rate (for putting tokens into the token bucket), i.e., the average rate of the permitted traffic, and also the maximum bandwidth of the class. The value must be smaller than the actual bandwidth value of the interface. The value range is 32 to 1000000 Kbps.
- *cbs-value* – Specifies the committed burst size (the size of the first token bucket), i.e. the maximum traffic for each burst. The value must be larger than the size of the longest packet, and smaller than the actual bandwidth value of the interface. The value range is 2048 to 51200000 bytes.
- *ebs-value* – Specifies the excess burst size (the size of the second token bucket), i.e., the maximum traffic for the excess burst. The value must be smaller than the actual bandwidth value of the interface. The value range is 2048 to 51200000 bytes.

- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified shaping, in the QoS profile class configuration mode, use the command **no shape**.

Configuring IP-based QoS (IP QoS)

IP-based QoS, i.e., IP QoS, is used to control the maximum or reserved bandwidth for each IP within the LAN. The perquisite for implementing IP QoS is that the class in the QoS profile must contain the IP range (start IP, end IP or address entry) matching condition. IP QoS should not be used with other types of QoS simultaneously, i.e., if only one class in the QoS profile is configured with IP QoS, all the other classes in the QoS profile must also be configured with IP QoS.

To configure IP QoS, in the QoS profile class configuration mode, use the following command:

ip-qos {**shared-bandwidth** | **per-ip**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

- **shared-bandwidth** – Specifies the bandwidth to the maximum bandwidth (**max-bandwidth bandwidth**) or reserved bandwidth (**reserve-bandwidth bandwidth**) shared by all the IPs within the IP range. The IP range is specified by ip-range of the class.
- **per-ip** – Specifies the bandwidth to the maximum bandwidth (**max-bandwidth bandwidth**) or reserved bandwidth (**reserve-bandwidth bandwidth**) available to each IP within the IP range. The IP range is specified by ip-range of the class.
- **max-bandwidth bandwidth** – Specifies the maximum bandwidth, i.e., the maximum bandwidth shared by all the IPs (**shared-bandwidth**) or available to each IP (**per-ip**) within the IP range. The value range is 32 to 1000000 kbps. When configuring **reserve-bandwidth**, the default value of **max-bandwidth** is 100000.

- **reserve-bandwidth bandwidth** – Specifies the reserved bandwidth, i.e., the reserved bandwidth shared by all the IPs (**shared-bandwidth**) or available to each IP (**per-ip**) within the IP range. The value range is 32 to 1000000 kbps. This value must be smaller than the actual bandwidth value of the interface.

- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified IP QoS, in the QoS profile class configuration mode, use the command **no ip-qos** {**shared-bandwidth** | **per-ip**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*].

Allocation Principle of Reserved Bandwidth

The allocation of reserved bandwidth for IP addresses should following the principles below:

- Only when traffic is passing through the matched IP addresses will the system reserve the specified bandwidth; when the traffic terminates, the reserved bandwidth will be freed.

- If the sum of the reserved bandwidth is larger than the interface bandwidth, and the interface bandwidth is occupied by the IP addresses, then the traffic passing through the newly matched IP addresses will be diverted to class-default; if the bandwidth of class-default is 0, the traffic will be dropped.

Here is an example of configuring IP QoS. The reserved bandwidth per IP for IP1 - IP20 is 1M, and the maximum bandwidth per IP for IP21 - IP40 is 1M. The interface bandwidth is 10M.

When traffic is passing through IP1 - IP9 and IP21 - IP40, IP1 - IP9 will be allocated with the reserved bandwidth of 1M each; the traffic that exceeds 1M reserved bandwidth of IP1 - IP9 and the traffic passing through IP21 - IP40 will compete for the left 1M bandwidth. In such a case, if there is any traffic passing through IP10, the left 1M bandwidth will be reserved for IP10. Thus, IP1 - IP10 are allocated with 1M reserved bandwidth per IP, while all the exceeded traffic of IP1 - IP10 and all the traffic passing through IP21 - IP40 will be diverted to class-default. However,

the bandwidth of class-default is 0 (all the interface bandwidth is reserved), so the above traffic will be dropped.

Configuring an IP QoS Priority

Sometimes the maximum bandwidth available to a user is restricted. In such a case if the user is trying to download large files via Thunder or other P2P software, he will find it's rather slow to open WebPages or receive responses from game servers. To solve the problem, Hillstone devices introduce an IP QoS priority mechanism. The traffic for each IP is assigned with a priority, specifically depending on the type of the application. The traffic with higher priority has the priority in processing. The IP QoS priority should be used in combination with IP QoS to realize the following effect: the bandwidth is restricted, at the same time important bandwidth is allocated with higher priority. The QoS profile with IP QoS priority configured can only be applied to the ingress interfaces.

StoneOS supports 5 IP QoS priorities (1 to 5) among which 1 is the highest priority, and 3 is the default priority. The IP QoS priority is only valid within the device. Once the packets leave the Hillstone device, the marked IP QoS priority will be void.

To make the IP QoS priority take effect, you should take the following steps on the device:

1. Configure an IP QoS priority for the ingress interface, specifically depending on the type of the application.
2. Configure an IP-based QoS profile on the egress interface, and apply the configured IP QoS priority to the profile.

To configure an IP QoS priority, in the QoS profile class configuration mode, use the following command:

set ip-qos-priority *number*

- *number* – Specifies the IP QoS priority. The value range is 1 to 5. The default value is 3.

To restore to the default IP QoS priority, in the QoS profile class configuration mode, use the command **no set ip-qos-priority**.

Configuring LLQ

Low Latency Queuing (LLQ) is a comprehensive algorithm of Priority Queuing (PQ), Custom Queuing (CQ) and Weighted Fair Queuing (WFQ). LLQ is usually used for voice and interactive video stream. The total bandwidth configured for LLQ should not be more than 33% of total application bandwidth. To configure LLQ for the class, in the QoS profile class configuration mode, use the following command:

priority {*bandwidth-value* | **percent** *percentage*} [*burst-size*] [**schedule** *schedule-name*]

- *bandwidth-value* – Specifies the reserved bandwidth. The value range is 32 to 1000000 Kbps;
- **percent** *percentage* – Specifies the reserved bandwidth percentage in the interface's total bandwidth. The value range is 1 to 100.
- *burst-size* – Specifies the burst size. The value range is 2048 to 51200000 bytes.
- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

To cancel the specified LLQ, in the QoS profile class configuration mode, use the command **no priority**.

Configuring Congestion Avoidance

The congestion avoidance on Hillstone devices is implemented by the Weighted Random Early Detection (WRED) mechanism. With WRED enabled, the system will drop packets at random in case of congestion, in order to avoid TCP global synchronization and improve line utilization. WRED is disabled by default. To configure WRED, in the QoS profile class configuration mode, use the following command:

random-detect [**dscp-based** | **prec-based**]

- **dscp-based** – WRED calculates the possibility of dropping the packets based on DSCP.
- **prec-based** – WRED calculates the possibility of dropping the packets based on IP precedence. This is the default options.

To cancel the specified WRED, in the QoS profile class configuration mode, use the command **no random-detect**.

Configuring CoS

You can configure a Layer 2 CoS value for the outbound packets, and in combination of the command match cos, enable the device to implement QoS on packets based on the marked CoS value. The QoS profile with CoS configured can only be bound to the ingress interfaces. To configure CoS for the class, in the QoS profile class configuration mode, use the following command:

set cos *cos-value*

- **cos-value** – Specifies the CoS value. The value range is 0 to 7.

To cancel the specified CoS, in the QoS profile class configuration mode, use the command **no set cos** .

Configuring DSCP

You can mark DSCP values for different packets, so that all the other QoS functions can operate on the packets based on the configured DSCP values. The QoS profile with DSCP configured can only be bound to the ingress interface. One single packet should not be configured with DSCP and IP precedence simultaneously. You can only select one of them. To configure DSCP for the class, in the QoS profile class configuration mode, use the following command:

set dscp *dscp-value*

- *dscp-value* – Specifies a DSCP value, either in form of an integer (0 to 63) or a keyword (such as af11, cs2).

To cancel the specified DSCP, in the QoS profile class configuration mode, use the command **no set dscp**.

Configuring IP Precedence

You can mark IP precedence values for different packets, so that all the other QoS functions can operate on the packets based on the configured IP precedence values. The QoS profile with IP precedence configured can only be bound to the ingress interface. One single packet should not be configured with DSCP and IP precedence simultaneously. You can only select one of them. To configure IP precedence for the class, in the QoS profile class configuration mode, use the following command:

set precedence *precedence-value*

- *precedence-value* – Specifies an IP precedence value. The value range is 0 to 7.

To cancel the specified IP precedence, in the QoS profile class configuration mode, use the command **no set precedence**.

Configuring a Matching Priority

Sometimes the traffic might be matched to multiple classes in the QoS profile. In such a case the system will select a class based on the matching priority of the classes. To configure a matching priority, in the QoS profile class configuration mode, use the following command:

match-priority *priority-number*

• **priority-number** – Specifies the priority for the class. The value range is 1 to 256. 1 is the highest priority. Except for class-default, the default priority of all the other classes is 255. The classes without any priority configured will be matching based on their creation sequence in the QoS profile. The priority of class-default is 256, i.e., the lowest priority by default.

To cancel the specified matching priority, in the QoS profile class configuration mode, use the command **no match-priority**.

Configuring an Exception Policy

Hillstone devices support exception policies. With this function configured, the system will not implement QoS on the specified traffic. To configure an exception policy, in the QoS profile configuration mode, use the following command:

exception-list {**ip-range** *A.B.C.D A.B.C.D* | **address** *address-entry*}

- *A.B.C.D A.B.C.D* – Specifies the IP range. The traffic in this range will not be controlled by QoS.
- **address-entry** – Specifies the address entry. The traffic in this range will not be controlled by QoS.

To delete the specified exception policy, in the QoS profile configuration mode, use the command **no exception-list**.

Example: The maximum bandwidth available to each user for Internet access is restricted to 1000 K, but access to the DMZ segment should not be restricted. The IP range for the Intranet users is 10.101.1.0 to 10.101.1.150; the internal servers (such as Web servers, FTP server, etc.) are located in the DMZ segment with the IP range of 10.100.6.10 to 10.100.6.20. Use the following commands:

```
hostname(config)# class-map internet
hostname(config-class-map)# match ip-range 10.101.1.0 10.101.1.150
hostname(config-class-map)# exit
hostname(config)# qos-profile ipqos
hostname (config-qos-profile)# exception-list ip-range 10.100.6.10 10.100.6.20
hostname (config-qos-profile)# class internet
hostname (config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 1000
hostname (config-qos-prof-cmap)# exit
hostname (config-qos-profile)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile input ipqos
hostname(config-if-eth0/2)# qos-profile output ipqos
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Configuring Role-based QoS (Role QoS)

Role-based QoS, i.e., role QoS, is used to control the maximum or reserved bandwidth for each user within the role. The perquisite for implementing role QoS is that the class in the QoS profile must contain the role matching condition. Role QoS should not be used with other types of QoS simultaneously, i.e., if only one class in the QoS profile is configured with role QoS, all the other classes in the QoS profile must also be configured with role QoS.

To configure role QoS, in the QoS profile class configuration mode, use the following command:

role-qos {**share** | **per-user**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*]

- **share** – Specifies the bandwidth to the maximum bandwidth (**max-bandwidth bandwidth**) or reserved bandwidth (**reserve-bandwidth bandwidth**) shared by all the users within the role. The IP range is specified by ip-range of the class.
- **per-user** – Specifies the bandwidth to the maximum bandwidth (**max-bandwidth bandwidth**) or reserved bandwidth (**reserve-bandwidth bandwidth**) available to each user within the role. The IP range is specified by ip-range of the class.
- **max-bandwidth bandwidth** – Specifies the maximum bandwidth, i.e., the maximum bandwidth shared by all the users (**share**) or available to each user (**per-user**) within the role. The value range is 32 to 1000000 Kpbs. When configuring **reserve-bandwidth**, the default value of **max-bandwidth** is 100000.
- **reserve-bandwidth bandwidth** – Specifies the reserved bandwidth, i.e., the reserved bandwidth shared by all the users (**shared-bandwidth**) or available to each user (**per-ip**) within the role. The value range is 32 to 1000000 Kpbs. This value must be smaller than the actual bandwidth value of the interface.
- *schedule-name* – Specifies the name of the schedule defined in the system. The configuration will only take effect during the specified period. Repeat the command to specify

more schedules (up to 8). To avoid possible unknown problems, you are not recommended to use schedules with time overlapping.

If one user matches multiple roles, and all the roles are configured with role QoS in the QoS profile, then only the first matched role QoS will work on the users. Therefore, when one user matches multiple roles, you should pay special attention to the order of role QoS rules.

To cancel the specified role QoS, in the QoS profile class configuration mode, use the command **no role-qos** {**share** | **per-user**} {**max-bandwidth** *bandwidth* | **reserve-bandwidth** *bandwidth* [**max-bandwidth** *bandwidth*]} [**schedule** *schedule-name*].

The traffic without any role configured will be diverted to the default class class-default. By default the system will not control the bandwidth of class-default.

Allocation Principle of Reserved Bandwidth

The allocation of reserved bandwidth for roles should following the principles below:

- Only when traffic is available to the matched users will the system reserve the specified bandwidth; when the traffic terminates, the reserved bandwidth will be freed.
- If the sum of the reserved bandwidth is larger than the interface bandwidth, and the interface bandwidth is occupied by the users, then the traffic available to the newly matched users will be diverted to class-default; if the bandwidth of class-default is 0, the traffic will be dropped.

Here is a role-based QoS example. The the reserved bandwidth per user for role1 - role20 is 1M, and the maximum bandwidth per user for role21 - role40 is 1M. The interface bandwidth is 10M. role1 - role40 correspond to user1 - user40 respectively.

When there is traffic available to user1 - user9 and user21 - user40, user1 - user9 will be allocated with the reserved bandwidth of 1M each; the traffic that exceeds 1M reserved bandwidth of user1 - user9 and the traffic available to user21 - user40 will compete for the left 1M bandwidth. In such a case, if there is any traffic available to user10, the left 1M bandwidth will be reserved for user10. Thus, user1 - user10 are allocated with 1M reserved bandwidth per user, while all the exceeded traffic of user1 - user10 and all the traffic passing through user21-user40 will be diverted to class-default. However, the bandwidth of class-default is 0 (all the interface bandwidth is reserved), so the above traffic will be dropped.

Nesting a QoS Profile

Nesting a QoS profile is the process of binding the class of a QoS profile to another QoS profile, so that you can reasonably allocate application bandwidth to different IPs/roles/users. To configure a nest QoS profile, in the QoS profile class configuration mode, use the following command:

qos-profile *qos-profile-name*

- **qos-profile-name** – Specifies the name of QoS profile which should be an existing QoS profile name in the system.

To cancel the specified nest QoS profile, in the QoS profile class configuration mode, use the command **no qos-profile**.



Notes: When using the nest QoS profile, you should keep in mind:

- The application QoS can nest an IP QoS profile or role QoS profile, but cannot nest an application QoS profile.
- The bandwidth of the nested IP QoS profile and role QoS profile must be shared, and these profiles can only contain up to sixteen classes (including the default class).
- IP QoS profile and role QoS profile cannot be mutually nested.
- The nested application QoS profile can only contain up to sixteen classes (including the default class); the bandwidth and priority parameters of the nested application QoS profile must be configured in form of percentage.

Specifying a QoS Operation for the Egress Interface

You can specify a QoS operation for the egress interface, including policing and shaping. This function only applies to IP QoS and role QoS. By default the system will perform policing on the

egress interfaces with QoS enabled. To perform shaping on the egress interface, in the QoS profile configuration mode, use the following command:

shaping-for-egress

To restore to the default operation, in the QoS profile configuration mode, use the command **no shaping-for-egress**.

Disabling a Class

By default all the classes in the QoS profile are enabled. To disable a specific class in the QoS profile, in the QoS profile class configuration mode, use the following command:

disable

To restore to the default status, in the QoS profile class configuration mode, use the command **`no disable`**.



Notes: The disabled classes still exist in the QoS profile. To delete the specified class from the QoS profile, use the command **`no class`** *`class-name`*.

Binding to an Interface

The configured QoS profiles will not take effect until being bound to an interface. To bind a QoS profile to an interface, in the interface configuration mode, use the following command:

qos-profile [**1st-level** | **2nd-level**] {**input** | **output**} *qos-profile-name*

- **1st-level | 2nd-level** – Applicable to multi-level QoS. 1st-level indicates the first level, and 2nd-level indicates the second level. If this parameter is not specified, the profile will be bound to the second level.
- **input | output** – Specifies the interface direction (either **input** or **output**) the QoS profile will be bound to.
- *qos-profile-name* – Specifies the name of the QoS profile that will be bound.

To cancel the binding, in the interface configuration mode, use the command **no qos-profile** [**1st-level** | **2nd-level**] {**input** | **output**} .



Notes: IP QoS profile and role QoS profile should not be bound to the different levels of one single interface.

Viewing QoS Information of an Interface

After configuring QoS for the interface, to view the QoS configuration and statistics, use the following command:

show qos interface *interface-name* [**1st-level-input** | **1st-level-output** | **2nd-level-input** | **2nd-level-output**] [**detail**]

- **interface-name** – Specifies the interface.
- **1st-level-input** – Only shows the QoS statistics of the first level of the input interface.
- **1st-level-output** - Only shows the QoS statistics of the first level of the output interface.
- **2st-level-input** – Only shows the QoS statistics of the second level of the input interface.
- **2st-level-output** - Only shows the QoS statistics of the second level of the output interface.
- **detail** – Shows the statistics and the corresponding QoS configuration information.

Viewing QoS Profile Information

To view the QoS profile configuration, in any mode, use the following command:

show qos-profile [*qos-profile-name*]

- **qos-profile-name** – Shows the configuration of the specified QoS profile. If this parameter is not specifies, the command will show the configurations of all the QoS profiles.

FlexQoS

FlexQoS is applicable to IP-based QoS and role-based QoS. If the system is configured with QoS, the maximum bandwidth available to different IP addresses is typically restricted to a specified range. In such a case, even if the interface has some free bandwidth available, the restricted IP cannot make use of it, leading to resource waste. To solve this problem, StoneOS provide FlexQoS to make full use of bandwidth resources. The configuration of FlexQoS includes global FlexQoS and Class Flex QoS which can implement specific FlexQoS control over different IP queues and roles. The global FlexQoS is disabled by default. In such a case, no matter whether the Class FlexQoS is enabled, both the global and Class FlexQoS are disabled. The Class FlexQoS is only valid when both the global and Class FlexQoS are enabled.

You can set a lower threshold and upper threshold for the global FlexQoS. The default lower threshold is 75, and the default upper threshold is 85. If FlexQoS is enabled with the default values, when the utilization of output bandwidth is less than 75%, the available bandwidth will increase linearly (you can specify the flex factor); when the utilization reaches 85%, the available bandwidth will decrease exponentially to the specified lower threshold; when the utilization is between the upper and lower threshold, the FlexQoS is stable, i.e., the available bandwidth will neither increase nor decrease.

Configuring Global FlexQoS

To configure global FlexQoS, in the global configuration mode, use the following command:

flex-qos low-water-mark *value* **high-water-mark** *value*

- **low-water-mark** *value* – Specifies the upper threshold. The value range is 50 to 80. The default value is 75.
- **high-water-mark** *value* – Specifies the lower threshold. The value range is 81 to 90. The default value is 85.

To disable global FlexQoS, in the global configuration mode, use the command **no flex-qos**.

When global FlexQoS is enabled, if the bandwidth utilization of the egress interface is lower than the upper threshold, the available bandwidth will increase. To configure the flex factor, in the global configuration mode, use the following command:

flex-qos-up-rate *rate*

- *rate* – Specifies the flex factor. The value range is 1 to 16 times/min. The default value is 1. The calculation formula of available bandwidth is flex factor multiplies IP bandwidth.

To restore to the default flex factor, in the global configuration mode, use the following command:

no flex-qos-up-rate



Notes: A large flex factor might lead to tremendous bandwidth changes.

Configuring FlexQoS for a Class

By default the FlexQoS for class is enabled. To enable or disable this function for a class, in the QoS profile class configuration mode, use the following commands:

- Enable: **flex-qos**
- Disable: **no flex-qos**

After enabling FlexQoS for a class, to specify the maximum FlexQoS bandwidth for each IP of the class, in the QoS profile class configuration mode, use the following command:

flex-qos max-bandwidth *bandwidth*

- *bandwidth* – Specifies the maximum FlexQoS bandwidth. The value range is 64 to 1000000 kbps. The default value is 100 times of the IP bandwidth.

To cancel the specified maximum FlexQoS bandwidth, in the QoS profile class configuration mode, use the following command:

no flex-qos max-bandwidth *bandwidth*

Multi-level QoS

The application QoS and IP QoS are two independent data stream control mechanisms. The application QoS is a global control that is used to re-organize the data stream passing through the device, and provide faster and better service for the data with higher priority; while the IP QoS focuses on each individual IP, and controls the bandwidth available to each IP. The combination

of the two QoS mechanisms is known as multi-level QoS. With multi-level QoS configured, the traffic passing through the device will be controlled by the two QoS mechanisms respectively.

The recommendation for the multi-level QoS is: the application QoS is applied to the first level and the IP QoS is applied to the second level. After the traffic is processed by the 1st-level QoS, important data such as game or VoIP will be accelerated, while the non-important data like P2P will be dropped or delayed. Thus, the traffic passing through the device will be marked with priorities after the 1st-level QoS, and then the bandwidth will be further controlled by the 2nd-level QoS.

Examples of Configuring QoS

This section describes some QoS configuration examples, including:

- Example 1: Matching priority
- Example 2: Classification and marking
- Example 3: Policing and shaping
- Example 4: Application QoS
- Example 5:CBWFQ
- Example 6: LLQ
- Example 7: IP QoS (1)
- Example 8: IP QoS (2)
- Example 9: Multi-VR Application in IP QoS
- Example 10: IP QoS Priority
- Example 11: Role QoS
- Example 12: Nest QoS profile
- Example 13: Multi-level QoS

Example 1: Configuring a Matching Priority

The QoS profile of Profile1 contains two classes: class1 and class2. The matching condition for class1 is HTTP service, and the matching condition for class2 is QoS tag 2. Take the following steps:

Step 1: Configure class1 and class2

```
hostname(config)# class-map class1
hostname(config-class-map)# match application http
hostname(config-class-map)# exit
hostname(config)# class-map class2
hostname(config-class-map)# match policy-qos-tag 2
hostname(config-class-map)# exit
hostname(config)#class trashmatch address 1m
```

Step 2: Configure Profile1

```
hostname(config)# qos-profile profile1
hostname(config-qos-profile)# class class1
hostname(config-qos-prof-cmap)# set dscp 20
hostname(config-qos-prof-cmap)# match-priority 1
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class class2
hostname(config-qos-prof-cmap)# set dscp 35
hostname(config-qos-prof-cmap)# match-priority 15
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Bind Profile1 to ethernet0/3

```
hostname(config)# interface ethernet0/3
```

```
hostname(config-if-eth0/3)# qos-profile input profile1
hostname(config-if-eth0/3)# exit
hostname(config)#
```

After the above configurations, for the traffic that is destined to the device on ethernet0/3, the DSCP of the traffic whose application type is HTTP and Policy QoS tag is 2 will be marked 20 instead of 35. Since the priority of class1 is higher than that of class2, the traffic is matched to class1.

Example 2: Classification and Marking

The ingress interface is bound with a QoS profile. Mark the DSCP of af11 to the HTTP traffic, mark the DSCP of cs7 to the packets with QoS tag 1 (the QoS tag is configured during the creation of policy rules and P2P profile), and mark the DSCP of ef to the FTP packets. The system and Internet will process the DSCP values of af11, cs7 and ef according the RFC standards.

Step 1: Configure classes named http, ftp and trash to classify the traffic

```
hostname(config)# class-map http
hostname(config-class-map)# match application http
hostname(config-class-map)# exit
hostname(config)# class-map ftp
hostname(config-class-map)# match application ftp
hostname(config-class-map)# exit
hostname(config)# class-map trash
hostname(config-class-map)# match policy-qos-tag 1
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Configure a QoS profile to mark applications of different types

```
hostname(config)# qos-profile classification
hostname(config-qos-profile)# class http
hostname(config-qos-prof-cmap)# set dscp af11
```

```
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class ftp
hostname(config-qos-prof-cmap)# set dscp ef
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)#
hostname(config-qos-prof-cmap)# set dscp cs7
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Bind the QoS profile to ethernet0/0 to classify the traffic on ethernet0/0 according to the QoS profile

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile inputclassification
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Example 3: Policing and Shaping

This example shapes the HTTP traffic to 12.8M, and regulates the P2P traffic to 6.4M. In Example 2, the HTTP traffic is marked af11, and the P2P traffic is marked cs7. This example is based on the classification and marking in Example 2.

Step 1: Configure classes named af11 and cs7

```
hostname(config)# class-map af11
hostname(config-class-map)# match dscp af11
hostname(config-class-map)# exit
hostname(config)# class-map cs7
hostname(config-class-map)# match dscp cs7
hostname(config-class-map)# exit
```

```
hostname(config)#
```

Step 2:Configure a QoS profile to police and shape the HTTP and P2P traffic

```
hostname(config)# qos-profile control
hostname(config-qos-profile)# class af11
hostname(config-qos-prof-cmap)# shape 12800
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class cs7
hostname(config-qos-prof-cmap)# police 6400 8000 8000conform-action transmit
exceed-action drop
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Bind the QoS profile to ethernet0/1 to control the outbound HTTP and P2P traffic on ethernet0/1 according to the QoS profile

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile output control
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Example 4: Application QoS

This section describes an application QoS configuration example. The requirement is: restricting the P2P traffic transmitting on ethernet0/0 to 1M/sec. In Example 2, the P2P traffic is marked cs7. This example is based on the classification and marking in Example 2.

Step 1: Configure a class named cs7

```
hostname(config)# class-map cs7
hostname(config-class-map)# match dscp cs7
hostname(config-class-map)# exit
```

```
hostname(config)#
```

Step 2: Configure a profile named p2p, and control the traffic that is matched to cs7 (P2P). The maximum bandwidth is restricted to 1000 kbps, and the Exceed action is Drop

```
hostname(config)# qos-profile p2p
hostname(config-qos-profile)# class cs7
hostname(config-qos-prof-cmap)# police 1000 conform-action transmit exceed-action drop
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
```

Step 3: Bind the QoS profile to ethernet0/0 to control the outbound P2P traffic on ethernet0/0

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile output p2p
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Example 5: CBWFQ

This example illustrates how to assure the bandwidth available to different classes in the QoS profile based on CBWFQ. In Example 2, the HTTP traffic is marked af11, and the P2P traffic is marked cs7. This example is based on the classification and marking in Example 2.

Step 1: Configure classes named af11 and cs7

```
hostname(config)# class-map af11
hostname(config-class-map)# match dscp af11
hostname(config-class-map)# exit
hostname(config)# class-map cs7
hostname(config-class-map)# match dscp cs7
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Create a QoS profile named qos-profile1, and configure the minumun bandwidth for af11 abd cs7

```
hostname(config)# qos-profile qos-profile1
hostname(config-qos-profile)# class af11
hostname(config-qos-prof-cmap)# bandwidth 5000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class cs7
hostname(config-qos-prof-cmap)# bandwidth 2500
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Configure the upstream bandwidth for ethernet0/2, and bind policy1 to ethernet0/2

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# bandwidth upstream 10000000
hostname(config-if-eth0/2)# qos-profile output qos-profile1
hostname(config-if-eth0/2)# exit
hostname(config)#
```

After the configuration, if the upstream bandwidth of ethernet0/2 is 10M, the available bandwidth to class-default will be 2.5M (10-5-2.5), and the default queue is CBWFQ.

When processing traffic based on the above configuration, if the available bandwidth for class1 is 20M, the available bandwidth for class2 is 15M, and the available bandwidth for class-default is 0, the device will allocate the 2.5M bandwidth of class-default to class1 and class2 proportionally.

Example 6: LLQ & Congestion Avoidance

The goal for this example is to reserve 3M bandwidth for VoIP traffic, set the minimum bandwidth for HTTP traffic to 4M, police the bandwidth for P2P traffic to 6.4M, and drop the exceeded P2P traffic. In Example 2, the VoIP traffic is marked ef, the HTTP traffic is marked

af11, and the P2P traffic is marked cs7. This example is based on the classification and marking in Example 2.

Step 1: Configure classes named af11, cs7 and ef

```
hostname(config)# class-map ef
hostname(config-class-map)# match dscp ef
hostname(config-class-map)# exit
hostname(config)# class-map af11
hostname(config-class-map)# match dscp af11
hostname(config-class-map)# exit
hostname(config)# class-map cs7
hostname(config-class-map)# match dscp cs7
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Create a QoS profile named llq and configure the bandwidth for ef, af11 and cs7

```
hostname(config)# qos-profile llq
hostname(config-qos-profile)# class ef
hostname(config-qos-prof-cmap)# priority 3000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class af11
hostname(config-qos-prof-cmap)# bandwidth 4000
hostname(config-qos-prof-cmap)# random-detect
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class cs7
hostname(config-qos-prof-cmap)# police 6400 8000 8000 conform-action transmit
exceed-action drop
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class class-default
```

```
hostname(config-qos-prof-cmap)# random-detect
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Configure the upstream bandwidth of ethernet0/3, and bind the QoS profile to ethernet0/3 to control the outbound bandwidth on ethernet0/3

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# bandwidth upstream10000000
hostname(config-if-eth0/3)# qos-profile output llq
hostname(config-if-eth0/3)# exit
hostname(config)#
```

In the example, the bandwidth of ethernet0/3 is 10M. Class cs7 is policed, so its bandwidth will not be calculated. Therefore, the bandwidth available to class-default is 3M (10-3-4). When there is no traffic for class-default, the bandwidth available to class cf11 will be 7M (5+2). The bandwidth available to class ef will always be 3M.

Example 7: IP QoS (1)

The goal is to set maximum bandwidth available for each IP in Class ip-range1 to 2M and set the maximum bandwidth shared by all the IPs in class ip-range2 to 10M.

Step 1: Configure a class

```
hostname(config)# class-map ip-range1
hostname(config-class-map)# match ip-range 2.2.0.0 2.2.10.255
hostname(config-class-map)# exit
hostname(config)# class-map ip-range2
hostname(config-class-map)# match ip-range 192.168.100.200 192.168.100.200
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Configure a QoS profile

```
hostname(config)# qos-profile profile1
hostname(config-qos-profile)# class ip-range1
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 2000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class ip-range2
hostname(config-qos-prof-cmap)# match-priority 3
hostname(config-qos-prof-cmap)# ip-qos shared-bandwidth max-bandwidth 10000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Bind the QoS profile to an interface

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile input profile1
hostname(config-if-eth0/2)# qos-profile output profile1
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Example 8: IP QoS (2)

The available bandwidth shared by all the IPs in class ip-range1 is 2M, while the bandwidth available to each IP should not exceed 800 KB.

The device is connected to the Internet on ethernet0/1, and ethernet0/0 is connected to the Intranet. The requirement is: the IP segment of 1.1.1.1 to 1.1.1.255 in the Intranet share 2M bandwidth, while the bandwidth available to each IP should not exceed 800 KB. You can implement the requirement by two approaches:

Solution 1

This solution reaches the goal by configuring two IP QoS profiles. Take the following steps:

Step 1: Create a class named ip-range:

```
hostname(config)# class-map ip-range
hostname(config-class-map)# match ip-range 1.1.1.1 1.1.1.255
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Create a QoS profile named ipq-share and allow all the IPs within the range to share 2M bandwidth

```
hostname(config)# qos-profile ipq-share
hostname(config-qos-profile)# class ip-range
hostname(config-qos-prof-cmap)# ip-qos share max-bandwidth 2000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
hostname(config)# qos-profile ipq-per
hostname(config-qos-profile)# class ip-range
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 800
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 3: Bind the QoS profiles to an interface (first restrict the individual bandwidth, and then restrict the total bandwidth)

```
Output bandwidth:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile input ipq-per
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
```

```
hostname(config-if-eth0/1)# qos-profile output ipq-share
hostname(config-if-eth0/1)# exit
hostname(config)#
Input bandwidth:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile output ipq-share
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile input ipq-per
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Solution 2

Configure an application QoS profile and an IP QoS profile. Take the following steps:

Step 1: Create a class named ip-range

```
hostname(config)# class-map ip-range
hostname(config-class-map)# match ip-range 1.1.1.1 1.1.1.255
hostname(config-class-map)# exit
hostname(config)#
```

Step 2: Create a QoS profile named appq, and allow all the IPs within the range to share 2M bandwidth

```
hostname(config)# qos-profile appq
hostname(config-qos-profile)# class ip-range
hostname(config-qos-prof-cmap)# police 2000conform-action transmit exceed-action drop
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
```

```
hostname(config)#
```

Step 3: Create a QoS profile named ipq-per, and restrict the bandwidth available to each IP within the range to 800 KB

```
hostname(config)# qos-profile ipq-per
hostname(config-qos-profile)# class ip-range
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 800
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 4: Bind the QoS profiles to an interface (first restrict the individual bandwidth, and then restrict the total bandwidth)

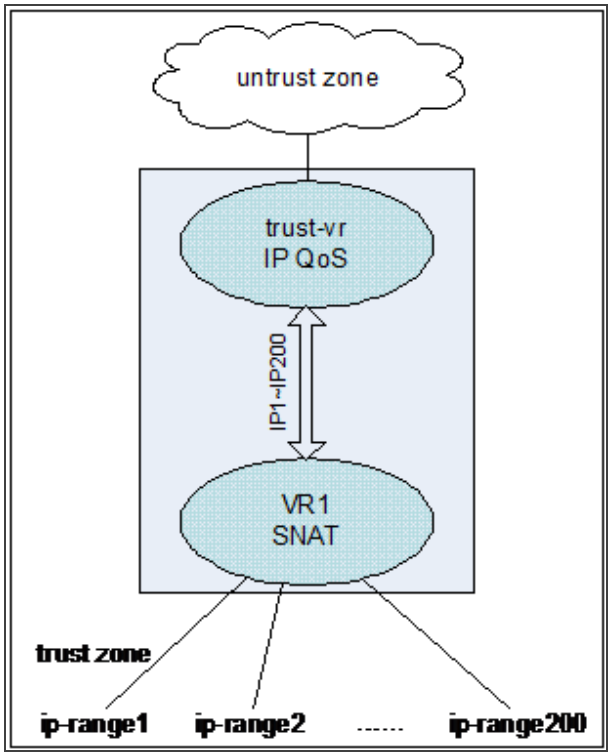
```
Output bandwidth:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile input ipq-per
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile output appq
hostname(config-if-eth0/1)# exit
hostname(config)#
Input bandwidth:
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile output appq
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile input ipq-per
hostname(config-if-eth0/1)# exit
```

```
hostname(config)#
```

Example 9: Multi-VR Application in IP QoS

There are 200 IP segments: ip-range1 (1.1.1.1 to 1.1.1.10), ip-range2 (2.1.1.1 to 2.1.1.10) ⋯ ip-range200 (200.1.1.1 to 200.1.1.10). The requirement is: restricting the maximum bandwidth available to each IP segment to a specified value (such as 1M, 4M, 10M⋯) by IP QoS.

One QoS profile can only support up to 64 classes, so in order to restrict bandwidth for 200 IP segments, you need to combine multi-VR to the IP QoS, as shown the figure below:



As shown above, there are two VRs: trust-vr and VR1. SNAT is implemented in VR1, so the 200 IP segments can be translated to individual IPs, i.e., translating ip-range1, ip-range2 ⋯ ip-range200 to IP1, IP2 ⋯ IP200 respectively; then classify the 200 IPs according to the bandwidth, and in trust-vr restrict the bandwidth available to the IPs, specifically depending on the IP QoS configuration.

Step 1: Enable multi-VR on the device

```
hostname# exec vrouter enable

Warning: please reboot the device to make the change validation!
```

```
hostname# reboot
System reboot, are you sure? y/[n]: y
```

Step 2: After rebooting, create VR1

```
hostname(config)# ip vrouter VR1
hostname(config-vrouter)# exit
hostname(config)#
```

Step 3: Configure a security zone

```
hostname(config)# zone trust
hostname(config-zone-trust)# vrouter VR1
hostname(config-zone-trust)# exit
hostname(config)#
```

Step 4: Create 200 address ranges that contain the above 200 segments respectively

```
hostname(config)# address ip-range1
hostname(config-addr)# range 1.1.1.1 1.1.1.10
hostname(config-addr)# exit
hostname(config)# address ip-range2
hostname(config-addr)# range 2.1.1.1 2.1.1.10
hostname(config-addr)# exit
……
hostname(config)# address ip-range200
hostname(config-addr)# range 200.1.1.1 200.1.1.10
hostname(config-addr)# exit
hostname(config)#
```

Step 5: Create 200 address entries that contain the above 200 IPs respectively

```
hostname(config)# address ip1
hostname(config-addr)# ip 1.1.1.100/32
```

```
hostname(config-addr)# exit
hostname(config)# address ip2
hostname(config-addr)# ip 2.1.1.100/32
hostname(config-addr)# exit
……
hostname(config)# address ip200
hostname(config-addr)# ip 200.1.1.100/32
hostname(config-addr)# exit
hostname(config)#
```

Step 6: Create 200 SNAT rules in VR1 to translate the 200 segments to 200 IPs respectively

```
hostname(config)# ip vrouter VR1
hostname(config-vrouter)# snatrule id 1 from ip-range1 to any evr trust-vr trans-to ip1
hostname(config-vrouter)# snatrule id 2 from ip-range2 to any evr trust-vr trans-to ip2
……
hostname(config-vrouter)# snatrule id 200 from ip-range200 to any evr trust-vr trans-to ip200
hostname(config-vrouter)# exit
hostname(config)#
```

Step 7: After SNAT, classify the 200 IPs according to the bandwidth; create address entries, each entry contains IPs of the equal bandwidth

```
hostname(config)# address 1m
hostname(config-addr)# member ip1
hostname(config-addr)# member ip5
hostname(config-addr)# member ip6
……
```

```
hostname(config-addr)# exit
hostname(config)# address 4m
hostname(config-addr)# member ip101
hostname(config-addr)# member ip15
……
hostname(config-addr)# exit
……
hostname(config)#
```

Step 8: Create classes, and configure each class with an address entry matching condition

```
hostname(config)# class-map 1m
hostname(config-class-map)#
hostname(config-class-map)# exit
hostname(config)# class-map 4m
hostname(config-class-map)# match address 4m
hostname(config-class-map)# exit
……
hostname(config)#
```

Step 9: Create a QoS profile named ipq

```
hostname(config)# qos-profile ipq
hostname(config-qos-profile)# class 1m
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 1000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class 4m
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 4000
hostname(config-qos-prof-cmap)# exit
……
```

```
hostname(config)#
```

Step 10: Bind the QoS profile to an interface

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile input ipq
hostname(config-if-eth0/2)# qos-profile output ipq
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Example 10: IP QoS Priority

The goal of this example is to assure that the webpage browsing and webgame have the highest priority. The device is connected to the Internet on ethernet0/0 (176.133.13.8); PC1 (10.200.2.2) and PC2 (10.200.1.2) are connected to ethernet0/1 (10.200.2.1) and ethernet0/2 (10.200.1.1) respectively.

Step 1: Configure classes

```
hostname(config)# class-map http
hostname(config-class-map)# match application http
hostname(config-class-map)# exit
hostname(config)# class-map game
hostname(config-class-map)# match application game_kart
hostname(config-class-map)# match application game_dance
hostname(config-class-map)# exit
hostname(config)# class-map ip-range1
hostname(config-class-map)# match ip-range 10.200.2.2 10.200.2.255
hostname(config-class-map)# exit
hostname(config)# class-map ip-range2
hostname(config-class-map)# match ip-range 10.200.1.2 10.200.1.255
hostname(config-class-map)# exit
```

```
hostname(config)#
```

Step 2: Configure a QoS profile

```
hostname(config)# qos-profile ip-priority-mark
hostname(config-qos-profile)# class game
hostname(config-qos-prof-cmap)# set ip-qos-priority 1
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class http
hostname(config-qos-prof-cmap)# set ip-qos-priority 2
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)# qos-profile ip-qos
hostname(config-qos-profile)# class ip-range1
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 3000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class ip-range2
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 2000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
```

Step 3: Bind the QoS profile to an interface

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile input ip-priority-mark
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile input ip-priority-mark
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/0
```

```
hostname(config-if-eth0/0)# qos-profile output ip-qos
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Example 11: Role QoS

The requirement is: The maximum bandwidth available to each user (user11 and user12) corresponding to role1 is 1M, and maximum bandwidth shared by all the users (user21, user 22 and user23) corresponding to role2 is 4M. The maximum bandwidth available to each user of class-default is 200 KB.

Step 1: Configure roles and users

```
hostname(config)# role role1
hostname(config)# role role2
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user11
hostname(config-user)# exit
hostname(config-aaa-server)# user user12
hostname(config-user)# exit
hostname(config-aaa-server)# user user21
hostname(config-user)# exit
hostname(config-aaa-server)# user user22
hostname(config-user)# exit
hostname(config-aaa-server)# user user23
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user user11 role role1
hostname(config-role-mapping)# match user user12 role role1
```

```
hostname(config-role-mapping)# match user user21 role role2
hostname(config-role-mapping)# match user user22 role role2
hostname(config-role-mapping)# match user user23 role role2
hostname(config-role-mapping)# exit
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# role-mapping-rule rule1
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 2: Configure an appropriate management method which can be WebAuth, SSL VPN or 802.1X.

Step 3: Configure classes

```
hostname(config)# class-map class1
hostname(config-class-map)# match role role1
hostname(config-class-map)# exit
hostname(config)# class-map class2
hostname(config-class-map)# match role role2
hostname(config-class-map)# exit
hostname(config)#
```

Step 4: Configure a QoS profile

```
hostname(config)# qos-profile role-profile
hostname(config-qos-profile)# class class1
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 1000
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class class2
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 4000
hostname(config-qos-prof-cmap)# exit
```

```
hostname(config-qos-profile)# class class-default
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 200
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 5: Bind the QoS profile to an interface

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile input role-profile
hostname(config-if-eth0/2)# qos-profile output role-profile
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Example 12: Nest QoS Profile

Configure a nest QoS profile based on Example 10 to implement the following QoS controls:

- For the users that can be matched to a role, guarantee the HTTP and FTP application bandwidth, but restrict the P2P application bandwidth;
- For the users that cannot be matched any role, do not implement QoS control.

For more information about how to configure a role, user, role-related class, and how to bind the QoS profile to an interface, see Example 10: IP QoS Priority.

Step 1: Configure application classes

```
hostname(config)# application-group p2p
hostname(config-svc-group)# application bt
hostname(config-svc-group)# application emule
hostname(config-svc-group)# application xunlei
hostname(config-svc-group)# application vagaa
hostname(config-svc-group)# application pplive
hostname(config-svc-group)# application kugoo
```

```
hostname(config-svc-group)# exit
hostname(config)# class-map http
hostname(config-class-map)# match application http
hostname(config-class-map)# exit
hostname(config)# class-map ftp
hostname(config-class-map)# match application ftp
hostname(config-class-map)# exit
hostname(config)# class-map p2p
hostname(config-class-map)# match application p2p
hostname(config-class-map)# exit
hostname(config)#
hostname(config)# role role1
hostname(config)# role role2
hostname(config)# role role3
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# user user1
hostname(config-user)# exit
hostname(config-aaa-server)# user user2
hostname(config-user)# exit
hostname(config-aaa-server)# user user21
hostname(config-user)# exit
hostname(config-aaa-server)# user user22
hostname(config-user)# exit
hostname(config-aaa-server)# user user23
hostname(config-user)# exit
hostname(config-aaa-server)# exit
```

```
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user user1 role role1
hostname(config-role-mapping)# match user user2 rolerole1
hostname(config-role-mapping)# match user user21 role role2
hostname(config-role-mapping)# match user user22 role role2
hostname(config-role-mapping)# match user user23 role role3
hostname(config-role-mapping)# exit
hostname(config)# aaa-server local type local
hostname(config-aaa-server)# role-mapping-rule rule1
hostname(config-aaa-server)# exit
hostname(config)# class-map class1
hostname(config-class-map)# match role role1
hostname(config-class-map)# exit
hostname(config)# class-map class2
hostname(config-class-map)# match role role2
hostname(config-class-map)# exit
hostname(config)# class-map class3
hostname(config-class-map)# match role role3
```

Step 2: Configure QoS profiles

```
hostname(config)# qos-profile app-qos
hostname(config-qos-profile)# class http
hostname(config-qos-prof-cmap)# bandwidth percent 40
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class ftp
hostname(config-qos-prof-cmap)# bandwidth percent 20
hostname(config-qos-prof-cmap)# exit
```

```
hostname(config-qos-profile)# class p2p
hostname(config-qos-prof-cmap)# police 32 conform-action transmit exceed-action drop
hostname(config)# qos-profile role-profile
hostname(config-qos-profile)# class class1
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 1000
hostname(config-qos-prof-cmap)# qos-profile app-qos
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class class2
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 4000
hostname(config-qos-prof-cmap)# qos-profile app-qos
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class class3
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 200
hostname(config-qos-profile)# exit
hostname(config)#
```

Example 13: Multi-level QoS

This section describes a multi-level QoS example.

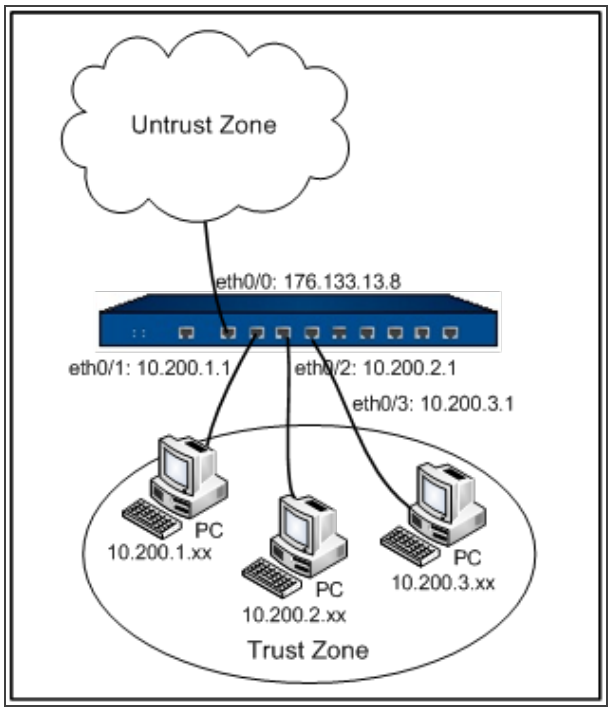
Requirement

The total bandwidth available to users is 600 M. During the peak hours, the amount of active PCs in the Intranet can reach 5000. The requirement for QoS is:

- When the bandwidth utilization reaches 85%, restrict the maximum bandwidth available to each user to 100 KB; when the network link is free, cancel the restriction. Besides, the bandwidth occupied by P2P traffic should not exceed 200 MB.

- Intelligent bandwidth allocation: When users are only downloading files by P2P software, all the bandwidth should be allocated to P2P, such as BT; however, if users are trying to browse WebPages later, the priority is to guarantee the HTTP bandwidth. The P2P download will still continue, but the available bandwidth will decrease.

The network topology is shown in the figure below:



Configuring First-level Application QoS

The first-level application QoS restricts the bandwidth for P2P traffic to 200M.

Step 1: In the policy rule, mark the P2P traffic with QoS tag 16

```
hostname(config)# servgroup p2p
hostname(config-svc-group)# service bt*
hostname(config-svc-group)# service emule*
hostname(config-svc-group)# service xunlei*
hostname(config-svc-group)# service vagaa*
hostname(config-svc-group)# service pplive*
```

```
hostname(config-svc-group)# service kugoo*
hostname(config-svc-group)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# policy-qos-tag 16
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service p2p
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure a QoS profile to restrict the P2P traffic

```
hostname(config)# class-map match-p2p
hostname(config-class-map)# match policy-qos-tag 16
hostname(config-class-map)# exit
```

```
hostname(config)# qos-profile p2p-limit
hostname(config-qos-profile)# class match-p2p
hostname(config-qos-prof-cmap)# police 200000 conform-action transmit exceed-action drop
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
```

Step 3: Bind the P2P QoS profile to the ingress interface of WAN

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile 1st-level input p2p-limit
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Configuring Second-level IP QoS

Step 1: Configure an IP QoS priority. The priority of HTTP should be higher than that of P2P

```
hostname(config)# class-map http
hostname(config-class-map)# match application http
hostname(config-class-map)# exit
hostname(config)# qos-profile ip-priority
hostname(config-qos-profile)# class http
hostname(config-qos-prof-cmap)# set ip-qos-priority 1
hostname(config-qos-profile)# class match-p2p
hostname(config-qos-prof-cmap)# set ip-qos-priority 5
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 2: Bind the priority QoS profile to interfaces

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# qos-profile 2nd-level input ip-priority
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# qos-profile 2nd-level input ip-priority
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# qos-profile 2nd-level input ip-priority
hostname(config-if-eth0/3)# exit
hostname(config)#
```

Step 3: Configure IP QoS

```
hostname(config)# class-map ip-range
hostname(config-class-map)# match ip-range 10.200.1.0 10.200.3.255
hostname(config-class-map)# exit
hostname(config)# qos-profile ip-qos-limit
hostname(config-qos-profile)# class ip-range
hostname(config-qos-prof-cmap)# ip-qos per-ip max-bandwidth 100
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# qos-profile 2nd-level output ip-qos-limit
hostname(config-if-eth0/0)# qos-profile 2nd-level input ip-qos-limit
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 4: Configure FlexQoS

```
hostname(config)# flex-qos low-water-mark 75 high-water-mark 85
```

Example 14: Comprehensive QoS Application

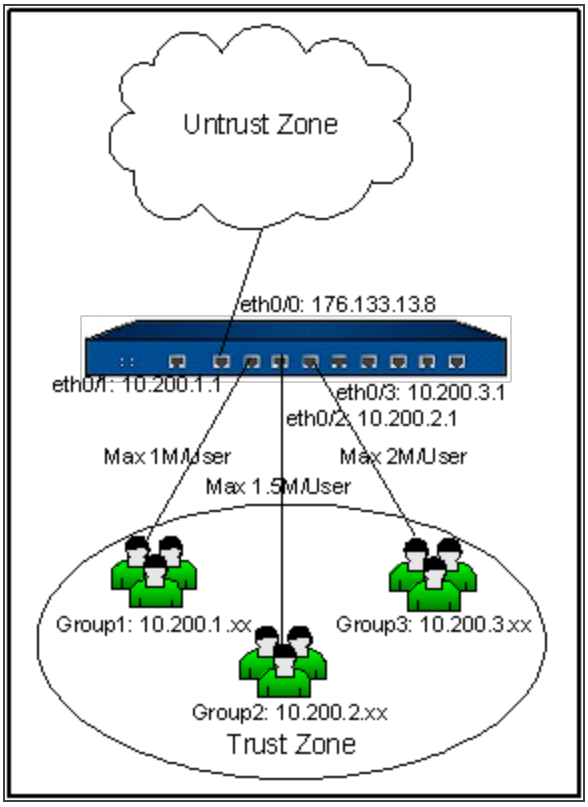
This section describes a comprehensive QoS application example. The goal is to control all the applications in the system, and restrict the total bandwidth and application bandwidth available to different users and applications.

Requirement

The total bandwidth available to users is 600M. The requirement for QoS is:

- Control the application bandwidth: the VoIP bandwidth ⩾ 15%, key business bandwidth ⩾ 30%, webpage browsing bandwidth ⩾ 20%; the P2P bandwidth should be 20M to 300M, specifically depending on the schedule.
- Control the bandwidth available to each user in the Intranet: the maximum bandwidth available to each user in Group1 is 1M; to each user in Group2 is 1.5M; to each user in Group3 is 2M.
- Implement fine-grained control on the bandwidth available to each user in the Intranet: the VoIP bandwidth = 15%, key business bandwidth = 30%, webpage browsing bandwidth = 20%, P2P bandwidth = 10%.

The network topology is shown in the figure below:



The requirement needs to be implemented by configuring multi-level QoS: the first-level QoS is used to control the applications, and the second-level QoS is used to control each user.

Configuration Steps

Step 1: Configure interfaces and security zones

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 176.133.13.8/32
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 10.200.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
```

```
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 10.200.2.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone trust
hostname(config-if-eth0/3)# ip address 10.200.3.1/24
hostname(config-if-eth0/3)# exit
hostname(config)# zone trust
hostname(config-zone-trust)# application-identify
hostname(config-zone-trust)# exit
hostname(config)#
```

Step 2: Configure users, user groups and roles

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user user1
hostname(config-user)# password 111111
hostname(config-user)# exit
hostname(config-aaa-server)# user user2
hostname(config-user)# password 222222
hostname(config-user)# exit
hostname(config-aaa-server)# user user3
hostname(config-user)# password 333333
hostname(config-user)# exit
hostname(config-aaa-server)# user-group group1
hostname(config-user-group)# member user user1
hostname(config-user-group)# exit
hostname(config-aaa-server)# user-group group2
```

```
hostname(config-user-group)# member user user2
hostname(config-user-group)# exit
hostname(config-aaa-server)# user-group group3
hostname(config-user-group)# member user user3
hostname(config-user-group)# exit
hostname(config-aaa-server)# exit
hostname(config)# role role1
hostname(config)# role role2
hostname(config)# role role3
hostname(config)# role-mapping-rule rule1
hostname(config-role-mapping)# match user-group group1 role role1
hostname(config-role-mapping)# match user-group group2 role role2
hostname(config-role-mapping)# match user-group group3 role role3
hostname(config-role-mapping)# exit
hostname(config)# aaa-server local
hostname(config-aaa-server)# role-mapping-rule rule1
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure a route and NAT rule

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0 0.0.0.0 176.133.13.1
hostname(config-vrouter)# snatrule from any to 176.133.13.8 trans-to eif-ip mode
dynamicport
hostname(config-vrouter)# exit
hostname(config)#
```

Step 4: Configure WebAuth and policy rules

```
hostname(config)# address authaddr
hostname(config-addr)# ip 10.200.0.0/16
hostname(config-addr)# exit
hostname(config)# address group1
hostname(config-addr)# ip 10.200.1.0/24
hostname(config-addr)# exit
hostname(config)# address group2
hostname(config-addr)# ip 10.200.2.0/24
hostname(config-addr)# exit
hostname(config)# address group3
hostname(config-addr)# ip 10.200.3.0/24
hostname(config-addr)# exit
hostname(config)# webauth
hostname(config-webauth)# enable
hostname(config-webauth)# protocal http
hostname(config-webauth)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr authaddr
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role unknown
hostname(config-policy-rule)# action webauth local
hostname(config-policy-rule)# exit
```

```
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr group1
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role role1
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr group2
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role role2
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr group3
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# role role3
hostname(config-policy-rule)# action permit
```

```
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 5: Configure schedules

```
hostname(config)# schedule working
hostname(config-schedule)# periodic daily 06:00 to 18:00
hostname(config-schedule)# exit
hostname(config)# schedule evening
hostname(config-schedule)# periodic daily 18:00 to 21:00
hostname(config-schedule)# exit
hostname(config)# schedule night
hostname(config-schedule)# periodic daily 21:00 to 06:00
hostname(config-schedule)# exit
hostname(config)#
```

Step 6: Configure QoS classes (The key businsess may vary from different environments. This section takes POP3 as the example)

```
hostname(config)# class-map voip
hostname(config-class-map)# match application SIP*
hostname(config-class-map)# match application SIP
hostname(config-class-map)# exit
hostname(config)# class-map critical
hostname(config-class-map)# match application POP3
hostname(config-class-map)# exit
hostname(config)# class-map websurf
hostname(config-class-map)# match application HTTP
hostname(config-class-map)# exit
```

```
hostname(config)# class-map p2p
hostname(config-class-map)# match application APP_P2P
hostname(config-class-map)# match application APP_P2P_STREAM
hostname(config-class-map)# exit
hostname(config)# class-map group1
hostname(config-class-map)# match role role1
hostname(config-class-map)# exit
hostname(config)# class-map group2
hostname(config-class-map)# match role role2
hostname(config-class-map)# exit
hostname(config)# class-map group3
hostname(config-class-map)# match role role3
hostname(config-class-map)# exit
hostname(config)#
```

Step 7: Configure application QoS profiles

```
hostname(config)# qos-profile p2p-fine-control
hostname(config-qos-profile)# class group1
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 8000 schedule working
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 80000 schedule evening
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 150000 schedule night
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class group2
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 8000 schedule working
```

```
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 80000 schedule evening
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 150000 schedule night
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class group3
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 8000 schedule working
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 80000 schedule evening
hostname(config-qos-prof-cmap)# role-qos share max-bandwidth 150000 schedule night
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)# qos-profile application
hostname(config-qos-profile)# class voip
hostname(config-qos-prof-cmap)# bandwidth percent 15
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class critical
hostname(config-qos-prof-cmap)# bandwidth percent 30
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class websurf
hostname(config-qos-prof-cmap)# bandwidth percent 20
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class p2p
hostname(config-qos-prof-cmap)# shape 20000 schedule working
hostname(config-qos-prof-cmap)# shape 150000 schedule evening
```

```
hostname(config-qos-prof-cmap)# shape 300000 schedule night
hostname(config-qos-prof-cmap)# qos-profile p2p-fine-control
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 8: Configure User QoS profiles

```
hostname(config)# qos-profile user-app-fine-control
hostname(config-qos-profile)# class voip
hostname(config-qos-prof-cmap)# bandwidth percent 15
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class critical
hostname(config-qos-prof-cmap)# bandwidth percent 30
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class websurf
hostname(config-qos-prof-cmap)# bandwidth percent 20
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class p2p
hostname(config-qos-prof-cmap)# bandwidth percent 10
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)# qos-profile user-qos
hostname(config-qos-profile)# class group1
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 1000
hostname(config-qos-prof-cmap)# qos-profile user-app-fine-control
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class group2
```

```
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 1500
hostname(config-qos-prof-cmap)# qos-profile user-app-fine-control
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# class group3
hostname(config-qos-prof-cmap)# role-qos per-user max-bandwidth 2000
hostname(config-qos-prof-cmap)# qos-profile user-app-fine-control
hostname(config-qos-prof-cmap)# exit
hostname(config-qos-profile)# exit
hostname(config)#
```

Step 9: Bind the QoS profiles

```
hostname(config)# zone untrust
hostname(config-zone-untrust)# qos 1st-level output application
hostname(config-zone-untrust)# qos 2nd-level input user-qos
hostname(config-zone-untrust)# qos 2nd-level output user-qos
hostname(config-zone-untrust)# exit
hostname(config)# zone trust
hostname(config-zone-trust)# qos 1st-level output application
hostname(config-zone-trust)# exit
hostname(config)#
```

Configuration Recommandations

The table below recommends different QoS configurations for different types of applcations to help you better understanduse the QoS function.

Application Characteristics	Example	Configuration Recommendation
Important real-time applications that occupy some bandwidth	VoIP, interactive video	Reserve sufficient bandwidth by using the command priority to assure that the reserved bandwidth will not be occupies by other applications.
Important real-time applications that occupy a little bandwidth	SNMP, Telnet	Guarantee the minumun bandwidth by the command bandwidth.
Non-important real-time applications that occupy most bandwidth	Email, file transfer	Guarantee the minumun bandwidth by using the command bandwidth, and also allow using the free bandwidth.
Non-important applications that occupy most bandwidth	P2P	Restrict the maximum bandwidth by using the command police.
Applications that occupy some bandwidth, but the importance may vary depending on different situations.	webgame	Important: Guarantee the minumun bandwidth by using the command bandwidth. Non-important: Restrict the maximum bandwidth by using the command police.

Load Balancing

This chapter introduces the following topics:

- server load balancing
- link load balancing

SLB

The Server Load Balancing (SLB) function can distribute traffic to different intranet servers by using load balancing algorithms, fully utilizing each intranet server and improving business processing capacities. The SLB function can be implemented by using one of the following methods:

- Balancing traffic to the specified port on different intranet servers: This is suitable for scenarios where different intranet servers provide the same application service on their respective specified port simultaneously.
- Balancing traffic to different ports on the same intranet server: This is suitable for scenarios where the same server runs multiple processes on different ports to provide the same application service.
- Combining the two methods above for traffic balancing.



Notes: The SLB function can be configured only by using the CLI. For more information, refer to *StoneOS CLI User Guide*.

Configuring Server Load Balancing

This topic consists of the following sections:

- Adding/Deleting SLB Server Pool
- Configuring Parameters for SLB Server Pool Entry
- Assigning an Algorithm for SLB

- Adding/Deleting Track Rule for SLB
- Configuring Minimum Working Servers
- Configuring Threshold Value
- Binding SLB Server Pool Entry to DNAT Rule

Adding/Deleting SLB Server Pool

A glocal SLB server pool is a database which stores the internal server IP ranges and the server names. The mapping between a server IP and the server name is called an SLB server pool entry.

The gobal SLB server pool includes SLB server pool entries. To add an entry into the global SLB server pool, under configuraiotn mode, use the following command:

slb-server-pool *pool-name* [**ipv6**]

- *pool-name* - Specify a name for SLB server pool entry.
- **ipv6** - Specify the type of SLB server pool entry is IPv6.

To delele an entry, use the command:

no slb-server-pool *pool-name*



Notes: Before deleting an entry, make sure this entry has not binding with any other items.

Configuring Parameters for SLB Server Pool Entry

Parameters of an SLB Server Pool Entry includes IP range, port, weight, and maximum connections. There are two types of IP range in SLB server pool

- IP address/netmask, e.g. 10.100.2.0/24
- IP address range, e.g. 10.100.2.3 – 10.100.2.100

- IPv6 address/Mask, e.g. 2000::2/127
- IPv6 address range, e.g. 2000::2 - 2000::5

To add members and configure detailed parameters for an SLB server pool entry of IPv4, under SLB server pool configuration mode, use the following command. You can add up to 256 members.

server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*]{**weight-per-server** *weight-num*} [**max-connection-per-server** *max-num*][**priority** *value*]

- **ip** *ip-address* – Specify IPv4 address and netmaks.
- **ip-range** *start-ip* [*max-ip*] – Specify IPv4 address range, *start-ip* is start IP address and *end-ip* is end IP address.
- **port** *port-num* – Specify port number.
- **weight-per-server** *weight-num* – Specify the weight in load balance. The range is from 1 to 255.
- **max-connection-per-server** *max-num* – Specify the maximum connection number for a server. The range is from 1 to 1,000,000,000 and default value is 0, which mean no limit on maximum connection.
- **priority** *value* – Specifies server priority. The value range is from 1 to 100. The default value is 1. The bigger the number is, the higher priority the server has.

To delete an entry in SLB server pool of IPv4, use the following command:

no server {**ip** *ip/netmask* | **ip-range** *min-ip* [*max-ip*]} [**port** *port-num*]{**weight-per-server***weight-num*} [**max-connection-per-server** *max-num*][**priority** *value*]

To add members and configure detailed parameters for a SLB server pool entry of IPv6, under SLB server pool configuration mode, use the following command. You can add up to 256 members.

server {**ipv6***ipv6-address/Mask* | **ipv6-range***min-ipv6-address* [*max-ipv6-address*]} [**port***port-num*]{**weight-per-server***weight-num*} [**max-connection-per-server***max-num*][**priority** *value*]

- **ipv6***ipv6-address/Mask* – Specify IPv6 address and prefix length.
- **ipv6-range***min-ipv6-address* [*max-ipv6-address*] – Specify IPv6 address range, *min-ipv6-address* is start IP address and *max-ipv6-address* is end IP address.
- **port** *port-num* – Specify port number.
- **weight-per-server***weight-num* – Specify the weight in load balance. The range is from 1 to 255.
- **max-connection-per-server** *max-num* – Specify the maximum connection number for a server. The range is from 1 to 1,000,000,000 and default value is 0, which mean no limit on maximum connection.
- **priority** *value* – Specifies server priority. The value range is from 1 to 100. The default value is 1. The bigger the number is, the higher priority the server has.

To delete an entry in SLB server pool of IPv6, use the following command:

no server {**ipv6***ipv6-address/Mask*| **ipv6-range***min-ipv6-address* [*max-ipv6-address*]} [**port***port-num*]

Assigning an Algorithm for SLB

The system supports three types of SLB algorithms: weighted hash algorithm, weighted round robin, and weighted least connection. By default, weight hash algorithm is used.

To apply an algorithm, in the SLB server pool configuration mode, use the following command:

load-balance-algorithm {**weighted-hash** | **weighted-round-robin** [**sticky** [**timeout** *value*]] | **weighted-least-connection** [**sticky** [**timeout** *value*]]}

- **weighted-hash** - Specify weighted hash as SLB algorithm.
- **weighted-round-robin** - Specify weighted round robin as SLB algorithm.
- **weighted-least-connection** - Specify weighted least connection as SLB algorithm.

- **sticky** [**timeout** *value*] − If you use sticky, all sessions from the same source IP will be mapped to one server.**timeout** *value*Specify the keepalive time of the session mapping, that is, during the specified time, sticky is effective. When the Sticky function is used on X series devices and K9180 devices, you need to run the **session-schedule-mode src-ip** command in the flow configuration mode to make the Sticky function take effect.

Adding/Deleting Track Rule for SLB

To add a track rule for SLB, under SLB server pool configuration mode, use the following command:

monitor{**track-ping** | {**track-tcp** |**track-udp** }[**port** *port-num*]} [**src-interface***interface_name*] **interval** *interval-value* **threshold** *number* **weight** *weight-num*

- **track-ping** - Specify the track protocol type as PING.
- **track-tcp** - Specify the track protocol type as TCP.
- **track-udp** - Specify the track protocol type as UDP.
- **port** *port-num* - Specify the track port number. The range is from 0 to 65535.
    - When the members in the SLB server pool have the same IP address and different ports, you don't need to specify the port when configuring the track rule. The system will track each IP address and its port in the SLB server pool.
    - When there is a member whose port is not configured exists in the SLB sever pool, you must specify the port when configuring the track rule. The system will track the specified port of the IP addresses in the SLB server pool.
    - When the members in the SLB server pool are all configured with IP addresses and ports and these configured IP addresses are different from each other, you can select whether to specify the port when configuring the track rule. If specified, the system will track the specified port of these IP addresses. If not, the system will track the configured ports of the IP addresses of the members.

- **src-interface***interface_name* - Specify the source interface of the track rule. The system will use the IP address of the specified interface as the source IP address to send Ping/TCP/UDP messages. To cancel the specification of the source interface of the track rule, delete the corresponding parameters of **src-interface** and *interface_name*, and then execute again the command for adding track rule for SLB .
- **interval** *interval-value* - Specify the interval of track packets. The range is 1 to 255.
- **threshold** *number* - Specify the threshold which determines if track object failes or not. If the system cannot get respond within the threshold packet number, the track object will be deemed as failure, i.e. the object cannot be reached. The range of threshold is 1 to 255. The default number is 3.
- **weight** *weight-num* - Specify the weight of the current track object. The weight determines if the whole track is failed or not when this object fails. The weight range is 1 to 255.

To delete an SLB track rule, use the no command below:

no monitor{**track-ping** | {**track-tcp** |**track-udp** }[**port** *port-num*]}

Configuring Minimum Working Servers

The system checks from high priority to low priority according to the configured minimum number of working servers. When the number of working servers within the current priority range meets the minimum requirement, the working servers within that priority range will participate in traffic distribution. If the minimum number of working servers is not met, or if the status of one of the servers becomes unreachable resulting in the number of working servers in the current priority range being less than the minimum threshold, the system will continue to check the servers in the next lower priority range until the minimum number of working servers is met. To specify the minimum working servers, in the SLB server pool configuration mode, use the following command:

minmum-working-servers*value*

- *value* − Specifies the minimum working servers. The value range is from 1 to 256. The default value is 256.

To delete the configured minimum number of working servers, use the following command:

no minmum-working-servers

Configuring Threshold Value

When the weight sum of all track objects exceed the threshold, the server is deemed as failed. To specify the threshold, under SLB server pool configuration mode, use the following command:

monitor threshold *number*

- *number* - Specify threshold value. The range is from 1 to 255.

Binding SLB Server Pool Entry to DNAT Rule

SLB server pool entry can be bound to DNAT rule to achieve server load balancing.

To bind an SLB server pool entry to a DNAT rule, under VRouter configuration mode, use the following command:

dnatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**service** *service-name*] **trans-to** *trans-to-address* [**slb-server-pool** *pool-name*][**port** *port*] [**load-balance**] [**track-tcp** *port*] [**track-ping**] [**log**] [**group** *group-id*] [**description** *description*]

- **slb-server-pool** *pool-name* – Specify the name of SLB server pool entry, you can refer to the IPv4 or IPv6 type SLB server pool entry.



Tip: For information about how to set up DNAT rules, see "Creating a DNAT Rule" in the "Firewall"

Viewing SLB Status

To view SLB server pool entry and track rule, under any mode, use the following command:

show slb-server-pool *pool-name*

- *pool-name* – Specify SLB server pool entry name.

To view SLB server, under any mode, use the following command:

show load-balance server

To view SLB DNAT:

show load-balance slb-server-pool *pool-name*

To view SLB DNAT rule, under any mode, use the following command:

show load-balance rule

LLB

For multiple ISP links, the system uses real-time link monitoring technology and dynamic link detection technology to distribute traffic reasonably across different links, reducing network latency, jitter, and packet loss rate on each link, achieving a more balanced bandwidth utilization. You can enable LLB respectively for outbound and inbound traffic. Two different dynamic link detection technologies are used for outbound and inbound traffic, namely real-time link monitoring technology for outbound traffic and SmartDNS technology for inbound traffic. Based on the detection results, automatic load balancing of traffic is achieved.

This topic consists of the following sections:

- "Inbound Link Load Balancing" on Page 2054
- "Outbound Link Load Balancing" on Page 2038
- "Example of Configuring LLB" on Page 2059 (via CLI)

Outbound Link Load Balancing

In the outbound direction, the system implements intelligent routing based on real-time monitoring of the latency, jitter, packet loss rate, and bandwidth utilization of each link, and dynamically adjusts the traffic load on each link. You can configure flexibleSLA profiles and LLB Profiles and bind them with routing (the system only supports destination-based routes and policy-based routes) to form LLB rules, which can control and load balance outbound link traffic.

Outbound Load Balancing Implementation Mechanism

Outbound load balancing implementation mechanism is as follows:

1. Based on business requirements, users customize the SLA link quality measurement criteria. The system will dynamically detect the quality of outbound links in real time, including

latency, jitter, and packet loss rate, and compare them with the thresholds set in the profile to filter available outbound links.

2. The LLB further optimizes the selected available outbound links (Links that meet the SLA measurement criteria) by comprehensively calculating the cost of each link based on key parameters such as latency weight, packet loss weight, jitter weight, and bandwidth weight.
3. The system allocates more outbound traffic to links with lower costs while reducing traffic allocation on links with higher costs, achieving efficient and balanced outbound traffic load.
4. If none of the links meet the SLA measurement criteria, the LLB will forward traffic based on the cost of all links.

Configuration Method

Please follow the steps below to configure outbound load balancing:

- Configure an LLB profile

  The LLB profile contains parameters for load balancing algorithms, allowing you to flexibly configure settings such as balancing mode, bandwidth utilization threshold, detection switch, detection mode, balancing direction, and the impact factor of link Cost value. The system will select links and balance traffic based on the configured parameters:

  - If the balancing mode is the compatibility mode, the system will select the original link (cached link) for traffic forwarding. This mode is suitable for businesses sensitive to link switching, such as banking services.
  - If network detection is enabled, the system will detect the network link status based on configured parameters to select the optimal link:
    - When the link's bandwidth utilization is below the specified threshold, the system calculates link quality based on latency weight, packet loss weight, and jitter weight, prioritizing links with a higher quality.

- When the link's bandwidth utilization exceeds the specified threshold, the system calculates link quality based on latency weight, packet loss weight, jitter weight, bandwidth weight, link bandwidth, and bandwidth utilization, prioritizing links with a higher quality.

- If network detection is enabled and LLB rules are bound to a domain name book, the system will use real-time detection technology for domain names to ensure more accurate route selection. This method is suitable for link selection within specific domain name:

  - When the link's bandwidth utilization is lower than the specified threshold, the system calculates link quality based on latency weight, prioritizing links with a higher quality.

  - When the link's bandwidth utilization exceeds the user-defined threshold, the system calculates link quality based on latency weight, bandwidth weight, link bandwidth, and bandwidth utilization, prioritizing links with a higher quality.



Notes: By default, network detection is enabled. You can use the **show llb profile** command to view the status of network detection. If the function is disabled, it can be enabled by using the **detect enable** command.

- Configure an LLB rule

  By configuring LLB rules, LLB profiles are bound to routes (the system only supports destination-based routes and policy-based routes) to control and load balance outbound link traffic.

If you need to filter the outbound links for traffic based on customized link quality criteria (such as latency, jitter, and packet loss rate), you can configure an SLA Profile. By using the SLA Profile to filter out links that meet the SLA standards, and binding the SLA Profile together with the LLB Profile to the route, you can achieve more precise control and balancing of link traffic.

Configuring Outbound Link Load Balancing

Configuring SLA Profile

To create or configure an SLA profile, use the following command in the global configuration mode:

sla-profile*profile-name*

- *profile-name* – Specifies the name of the SLA profile. After you execute this command, the system creates an SLA profile with the specified name and enters the SLA profile configuration mode. If the specified name already exists, the system will directly enter the SLA profile configuration mode.

To delete the specified SLA profile, in the global configuration mode, use the command: **no sla-profile***profile-name*.

Enabling or Disabling SLA Function

In SLA profile configuration mode, the SLA function is enabled by default. To enable or disable it, use the following command:

sla-status {**disable** | **enable**}

- **disable** – Disable the SLA function.
- **enable** – Enable the SLA function.

Configuring Detection Mode

SLA detection modes include passive detection mode and active detection mode:

- Passive detection mode: The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.

- Active detection mode: In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.

To set the detection mode to passive detection mode, in SLA Profile configuration mode, use the following command:

detect-mode passive type {**ipv4** | **ipv6**}

- **ipv4** | **ipv6** - Specifies the IP type of passive detection, which can be IPv4 or IPv6. The default type is IPv4.

To set the detection mode to active detection mode, in SLA Profile configuration mode, use the following command:

detect-mode active type {**ipv4** {**domain-name***domain-name* | **ipv4-addr***A.B.C.D*} **protocol** {**icmp** | **tcp port***port-number*} | **ipv6** {**domain-name***domain-name* | **ipv6-addr***X:X:X:X::X*} **protocol** {**icmp6** | **tcp port***port-number*} [**interval***num* [**number***num*]]

- **ipv4** {**domain-name***domain-name* | **ipv4-addr***A.B.C.D*} **protocol** {**icmp** | **tcp port***port-number*} - Sets the type of active detection mode to IPv4 and configure the following parameters:
  - **domain-name***domain-name* | **ipv4-addr***A.B.C.D* - Specifies the destination address for detection packets in active detection mode, which can be an IPv4 address or a domain name.
  - **protocol** {**icmp** | **tcp port***port-number*} - Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP or TCP, with ICMP being the default. When you select TCP, you need to enter a TCP port number.
- **ipv6** {**domain-name***domain-name* | **ipv6-addr***X:X:X:X::X*} **protocol** {**icmp6** | **tcp port***port-number* - Sets the type of active detection mode to IPv6 and configure the following parameters:

- **domain-name***domain-name* | **ipv6-addr***X:X:X:X::X* - Specifies the destination address for detection packets in active detection mode, which can be an IPv6 address or a domain name.
- **protocol** {**icmp6** | **tcp port***port-number*} - Specifies the protocol type for sending detection packets in active detection mode, which can be ICMPv6 or TCP, with ICMPv6 being the default. When you select TCP, you need to enter a TCP port number.

- **interval***num* - Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
- **number***num* - Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.

Configuring SLA Threshold

To configure SLA threshold, in SLA Profile configuration mode, use the following command:

threshold {**delay-thres***num*| **jitter-thres***num* | **lossrate-thres***num*}

- **delay-thres***num* - Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
- **jitter-thres***num* - Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
- **lossrate-thres***num* - Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.

To restore the SLA threshold to default values, in SLA Profile configuration mode, use the command: **no threshold** {**delay-thres**| **jitter-thres** | **lossrate-thres**}.

Configuring Success Times Required For Activation

The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. To configure the success times required for activation, in SLA Profile configuration mode, use the following command:

activation*num*

- *num* - Specifies the number of success times required for activation. Valid values: 1 to 100. Default value: 5.

To restore the number of success times required for activation to the default value, in SLA Profile configuration mode, use the command: **no activation**.

Configuring Failed Times Required For Deactivation

The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. To configure the failed times required for deactivation, in SLA Profile configuration mode, use the following command:

inactivation*num*

- *num* - Specifies the number of failed times required for deactivation. Valid values: 1 to 100. Default value: 5.

To restore the number of failed times required for deactivation to the default value, in SLA Profile configuration mode, use the command: **no inactivation**.

Configuring LLB Profile

The LLB profile contains the parameters of the load balancing algorithm, such as bandwidth utilization threshold, probe switch, probe mode, and equalization direction.

To create or configure an LLB profile, use the following command in the global configuration mode:

llb profile *llb-profile-name*[**ipv6**]

- *llb-profile-name* – Specifies the name of the LLB profile. After you execute this command, the system creates an LLB profile with the specified name and enters the LLB profile configuration mode. If the specified name already exists, the system will directly enter the LLB profile configuration mode.
- **ipv6** – Specifies the type of the LLB Profile as IPv6. If not specified, the type of the LLB Profile is IPv4.

To delete the specified LLB profile, in the global configuration mode, use the command: **no llb profile** *llb-profile-name*.



Notes: The LLB Profile name in the IPv4 should be different from that in IPv6.

In LLB profile configuration mode, the detect function is enabled by default. To enable or disable it, use the following command:

detect {**disable** | **enable**}

- **disable** – Disables the detect function, the system adjusts the routing link according to the bandwidth occupancy of each egress link, and the link with low bandwidth occupation rate is preferred.
- **enable** – Enables the detect function. When the detect function is enabled, the system detects the network link status according to the parameters configured by the user and then selects the optimal route. The priority is as follows:

1. When the link bandwidth occupancy rate is lower than the specified bandwidth threshold specified, the system will only calculate the link quality based on delay, packet loss and jitter, and select the link with high quality first.

2. When the link bandwidth occupation rate is higher than the specified bandwidth threshold, the system will combine delay, packet loss, jitter and bandwidth occupation rate to calculate the link quality, and select the link with high quality first.

When the type of the LLB Profile is specified as IPv4, , you can configure the related parameters as required. In LLB profile configuration mode, use the following command:

detect { **netmask** {*A.B.C.D* | *num*} | **threshold***value* | **max-entry-number***num* | **weight-update-interval***interval* | **weight-factors** {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factorjitter-factorloss-rate-factorbw-rate-factor*}

- **netmask** {*A.B.C.D* | *num*} - Specifies the detection subnet. The system will monitor the traffic in real time based on the subnet. The traffic of the same subnet will choose the same link. The system supports two formats, A.B.C.D or num. The value of A.B.C.D ranges from 255.0.0.0 to 255.255.255.255, and the default value is 255.255.240.0; num ranges from 8 to 32 and defaults to 28.

- **threshold** *value* − Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth, system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.

- **max-entry-number***num* - Specify the maximum value of the subnet entry. The lower range limit is 2000, and the upper range limit is determined according to different platforms. . Subnet entry is an entry that contains the detection results and weight values for all links in each destination subnet. When the specified maximum value is exceeded, the saved subnet entry is deleted dynamically.

- **weight-update-interval***interval* - Specifies the update cycle for the subnet entry weight, which ranges from 1 to 300 seconds, with a default of 10 seconds.
- **weight-factors** {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factorjitter-factorloss-rate-factorbw-rate-factor*} - Specifies the weight-factors of the Cost value of the link. "weight-factors" is used to calculate the Cost value of a link, including parameters such as latency, jitter, packet loss rate, and bandwidth weight. These factors indicate the proportion of weight that latency, jitter, packet loss rate, and bandwidth have on the Cost value of the link. You can select a predefined template or customize weight factors.
  - **delay-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 10, 2, 4, and 1, respectively, indicating that latency has the greatest impact on the Cost value of the link.
  - **jitter-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 10, 4, and 1, respectively, indicating that jitter has the greatest impact on the Cost value of the link.
  - **loss-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 2, 10, and 1, respectively, indicating that packet loss rate has the greatest impact on the Cost value of the link.
  - *delay-factorjitter-factorloss-rate-factorbw-rate-factor* - Customizes the weight of latency, jitter, packet loss rate, and bandwidth of the link. Valid values: 0 to 15. Default value: *delay-factor*: 1; *jitter-factor*: 2; *loss-rate-factor*: 4; *bw-rate-factor*: 1.

To restore the default values of the related parameters, use the command **nodetect** { **netmask** | **threshold** | **max-entry-number** | **weight-update-interval** | **weight-factors** }.

When the type of the LLB Profile is specified as IPv6, you can configure the related parameters as required. In LLB Profile configuration mode, use the following commands:

detect { **prefix***prefix-len* | **threshold***value* | **max-entry-number***num* | **weight-update-interval***interval* | **weight-factors** {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factorjitter-factorloss-rate-factorbw-rate-factor*}

- **prefix***prefix-len* – Specifies prefix length. The system will monitor the traffic in real time based on the prefix length. The traffic with the same prefix length will choose the same link. The value range of prefix len is 64 to 96, and the default value is 64.
- **threshold***value* – Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth, system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.
- **max-entry-number***num* - Specify the maximum value of the subnet entry. The lower range limit is 2000, and the upper range limit is determined according to different platforms. Subnet entry is an entry that contains the detection results and weight values for all links in each destination subnet. When the specified maximum value is arrived, the saved subnet entry is deleted dynamically.
- **weight-update-interval***interval* - Specifies the update cycle for the subnet entry weight, which ranges from 1 to 300 seconds, with a default of 10 seconds.
- **weight-factors** {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factorjitter-factorloss-rate-factorbw-rate-factor*} - Specifies the weight-factors of the Cost value of the link. "weight-factors" is used to calculate the Cost value of a link, including parameters such as latency, jitter, packet loss rate, and bandwidth weight. These factors indicate the proportion of weight that latency, jitter, packet loss rate, and bandwidth have on the Cost value of the link. You can select a predefined template or customize weight factors.
    - **delay-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 10, 2, 4, and 1, respectively, indicating that latency has the greatest impact on the Cost value of the link.

- **jitter-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 10, 4, and 1, respectively, indicating that jitter has the greatest impact on the Cost value of the link.
- **loss-template** - In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 2, 10, and 1, respectively, indicating that packet loss rate has the greatest impact on the Cost value of the link.
- *delay-factorjitter-factorloss-rate-factorbw-rate-factor* - Customizes the weight of latency, jitter, packet loss rate, and bandwidth of the link. Valid values: 0 to 15. Default value: *delay-factor*: 1; *jitter-factor*: 2; *loss-rate-factor*: 4; *bw-rate-factor*: 1.

To restore the default values of the related parameters, use the command **nodetect** { **prefix** | **threshold** | **max-entry-number** | **weight-update-interval** | **weight-factors** }.

When the bandwidth utilization of the link exceeds the specified limit, the system will record the logs. To record the logs, use the following command:

log enable [**utilization-limit***utilization-limit*]

- **utilization-limit***utilization-limit* - Specifies the limit value of link bandwidth utilization, the range is 1 to 100. The default value is 90.

Use the command **no log enable** to cancel recording logs.

To configure the load balancing direction, use the following command:

bandwidth-balance-direction {**bidirection** | **downstream** | **upstream**}

- **bidirection** – The system will compare the maximum bandwidth utilization ratio with the bandwidth utilization threshold in the two directions of data flow into and out, and then adjust the routing method.
- **downstream** – The system will compare the bandwidth utilization of the data stream into the bandwidth utilization threshold, and then adjust the routing method.

- **upstream** - The system will compare the bandwidth utilization of the data stream out the bandwidth utilization threshold, and then adjust the routing method.

To restore the default mode of the load balancing direction, use the command **no bandwidth-balance-direction**.

To configure the load balancing mode, use the following command:

mode {**compatibility** [**upper-limit***upper-limit-value***lower-limit***lower-limit-value*]| **performance**}

- **compatibility** – Configure the load balancing mode to work in high compatibility mode. When the link load changes, the system does not switch the link frequently, but ensures that the service is as far as possible on the previous link, such as banking services.
    - **upper-limit***upper-limit-value***lower-limit***lower-limit-value*- In the high compatibility mode, the system records the source, destination, output interface and other information into the cache. If the bandwidth of the link exceeds *upper-limit-value*and the other links are lower than *lower-limit-value*, the system will delete all caches of the link. The default value of **upper-limit**is 95, and the default value of **lower-limit**is 90.
- **performance** – Configure the load balancing mode for high-performance. In this mode, the system adjusts link to keep the link balance as fast as possible.

To restore the default mode of the load balancing mode, use the command **no mode**.

For more information about configuring load balancing, use the following command:

description*description*

- *description* – Configure Additional details of llb profile.

To cancel the configuration description, use the command: **no description**.

The active link detection interval is the interval at which the system sends detection packets to the specified host. To configure the link detection interval, use the following command:

host-detect interval*interval*

- *interval*- Specifies the link detection interval. The range is 60 to 86400s. The default value is 600s.

To restore the default value of the link detection interval, use the following command:

no host-detect interval

Viewing the Link Detection Result for a Specified Domain Name

To view the link detection result for a specified domain name, in any mode, use the following command:

show llb rule [*rule-name*] **spec-host task** { **all** | *host-name*} [**slot***slot-number*]

- **rule** [*rule-name*] – Specifies the LLB rule name.
- **spec-host task** { **all** | *host-name*} - View the link detection result for a specified domain name
  - **all**- View link detection results of all domain names in the LLB rule.
  - *host-name*- Specify the domain name and view the link detection result of this domain name.
- **slot***slot-number* - Specify the slot number of the module card. View the link detection result of all domain names (*all*) or the specified domain name (*host-name*) on the module card. This parameter is only supported on X-Series devices.

Configuring LLB Rule

After you bind SLA profile (optional) and LLB profile to the route to form an LLB rule, you can control and load balance outbound link traffic. Currently the system support binding destination routing (DBR) and policy-based routing (PBR). To configure LLB rules, use the following command in global mode:

llb rule*rule-name* [**ipv6**] {**pbr***pbr-name***id***match-id* | **dbr** [**vrouter***vr-name*] {{*X:X:X:X::X/M*} | {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}} {**profile***profile-name*} [**sla-profile***profile-name*] [**host** *host-book-name*]

- *rule-name* – Specify the name of llb rule.
- **ipv6** – Specifies the type of the LLB Rule as IPv6. If not specified, the type of the LLB Rule is IPv4.
- **pbr** *pbr-name* – Specify the name of PBR.
- **id***match-id* – Specify the match id of PBR. The IP type of PBR rule should be the same as the LLB Rule. If the IP tyoe of LLB Rule is IPv6, the IP type of PBR rule should be IPv6 as well.
- **dbrvrouter***vr-name* – Specify the vroute's name of DBR.
- {*X:X:X:X::X/M*} | {*A.B.C.D/M* | *A.B.C.D A.B.C.D* } – Specifies the Vrouter destination address. When the type of the LLB Rule is specified as IPv6, use *X:X:X:X::X/M* to configure the destination address of Vrouter. When the type of the LLB Rule is specified as IPv4, the device supports two modes, A.B.C.D / M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **profile***profile-name* – Specifies the bound LLB profile. The IP type of the LLB Profile should be the same as the LLB Rule.
- **sla-profile***profile-name* - Specifies the bound SLA profile. You need to select an SLA profile of the same type based on the IP type configured for the LLB rule.
- **host** *host-book-name* - Specifies the bound host book.

To delete the specified LLB rule,in the global configuration mode, use the command: **no llb rule***llb-rule-name*.



Notes: The LLB Rule name in the IPv4 should be different from that in IPv6.

Viewing LLB Rule Configuration Information

To view information about LLB rule configurations, in any mode, use the following command:

show llb rule [*rule-name*]

- *rule-name* – Displays the LLB rule configuration information of the specified name. If not specified, configuration information of all LLB rules is displayed.

Viewing Link Detection Results of Specified Domain

To view link detection results of the specified domain name, in any mode, use the following command:

show llb rule*rule-name***spec-host task** {**all** | *host-name*} [**slot***slot-number*]

- *rule-name* – Specifies the LLB rule name.
- **spec-host task** { **all** | *host-name*} - Displays the link detection results based on the specified domain name.
    - **all**- Displays link detection results of all domain names in the LLB rule.
    - *host-name*- Specifies the domain name to view its link detection results.
- **slot***slot-number* - Specifies the slot number of the module card to view link detection results of the module card based on all domain names (*all*) or specified domain name (*host-name*). This parameter is available only for X-series devices.

Viewing LLB Profile Configuration Information

To view LLB Profile configuration information, in any mode, use the following command:

show llb profile [*profile-name*]

- *profile-name* – Displays the LLB profile configuration information of the specified name. If not specified, configuration information of all LLB profiles is displayed.

Viewing SLA Profile Configuration Information

To view SLA Profile configuration information, in any mode, use the following command:

show sla-profile [*profile-name*]

- *profile-name* – Displays the SLA profile configuration information of the specified name. If not specified, configuration information of all SLA profiles is displayed.

Inbound Link Load Balancing

After enabling the LLB for inbound traffic, the system will resolve domains of different IPs based on the sources of the DNS requests and return IPs for different ISPs to the corresponding users who initiate the requests, which reduces access across ISPs. Such a resolution method is known as SmartDNS.

You can enable inbound LLB by the following steps:

1. Enable SmartDNS. This is the prerequisite for the implementation of inbound LLB.
2. Configure a SmartDNS rule table. The smart domain-to-IP resolution is implemented based on the rule table.

Configuring Inbound Link Load Balancing

Enabling SmartDNS

SmartDNS is enabled by default. To disable or enable the function, in the global configuration mode, use the following command:

llb inbound smartdns {**disable** | **enable**}

- **disable** – Disables SmartDNS.
- **enable** – Enables SmartDNS.

Configuring a SmartDNS Rule Table

The configuration of SmartDNS rule table includes creating a rule table, specifying the domain name, return IP and matching rule. The system resolves domains names into IPs of different ISP links based on the matching rule.

Creating a SmartDNS Rule Table

To create a SmartDNS rule table, in the global configuration mode, use the following command:

llb inbound smartdns *name*

- *name* – Creates a SmartDNS rule table, and enters SmartDNS rule table configuration mode. If the specified name already exists, the system will directly enters the SmartDNS rule table configuration mode. The system supports up to 2500 SmartDNS rule tables.

To delete the specified SmartDNS rule table, in the global configuration mode, use the following command:

no llb inbound smartdns *name*

Specifying the Domain Name

To specify the domain name that will be resolved smartly, in the SmartDNS rule table configuration mode, use the following command:

domain *domain-name*

- *domain-name* – Specifies the domain name that will be resolved smartly. The length is 1 to 255 characters.

Repeat the above command to add multiple domain names to the SmartDNS rule table. Each rule table supports up to 64 domain names (case insensitive).

To delete the specified domain name, in the SmartDNS rule table configuration mode, use the following command:

no domain *domain-name*

Specifying the Return IP

You can specify different return IPs for requests originating from different ISP links. The system determines the request sources based on the addresses in the ISP route (ISP static address). If the address of request source matches any entry of the above addresses, then the system will return the specified IP. In the SmartDNS rule table configuration mode, use the following command:

ip *ip-address* **isp** *isp-name* [**interface** *interface-name*] [**weight** *value*]

- *ip-address* – Specifies the return IP. You can configure up to 64 IPs for a domain name.
- **isp** *isp-name* – Specifies the ISP to which the request source address will be matched. If the source address matches any address entry of the ISP, the system will return the specified IP (**ip** *ip-address*). `isp-name` should be a predefined or user-defined ISP profile in the system. Each ISP can correspond to up to 16 IPs.
- **interface** *interface-name* – Specifies the inbound interface for the return IP address. System will judge whether the return IP address is valid according to the track result or the protocol status of the inbound interface. Only the valid IP address will be returned to the request source. When there's track object configured on the inbound interface, if the track status is successful, the return IP address is valid. Otherwise the IP address is invalid. When there's no track object configured on inbound interface, if the protocol state of the interface is UP, the return IP address is valid. Otherwise the IP address is invalid. If you don't specify the inbound interface for the return IP address, the return IP address is always valid.
- **weight** *value* – Specifies the weight of the return IP. The value range is 1 to 100. The default value is 1. In the SmartDNS rule table, one domain name might correspond to multiple IPs. The system will sort the IPs based on the weight and then return to the users.

To delete the specified return IP address, in the SmartDNS rule table configuration mode, use the following command:

no ip *ip-address*



Notes:

- The ISP route being referenced by the SmartDNS rule table cannot be deleted. For more information about ISP route, see "ISP Route" in the "Route".
- Before completing the configuration of domain name, return IP, etc., the new SmartDNS rule table will be disabled.

Viewing LLB Configuration

To view the outbound LLB configuration, in any mode, use the following command:

show llb {**profile** [*profile-name*] | **rule** [*rule-name*]}

- **profile** [*profile-name*] – Shows the profile of outbound LLB.
- **rule** [*rule-name*] – Shows the rule of outbound LLB.

To view the configuration of inbound or the specified SmartDNS rule table, in any mode, use the following command:

show llb inbound [**smartdns** *name*]

- **inbound** – Show the configuration of inbound LLB.
- **smartdns***name* – Specifies the name of SmartDNS rule table.

For example, to view the configuration of SmartDNS rule table named test, use the command **show llb inbound smartdns***test*. Below is a return example:

```
hostname# show llb inbound smartdns test
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active; I: inactive
=============================================================-
======================

----------------------------------------------------------------------
table name: test
table status: enable
domain count: 1
rule count: 1
domains: www.test.com;
ip addresses:
----------------------------------------------------------------------
IP ISP IF PROX TRACK W S
1.1.1.1 China-telecom ethernet0/1 E 1 I
=============================================================-
====================
```

- For more information about the track object under TRACK, see "Configuring a Track Object" in the "System Management"
- The rule status displayed under S can be active or inactive, specifically relying on the configured interface and track object on the interface:
    - If only ISP (**isp** isp-name) is configured while interface (**interface** *interface-name*) is not configured, then the rule status will always be active;

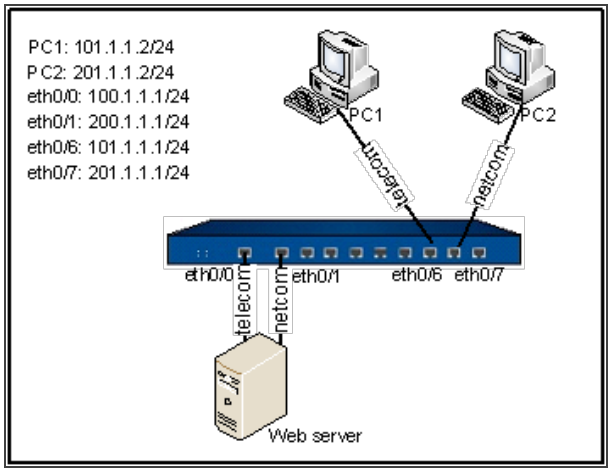
- If interface (**interface** *interface-name*) is configured but it is not configured with track object, then the rule status will be active when the protocol status of the interface is UP, and will be inactive when the protocol status is DOWN;
- If interface (**interface** *interface-name*) is configured and it is configured with track object, then the rule status will be active when track succeeds, and will be inactive when track fails.

Example of Configuring LLB

This section describes an inbound LLB configuration example.

Requirement

Ethernet0/6 and ethernet0/7 are connected to telecom and netcom links respectively. With inbound LLB enabled, the device will return the IP address defined in the ISP static address named telecom after receiving a DNS request from netcom users, and will return the IP address defined in the ISP static address named telecom after receiving a DNS request from telecom users. The network topology is shown below:



Configuration Steps

Configurations of interfaces are omitted. Only the configurations of ISP information and inbound LLB are provided.

Step 1: Configure ISP information

```
hostname(config)# isp-network telecom
hostname(config-isp)# 101.1.1.0/24
hostname(config-isp)# exit
hostname(config)# isp-network netcom
hostname(config-isp)# 201.1.1.0/24
hostname(config-isp)# exit
```

Step 2: Enable SmartDNS and configure SmartDNS rules

```
hostname(config)# llb inbound smartdns enable
hostname(config)# llb inbound smartdns test
hostname(config-llb-smartdns)# domain www.test.com
hostname(config-llb-smartdns)# ip 100.1.1.2 isp telecom interface ethernet0/0 weight 10
hostname(config-llb-smartdns)# ip 200.1.1.2 isp netcom interface ethernet0/1 weight 10
hostname(config-llb-smartdns)# exit
```

Step 3: Confirm the above configurations have taken effect by command **show**

```
hostname(config)# show isp-network all
ISP telecom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
101.1.1.0/24
ISP netcom status: Active
Binding to nexthop: 0
Subnet(IP/Netmask): 1
201.1.1.0/24
hostname(config)# show llb inbound smart test
```

```
domain:domain name; IP: ip address; ISP: isp name; IF: interface;
PROXY: proximity address book status; E: enable; D:disable
TRACK: track object name; W: ip weight; S:ip status;A:active;
I: inactive
==========================================================-
===============

--------------------------------------------------------------------

name: test
domain count: 1
rule count: 2
status: enable
domains: www.test.com;
ip addresses:

--------------------------------------------------------------------

ID IP ISP IF PROX TRACK W S
1 100.1.1.2 telecom ethernet0/0 D 10 A
3 200.1.1.2 netcom ethernet0/1 D 10 A
==========================================================-
================
```

When PC1 requests www.test.com, the device will return the IP address for telecom link (100.1.1.2); when PC2 requests www.test.com, the device will return the IP address for netcom link (200.1.1.2).

Session Limit

Hillstone devices support the zone-based session limit function. You can limit the session number and control the new session ramp-up rate for the source IP address, destination address, specified IP address,protocol,application,role or userin the security zone, thereby to protect against DoS attacks and control the bandwidth of applications, such as IM or P2P.

Creating a Session Limit Rule

To create a session limit rule, in the security zone configuration mode, use the following command:

ad session-limit [**id** *id*] {{**src-ip** *address-entry* **dst-ip** *address-entry* | **ip** *address-entry* } [**protocol** *protocol-id*] [**application** *application-name*] [**blacklist block-type ip block-time** *value*] [**role** *role-name* | **user** *aaa-server-name user-name* | **user-group** *aaa-server-name user-group-name*]} {**session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} | **ramp-rate**[**per-sec**]**max** *number*} [**schedule** *schedule-name*][**log**]

- **id** *id* – Specifies the ID of the session limit rule.
- **src-ip** *address-entry* – Limits the session number of the source IP address in the security zone. *address-entry* is the IP range of `src-ip`. This parameter should be an address entry defined in the address book.
- **dst-ip** *address-entry* – Limits the session number of the destination IP address in the security zone. *address-entry* is the IP range of *dst-ip*. This parameter should be an address entry defined in the address book.
- **ip** *address-entry* – Limits the session number of the specified IP address in the security zone. *address-entry* is the IP range of **ip**. This parameter should be an address entry defined in the address book.
- **protocol** *protocol-id* – Limits the session numbers of the specified protocol in the security zone.

- **application** *application-name* – Limits the session numbers of the specified application in the security zone.
- **role** *role-name* – Limits the session number of the specified role in the security zone.
- **user** *aaa-server-name user-name* – Limits the session number of the specified user in the security zone. *aaa-server-name* is the AAA server the user belongs to.
- **user-group** *aaa-server-name user-group-name* – Limits the session number of the specified user group in the security zone.*aaa-server-name* is the AAA server the user group belongs to.
- **blacklist block-type ip block-time***value* – Adds a single IP address to the dynamic IP blacklist and specifies the blocked period when the IP limit mode is "per IP". *value* is the blocked period, which ranges from 60 to 1,296,000 seconds. The default value is 60 seconds. If the concurrent session number/new session number of a single IP exceeds the session limit threshold, you can add the IP address to the dynamic IP blacklist. This way, the system blocks the IP address until the blocked period expires.
- **session** {**unlimit** | **max** *number* [**per-srcip** | **per-dstip** | **per-ip**] | **per-user**} – Specifies the maximum session number for the IP address or role. **unlimit** indicates no session limit. **session max** *number* specifies the maximum session number for all the IP addresses defined in the address entry or all the users defined in the role; if **per-srcip, per-dstip, per-ip** or **per-user** is used, **session max** *number* specifies the maximum session number for each IP address or each user defined in the role. **per-srcip, per-dstip, per-ip** and **per-user** should be correspond to **src-ip, dst-ip, ip** and **role** respectively. For example, only when **src-ip** is specified can you choose **per-srcip**.
- **ramp-rate max** *number* – Specifies the maximum new sessions that can be established every 5 seconds for the IP address or role.
- **ramp-rate max per-sec** *number* – Specifies the maximum new sessions that can be established every second for the IP address or role.

- **schedule** *schedule-name* – Specifies an schedule during which the session limit rule will take effect.
- **log** - Record the session limit log.



Notes: Session limit function support IPv4 address and IPv6 address. If the IPv6 function for interface is enabled, you can configure the address of IPv6 type. The type of the source address entry and the destination address entry must keep same.

To delete the session limit rule, in the security zone configuration mode, use the following command:

no ad session-limit id *id*

- **id** *id* – The session limit rule ID of the security zone. To view the rule ID, use the command **`show session-limit`**.

With session limit configured, StoneOS will drop the sessions that exceeds the maximum session number. To view the statistics on the dropped sessions, use the command **`show session-limit`**. To clear the statistics on the dropped sessions in the specified session limit rule, in any mode, use the following command:

clear session-limit id *id* **statistics**

- **id** *id* – Specifies the rule ID. The statistics on the dropped session in the specified session limit rule will be cleared.



Notes: After Full-cone NAT is enabled on the device, the destination IP address in the session limit refers to the IP address before DNAT translation. For more information about Full-cone NAT, see "Full-cone NAT" in the "Firewall"

Viewing Session Limit

To view the configuration information of the session limit after configuring session limit, in any mode, use the following command:

show session-limit

Pre-discarding Packets of Receiving Queue

When data packets enter system, they may wait in the receiving queue for a long time if system resources are insufficient, which may delay networking and degrade user's experience. At this time, you can enable the Pre-discarding Packets of Receiving Queue function to drop part packets waiting in the receiving queue in advance, helping system release resources and applications re-transmit messages.

Configuring Pre-discarding Packets of Receiving Queue

To pre-discard packets of the receiving queue, under the global configuration mode, use the following command:

flow head-drop-packet low-water-mask *value* **interval** *time*

- **low-water-mask** *value* - Specify the low water level threshold for pre-discarding packets. When the packets processed by system is bigger than the specified value, system will pre-discard some packets to reduce networking delay; when the processed packets is smaller than the specified value, system will not discard the packets, preventing system from discarding packets by mistake when the traffic is very low. The range of *Value* is 0 to 500000, and the default value is 8192.
- **interval** *time* - The default is 100 ms. Specify the interval for calculating the number of packets processed by system. The unit of time is milliseconds, ranging from 100 to 1000 milliseconds. The default value is 100 ms.

To disable the pre-discarding packets of receive queue, under global configuration mode, use the following command **no head-drop-packet**.

Viewing the Information of Pre-discarding Packets of Receiving Queue

To view the information of pre-discarding packets of receiving queue, in any mode, use the command:

show flow head-drop-packet

Traffic Quota

System supports the traffic quota function, which can limit and control the allowable flow quota of users/user groups per day or per month. When the user traffic reaches the daily or monthly quota defined by the traffic quota profile, the system will block the user traffic.

Configuring Traffic Quota

To configure the traffic quota via CLI, take the following steps:

- Configure the traffic quota profile and specify the daily quota and monthly quota of user traffic in the traffic quota profile.
- Create a user/user group traffic quota rule, specify the restricted user/user group in the user-/user group traffic quota rule, and bind the specified traffic quota profile to the traffic quota rule.
- Enable the traffic quota function in the specified zone.

Creating a Traffic Quota Profile

To create a traffic quota profile, in the global configuration mode, use the following command:

user-quota profile*profile-name*

- *profile-name* - Specifies the traffic quota profile name and enters the traffic quota profile configuration mode. If the specified name exists, then the system will directly enter the traffic quota profile configuration mode.

To delete the specified traffic quota profile, in the global configuration mode, use the command **no user-quota profile***profile-name*.

Specifying the Daily Quota/ Monthly Quota

To specify the daily quota, in the traffic quota profile configuration mode, use the following command:

daily*daily-value***unit** {**KB** |**MB** | **GB** | **TB**}

- *daily-value* – Specifies the daily quota, the range is 1 to 65535.
- **unit** {**KB** |**MB** | **GB** | **TB**} – Specifies the unit of the daily quota.

To delete the specified daily quota, in the traffic quota profile configuration mode, use the command **no daily**.

To specify the monthly quota, in the traffic quota profile configuration mode, use the following command:

monthly*daily-value***unit** {**KB** |**MB** | **GB** | TB}

- *daily-value* – Specifies the monthly quota, the range is 1 to 65535.
- **unit** {**KB** |**MB** | **GB** | **TB**} – Specifies the unit of the monthly quota.

To delete the specified monthly quota, in the traffic quota profile configuration mode, use the command **no monthly** .

Creating a User Traffic Quota Rule

To create a user traffic quota rule, in the global configuration mode, use the following command:

user-quota user-rule*rule-name*

- *rule-name* - Specifies the user traffic quota rule name and enters the user traffic quota rule configuration mode. If the specified name exists, then the system will directly enter the user traffic quota rule configuration mode.

To delete the specified user traffic quota rule, in the global configuration mode, use the command **no user-quota user-rule***rule-name*.

Specifying the User of User Traffic Quota Rule

To specify the user of the user traffic quota rule, in the user traffic quota rule configuration mode, use the following command:

user*aaa-server-nameuser-name*

- *aaa-server-name* – Specifies the name of the AAA server already configured in the system.
- *user-name* - Specifies the name of user.

To delete the specified user, in the user traffic quota rule configuration mode, use the following command:

no user*aaa-server-name user-name*

Binding a Traffic Quota Profile to a User Traffic Quota Rule

To bind the specified traffic quota profile to a user traffic quota rule, in the user traffic quota rule configuration mode, use the following command:

profile*profile-name*

- *profile-name* - Specifies the name of the traffic quota profile that will be bound to the user traffic quota rule.

To cancel the binding, in the user traffic quota rule configuration mode, use the following command:

no profile

Creating a User Group Traffic Quota Rule

To create a user group traffic quota rule, in the global configuration mode, use the following command:

user-quota group-rule*group-name*

- *group-name* - Specifies the name of the user group traffic quota rule and enters the user group traffic quota rule configuration mode. If the specified name exists, then the system will directly enter the user group traffic quota rule configuration mode.

To delete the specified user group traffic quota rule, in the global configuration mode, use the command **no user-quota group-rule***group-name*.

Specifying the User Group of User Group Traffic Quota Rule

To specify the user group of the user group traffic quota rule, in the user group traffic quota rule configuration mode, use the following command:

user-group*aaa-server-name group-name*

- *aaa-server-name* – Specifies the name of the AAA server already configured in the system.
- *group-name* - Specifies the name of user group.

To delete the specified user group, in the user group traffic quota rule configuration mode, use the following command:

no user-group*aaa-server-name group-name*

Binding a Traffic Quota Profile to a User Group Traffic Quota Rule

To bind the specified traffic quota profile to a user group traffic quota rule, in the user traffic quota rule configuration mode, use the following command:

profile*profile-name*

- *profile-name* - Specifies the name of the traffic quota profile that will be bound to the user group traffic quota rule.

To cancel the binding, in the user group traffic quota rule configuration mode, use the following command:

no profile

Adjusting Traffic Quota Rule Priority

To adjust the user traffic quota rule priority, in the global configuration mode, use the following command:

user-quota user-rule*rule-name* [**move**] { **before name***rule-name* | **after name***rule-name* | **top** | **bottom** }

- *rule-name* – Specifies the name of the user traffic quota rule that you want to adjust.
- **before name***rule-name* – Adjust the priority of the user traffic quota rule before the specified rule.
- **after name***rule-name* – Adjust the priority of the user traffic quota rule after the specified rule.
- **top** – Adjust the priority of the user traffic quota rule to the top of all rules.
- **bottom** – Adjust the priority of the user traffic quota rule to the bottom of all rules.

To adjust the user group traffic quota rule priority, in the global configuration mode, use the following command:

user-quota group-rule*group-name* [**move**] { **before name***group-name* | **after name***group-name* | **top** | **bottom** }

- *group-name* – Specifies the name of user group traffic quota rule that you want to adjust.
- **before name***group-name* – Adjust the priority of user group traffic quota rule before the specified rule.
- **after name***group-name* – Adjust the priority of user group traffic quota rule after the specified rule.
- **top** – Adjust the priority of user group traffic quota rule to the top of all rules.
- **bottom** – Adjust the priority of user group traffic quota rule to the bottom of all rules.

Enabling/Disabling the Traffic Quota Function in the Zone

To enable or disable the traffic quota function in the specified zone, in the zone configuration mode, use the following command:

- Enable the traffic quota function: **user-quota enable**
- Disable the traffic quota function: **no user-quota enable**

Resetting the User Used Traffic

You can reset the user used traffic as needed, in the global configuration mode, use the following command:

user-quota reset [*user-name*]{**daily** | **monthly** | **all**}

- *user-name* - Specifies the name of user who needs to reset the used traffic.
- **daily** - Reset the daily used traffic.
- **monthly** - Reset the monthly used traffic.
- **all** - Reset the all used traffic.

Viewing the Traffic Quota Profile Information

To view the traffic quota profile information, in any mode, use the following command:

show user-quota profile

Viewing the User Traffic Quota Rule Information

To view the user traffic quota rule information, in any mode, use the following command:

show user-quota user-rule

Viewing the User Group Traffic Quota Rule Information

To view the user group traffic quota rule information, in any mode, use the following command:

show user-quota group-rule

Viewing the Zone with Traffic Quota Function Enabled

To view the zone with traffic quota function enabled, in any mode, use the following command:

show user-quota zone

Viewing the Traffic Quota Statistics

To view the traffic quota statistics, in any mode, use the following command:

show user-quota {**user** | **user-group**}[*aaa-server-name user-name*]

Chapter 12 Threat Prevention

The chapter introduces the following topics:

- "ARP Defense" on Page 425 explains how to configure the host defense function to protect the proxy host from ARP attacks.
- "Attack Defense" on Page 2075 describes the common network attack concepts, how to configure Attack Defense, and examples of Attack Defense.
- "Sandbox" on Page 2143 describes sandbox protection function and how to configure sandbox protection rules and how to update the domain name whitelist used by the sandbox.
- "IPS" on Page 2158 explains how to detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
- "Abnormal Behavior Detection" on Page 2264 describes how to configure the zone-based abnormal behavior detection function to determine the abnormal behavior of the detection object and how to update the abnormal behavior model database.
- "Advanced Threat Detection" on Page 2269 describes how to intelligently analyze host-based suspicious traffic to determine whether it is malware and how to update the malware behavior model database.
- "Perimeter Traffic Filtering" on Page 2273 describes how to filter the perimeter traffic based on known IP of black/white list, take block action on the malicious traffic that hits the blacklist, and how to update the IP reputation database.
- "Mitigation" on Page 2293 describes how to configure the mitigation rules to identify the potential risks and network attacks dynamically, and take action on the risk , and how to update the mitigation rule database.

- "Correlation Analysis" on Page 2297 describes how to use the correlation analysis engine and makes the correlation analysis of the threat events generated by each modules of threat prevention.
- "Critical Assets" on Page 2298 describes how to configure the critical assets.
- "Geolocation Information Database" on Page 2302 describes how to update the geolocation information database.
- "Botnet Prevention" on Page 2313describes how to configure the botnet prevention function based on security zones or policies.
- "Encrypted Traffic Detection" on Page 2335 describes how to configure the encrypted traffic detection function to detect encrypted attack traffic.
- "Antispam" on Page 2342 describes how to filter the mails transmitted by SMTP and POP3 protocol through the cloud server, and discover the mail threats.
- "End Point Protection" on Page 2348: Obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.
- : Identify the network video monitoring devices, like IPC (IP Camera) and NVR (Network Video Recorder) via the flowing traffic, then monitor the identified devices and block illegal behaviors according to the configurations.

Attack Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, as network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems. Devices provide attack defense functions based on security zones.

Common Network Attacks

This section describes some common network attacks. Devices can take appropriate actions against network attacks to assure the security of your network systems.

IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized accesses to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

ARP Spoofing

LAN transmission network traffic based on MAC addresses. ARP spoofing attack is by filling in the wrong MAC address and IP address , to make a wrong corresponding relationship of the target host's ARP cache table. Follow-up will lead to the wrong destination host IP packets , and packet network unreasonable target resources are stolen.

Land Attack

In a land attack, the attacker carefully crafts a packet and sets its source and destination address to the address of the server that will be attacked. In such a condition the victim server will send a message to its own address, and this address will also return a response and establish a Null

connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

Fraggle Attack

A fraggle attack is quite similar to a Smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

Teardrop Attack

Teardrop attack is a denial of service attack. Is based on the method of attack morbid fragmented UDP packets, which works by sending multiple fragmented IP packets to the attacker is (IP fragmented packets include the fragmented packets belong to which the packet and the packet the location and other information) , some operating systems contain overlapping offset when received fragmented packets will forge a system crash , reboot and so on.

WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is ICMP fragment. Generally an ICMP packet will not be fragmented; therefore many systems cannot properly process ICMP fragments. If your system receives any ICMP fragment, it's almost certain that the system is under attack.

SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amount of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for response. Due to the heavy load, the attacked target cannot complete its normal transmission task.

ICMP Redirect Attack

An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network, but possibly used maliciously for attacks that redirect traffic to a specific system. In this type of an attack, the hacker, posing as a router, sends an ICMP redirect message to a host, which indicates that all future traffic must be directed to a specific system as the more optimal route for the destination.

IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweep or port scan, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

IP Fragment Attack

An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.

IP Option Attack

An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.

Huge ICMP Packet Attack

An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.

TCP Flag Attack

An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.

DNS Query Flood Attack

The DNS server processes and replies all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

DNS Reply Flood Attack

When the DNS server receives the reply message, it will process the message regardless whether it is valid. DNS reply flood is that the attacker sends a large number of DNS reply message to the DNS cache server, causing the cache server to run out of resources by processing these reply messages.

TCP Split Handshake Attack

When a client establishes TCP connection with a malicious TCP server, the TCP server responses with a fake SYN package and uses this fake one to initialize the TCP connection with the client. After establishing the TCP connection, the malicious TCP server switches its role and becomes the client side of the TCP connection. Thus, the malicious traffic might enter into the intranet.

SIP Flood

SIP (Session Initiation Protocol) is an application-layer signaling control protocol. It is used to initiate, modify and terminate interactive multimedia sessions, such as multimedia meetings and Internet telephone. The attacker of the SIP flood attack sends a large number of INVITE messages to the target SIP server in a short time. Therefore, the target SIP server exhausts its resources and fails to respond to the call requests from valid users.

Configuring Attack Defense

By default only part of the attack defense functions in the untrust zone of the device are enabled, including IP address spoofing attack defense, IP address sweep attack defense, IP protocol scan attack defense, TCP port scan attack defense, UDP port scan attack defense, ICMP Flood attack defense, SYN Flood attack defense, UDP flood attack defense, WinNuke attack defense, Ping of

Death attack defense, Teardrop attack defense, IP Option attack defense, IP Fragment attack defense, IP Directed Broadcast attack defense, Land attack defense and SIP Flood attack defense. To enable all the attack defense functions, in the security zone configuration mode, use the following command:

ad all

To disable all the attack defense functions in the security zone, in the security zone configuration mode, use the command **no ad all**.

You can configure the parameters of the above attack defense functions as needed. The attack defense configurations of Hillstone devices include:

- Configuring IP address sweep attack defense
- Configuring ICMP redirect attack defense
- Configuring IP protocol scan attack defense
- Configuring TCP port scan attack defense
- Configuring UDP port scan attack defense
- Configuring IP address spoofing attack defense
- Configuring SYN Flood attack defense
- Configuring SYN-Proxy
- Configuring SIP Flood attack defense
- Configuring ICMP Flood attack defense
- Configuring UDP Flood attack defense
- Configuring Flood protection threshold learning
- Configuring Large ICMP packet attack defense
- Configuring WinNuke attack defense

- Configuring Ping of Death attack defense
- Configuring Teardrop attack defense
- Configuring IP Option attack defense
- Configuring TCP option anomaly attack defense
- Configuring Land attack defense
- Configuring IP fragment attack defense
- Configuring Smurf and fraggle attack defense
- Configuring ARP spoofing attack defense
- Configuring DNS Query Flood attack defense
- Configuring DNS Reply Flood attack defense
- Configuring IP verification
- Configuring AD Whitelist
- Viewing the attack defense configurations of the security zone and statistics

Configuring IP Address Sweep Attack Defense

You can individually enable or disable IP address sweep attack defense for each security zone and configure the time threshold and action for IP address sweep attacks. To configure the IP sweep scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-sweep [**threshold***value* | **action** {**alarm** | **drop** | **block** [**block-time***number*]} | **tcp**]

- **ad ip-sweep** – Enables IP address sweep attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-sweep**.

- **threshold** *value* – Specifies the time threshold for IP address sweep. If over 10 ICMP/TCP packets from one single source IP address are sent to different hosts within the period specified by the threshold, system will identify them as an IP address sweep attack. The value range is 1 to 1,800,000 milliseconds. The default value is 1. To restore to the default value, use the command **no ad ip-sweep threshold**.
- **action** {**alarm** | **drop** | **block** [**block-time***number*]} – Specifies the action for IP address sweep attacks. To restore to the default action, use the command **no ad ip-sweep action**.
  - **alarm** – The system will permit 10 IMCP/TCP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (**threshold***value*). For the excessive packets, the system will send an alarm but still allow them to pass through.
  - **drop** – The system will only permit 10 IMCP/TCP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (**threshold***value*), and also give an alarm. All the excessive packets of the same type will be dropped during this period. This is the default action.
  - **block** [**block-time***number*]- The system will add the source IP addresses detected within the specified period (**threshold***value*) to the blacklist and block the data packets that are sent from the source IP addresses. **block-time***number*- Specifies the block time, which ranges from 1 minute to 15 days. If no blocking time is configured, data packets are permanently blocked.
- **tcp**- Specifies the device to detect TCP packets. If over 10 TCP packets from one single source IP address are sent to different hosts within the period specified by the threshold (**threshold***value*), system will identify them as an IP address sweep attack. Disable the detection function for TCP packets, use the command **no ad ip-sweep tcp**.



Notes:

In Tap zone, you cannot configure the Attack Defense (AD) function.

Configuring ICMP Redirect Attack Defense

You can individually enable or disable ICMP redirect attack defense for each security zone and configure the action for ICMP redirect attacks. To configure the ICMP redirect attack defense for a security zone, in security zone configuration mode, use the following command:

ad icmp-redirect [**action** {**alarm** | **drop**}]

- **ad icmp-redirect** – Enables ICMP redirect attack defense for the security zone. To disable the function, in security zone configuration mode, use the command **no ad icmp-redirect**. By default, the function is disabled.
- **action** {**alarm** | **drop**} – Specifies the action for ICMP redirect attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad icmp-redirect action**.

Configuring IP Protocol Scan Attack Defense

You can individually enable or disable IP protocol scan attack defense for each security zone and configure the time threshold and action for IP protocol scan attacks. To configure the IP protocol scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-proto-scan [**threshold***value* | **action** {**alarm** | **drop** | **block** [**block-time***number*]}]

- **ad ip-proto-scan** – Enable the IP protocol scan attack defense. To disable this function, use the command **no ad ip-proto-scan**.

- **threshold***value* – Specifies the time threshold for IP Protocol scan. If over 10 packets of the same IP protocol from the same source IP address are sent to the same host within the specified time threshold, StoneOS will identify them as an IP protocol scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 10. To restore to the default threshold, use the command **no ad ip-proto-scan threshold**.
- **action** {**alarm** | **drop** | **block** [**block-time***number*]} – Specifies an action for IP protocol scan attacks. To restore to the default action, use the command **no ad ip-sweep action**.
  - **alarm** – The system will permit 10 packets of the same IP protocol originating from one single source IP address while matched to the same host to pass through during the specified period (**threshold***value*). For the excessive packets, the system will send an alarm but still allow them to pass through.
  - **drop** – The system will only permit 10 packets of the same IP protocol originating from one single source IP address while matched to the same host to pass through during the specified period (**threshold***value*) and drop other IP protocol packets, and also give an alarm. This is the default action.
  - **block** [**block-time***number*]- The system will add the source IP addresses detected within the specified period (**threshold***value*) to the blacklist and block the data packets that are sent from the source IP addresses. **block-time***number*- Specifies the block time, which ranges from 1 minute to 15 days. If no blocking time is configured, data packets are permanently blocked.



Notes:

In Tap zone, you cannot configure the Attack Defense (AD) function.

Configuring TCP Port Scan Attack Defense

You can individually enable or disable TCP port scan attack defense for each security zone and configure the time threshold and action for the TCP port scan attacks. To configure the TCP port scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad port-scan [**threshold***value* | **action** {**alarm** | **drop** | **block** [**block-time***number*]}]

- **ad port-scan** – Enables TCP port scan attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command**no ad port-scan**.
- **threshold** *value* – Specifies the time threshold for TCP port scan. If over 10 TCP SYN packets from the same source IP address are sent to different ports within the period specified by the threshold, system will identify them as a port scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 1. To restore to the default value, in the security zone configuration mode, use the command **no ad port-scan threshold**.
- **action** {**alarm** | **drop** | **block** [**block-time***number*]} – Specifies the action for TCP port scan attacks. To restore to the default action, use the command **no ad port-scan action**.
    - **alarm** – The system will permit 10 TCP SYN packets destined to different ports to pass through during the specified period (**threshold***value*). For the excessive packets, the system will send an alarm but still allow them to pass through.
    - **drop** – During the specified period (**threshold***value*), the system will only permit 10 TCP SYN packets destined to different ports to pass through and drops the other packets of the same type, and also generates an alarm.
    - **block** [**block-time***number*]- The system will add the source IP addresses detected within the specified period (**threshold***value*) to the blacklist and block the TCP SYN packets that are sent from the source IP addresses to different ports. **block-**

time*number*- Specifies the block time, which ranges from 1 minute to 15 days. If no blocking time is configured, data packets are permanently blocked.



Notes:

In Tap zone, you cannot configure the Attack Defense (AD) function.

Configuring UDP Port Scan Attack Defense

You can individually enable or disable UDP port scan attack defense for each security zone and configure the time threshold and action for UDP port scan attacks. To configure the UDP port scan attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad udp-port-scan [**threshold***value* | **action** {**alarm** | **drop** | **block** [**block-time***number*]}]

- **ad udp-port-scan** – Enable the UDP port scan attack defense. To disable this function, use the command **no ad udp-port-scan**.
- **threshold***value* – Specifies an action for UDP port scan attacks. If over 10 UDP packets from the same source IP address are sent to different ports within the specified time threshold, StoneOS will identify them as a UDP port scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 5. To restore to the default threshold, use the command **no ad udp-port-scan threshold**.
- **action** {**alarm** | **drop**} – Specifies the action for UDP port scan attacks. To restore to the default action, use the command **no ad udp-port-scan action**.
    - **alarm** – The system will permit 10 UDP packets destined to different ports to pass through during the specified period (**threshold***value*). For the excessive packets, the system will send an alarm but still allow them to pass through.

- **drop** – During the specified period (**threshold***value*), the system will only permit 10 UDP packets destined to different ports to pass through and drops the other packets of the same type, and also generates an alarm.
- **block** [**block-time***number*]- The system will add the source IP addresses detected within the specified period (**threshold***value*) to the blacklist and block the UDP packets that are sent from the source IP addresses to different ports. **block-time***number*- Specifies the block time, which ranges from 1 minute to 15 days. If no blocking time is configured, data packets are permanently blocked.



Notes:

In Tap zone, you cannot configure the Attack Defense (AD) function.

Configuring IP Address Spoofing Attack Defense

System can defend against Layer 3 IP address spoofing attacks. After enabling the Layer 3 IP address spoofing attack defense function, when a packet is passing through the device, system will trace out the source IP address, and take different actions based on the traceout results, including:

- If the security zone of the packet destined to the device (with this IP as its source address) is the same as the security zone of the packet originating from the device (with this IP as the destination address), then system will permit the packet to pass through. You can identify security zone of the packet originating from the device based on the traceout results.
- Vice versa, system will identify the packet as an abnormal packet, and give an alarm and drop the packet.

To enable Layer 3 IP address spoofing attack defense for a security zone, in the Layer 3 security zone configuration mode, use the following command:

ad ip-spoofing

To disable Layer 3 IP address spoofing attack defense for a security zone, in the Layer 3 security zone configuration mode, use the command **no ad ip-spoofing**.

Configuring SYN Flood Attack Defense

You can enable or disable SYN flood attack defense for each security zone individually, and configure the packet number threshold and actions for the SYN flood attacks. To configure SYN flood attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad syn-flood [**source-threshold** *number* | **destination-threshold** [**ip-based** | **port-based**] *number* | **destination** [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*] | **action** {**alarm** | **drop**}]

- **ad syn-flood** – Enables SYN flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad syn-flood**.
- **source-threshold** *number* – Specifies a threshold for outbound SYN packets (ignoring the destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the source threshold is void. To restore to the default value, use the command **no ad syn-flood source-threshold**.
- **destination-threshold** [**ip-based** | **port-based**] *number* – Specifies a threshold for inbound SYN packets destined to one single destination IP address (**ip-based**) or one single destination port of the IP address (**port-based**). If not specified, the system will use ip-based by default. If the number of inbound SYN packets destined to one single destination IP address or one single destination port per second exceeds the threshold, system will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the destination threshold is void. To restore to the default value, use the command **no ad syn-flood destination-threshold** [**ip-base** | **port-base**].

- **destination** [**ip-based** | **port-based** [**address-book** *address-entry* | *A.B.C.D/M*] – Enables **ip-based** or **port-based** SYN flood attack defense. If not specified, the system will use ip-based by default. To enable port-based SYN Flood attack defense for a specific segment, use the parameter **address-book** *address-entry* | *A.B.C.D/M*. The SYN Flood attack defense for other segments will be based on the IP addresses. The value range of the destination IP mask is 24 to 32. To cancel the configuration, use the command **no ad syn-flood destination**.
- **action** {**alarm** | **drop**} – Specifies the action for SYN Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**source-threshold** *number* | **destination-threshold** *number*) of SYN packets to pass through, and also give an alarm; if source threshold and destination threshold are also configured, system will first detect if the traffic is a destination SYN flood attack: if so, system will drop the packets and give an alarm, if not, system will continue to detect if the traffic is a source SYN attack; if so, system will drop the packets and give an alarm. The default action is drop. To restore to the default action, use the command**no ad syn-flood action**.

Configuring SYN-Proxy

SYN-Proxy is designed to defend against SYN flood attacks in combination with ad syn-flood. When both ad syn-flood and SYN proxy are enabled, SYN proxy will act on the packets that have already passed the detections of ad syn-flood.

The Hillstone devices support SYN-Cookie, a stateless SYN-Proxy mechanism.

To configure the SYN-Proxy and the SYN-Cookie functions for the specified security zone, in the security zone configuration mode, use the following command:

ad syn-proxy [**min-proxy-rate** *number* | **max-proxy-rate** *number* | **proxy-timeout** number | cookie]

- **ad syn-proxy** – Enables SYN-Proxy for a security zone to defend against SYN Flood attacks. To disable the function, in the security zone configuration mode, use the command **no ad**

syn-proxy.

- **min-proxy-rate** *number* – Specifies the minimum number for SYN packets that will trigger SYN proxy or SYN-Cookie (if enabled by cookie). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will trigger SYN proxy or SYN-Cookie. The value range is 0 to 50000. The default value is 1000. To restore to the default value, use the command**no ad syn-proxy min-proxy-rate**.
- **max-proxy-rate** *number* – Specifies the maximum number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if enabled by cookie). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, system will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. To restore to the default value, use the command**no ad syn-proxy max-proxy-rate**.
- **proxy-timeout** *number* – Specifies the timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30. To restore to the default value, use the command **no ad syn-proxy proxy-timeout**.
- **cookie** – Enables SYN-Cookie (the prerequisite is SYN-Proxy is enabled). This function allows system to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand the range between **min-proxy-rate** and **max-proxy-rate** appropriately. To disable SYN-Cookie, use the command**no ad syn-proxy cookie**.

Configuring SIP Flood Attack Defense

You can enable or disable SIP flood attack defense for each security zone individually, and configure the packet number threshold and actions for the SIP flood attacks. To configure SIP Flood

attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad sip-flood [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad sip-flood** - Enables SIP Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad sip-flood**.
- **threshold** *number* - Specifies the threshold of the number of the SIP INVITE messages with the same destination IP to be received by the device. That is to say, the device determines that it is attacked by the SIP flood attack when it receives more SIP INVITE messages with the same destination IP than the configured threshold. In this scenario, the device takes further measures to deal with this attack. The value range is 0 to 800000000. The default value is 2000. To restore to the default value, use the command **no ad sip-flood destination-threshold**.
- **action** {**alarm** | **drop**} - Specifies the action of the system when it is attacked by the SIP flood attack. When the system detects the attack, it inspects whether there is a real SIP client behind the subsequent source IP address. If yes, the system bypasses the subsequent SIP INVITE messages sent by this source IP. Otherwise, the system will perform the configured action for the SIP INVITE messages sent by this source IP in three seconds. There are two system actions: **drop** - Means dropping the INVITE messages. It is the default action. **alarm** - Means that the system sends an alarm but still bypasses the INVITE messages. To restore to the default action, use the command **no ad sip-flood action**.

Configuring ICMP Flood Attack Defense

You can enable or disable ICMP flood attack defense for each security zone individually, and configure the packet number threshold and actions for the ICMP flood attacks. To configure ICMP Flood attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad icmp-flood [**threshold** *number* | **action** {**alarm** | **drop**}]

- **ad icmp-flood** – Enables ICMP Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad icmp-flood**.
- **threshold** *number* – Specifies a threshold for inbound ICMP packets. If the number of inbound ICMP packets destined to one single IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. To restore to the default value, use the command **no ad icmp-flood threshold**.
- **action** {**alarm** | **drop**} – Specifies the action for ICMP Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**threshold** *number*) of IMCP packets to pass through during the current and the next second, and also gives an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad icmp-flood action**.

Configuring UDP Flood Attack Defense

You can enable or disable UDP flood attack defense for each security zone individually, and configure the packet number threshold and actions for the UDP Flood attacks. To configure UDP Flood attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad udp-flood [**session-state-check**] [**source-threshold** *number* | **destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad udp-flood** – nables UDP Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad udp-flood**.
- **session-state-check** – Enables the function of session state check. After the function is enabled, system will not check whether there is UDP Flood attack in the backward traffic of

UDP packet of the identified sessions. To disable this function, use the command **no ad udp-flood session-state-check**.

- **source-threshold** *number* − Specifies a threshold for outbound UDP packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad udp-flood source-threshold**.
- **destination-threshold** *number* − Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad udp-flood destination-threshold**.
- **action** {**alarm** | **drop**} − Specifies an action for UDP flood attacks.**alarm** − Gives an alarm but still allows the packets to pass through; **drop** − Only permits the specified number (**source-threshold** *number* | **destination-threshold** *number*) of UDP packets to pass through during the current and the next second, and also gives an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad udp-flood action**.

Configuring Flood Protection Threshold Learning

For flood attacks, the system supports the Flood Protection Threshold Learning function. Flood protection threshold learning collects statistics on the maximum rate of traffic that passes through a normal network environment. Then, this function provides a proper reference value for the attack detection threshold. To configure this function, you need to configure flood protection threshold learning parameters and enable flood protection threshold learning.

To configure flood protection threshold learning parameters, use the following command in security zone mode:

ad threshold-learning {**duration** {**day** | **hour** | **minute**} *number* | **learn-mode** {**one-time** | **periodic** {**day** | **hour** | **minute**} *number*} **apply-mode** {**manual** | **auto**} **coefficient** {**default** | **loose** | **strict** | **userdefine***number*}}

- **duration** {**day** | **hour** | **minute**} *number* – Specifies the duration of flood protection threshold learning. The unit can be day, hour, or minute. To restore to the default learning duration, use the **no ad threshold-learning duration** command.
  - **day** – Sets the time unit to day. Valid values: 1 to 365 days. Default value: 1 day.
  - **hour** – Sets the time unit to hour. Valid values: 1 to 8760 hours. Default value: 1 hour.
  - **minute** – Sets the time unit to minute. Valid values: 10 to 525600 minutes. Default value: 1440 minutes.
- **learn-mode** {**one-time** | **periodic** {**day** | **hour** | **minute**} *number* – Specifies the type of flood protection threshold learning. The type can be one-time or periodic. By default, one-time is used. To restore to the default learning type, use the **no ad threshold-learning learn-mode** command.
  - **one-time** – Runs the learning task only once, which will be automatically stopped after completion.
  - **periodic** {**day** | **hour** | **minute**} *number* – Runs the learning task periodically based on the interval. You need to manually stop the learning task. If you set the learning type to periodic, you also need to specify the periodic interval, which indicates the interval between the last time when the learning task ends and the next time when the learning task starts. The unit can be day, hour, or minute.
    - **day** – If the time unit is set to days, valid values of the interval are 1 to 365 days and the default value is 7 days.
    - **hour** – If the time unit is set to hours, valid values of the interval are 1 to 8760 hours and the default value is 1 hour.

        - **minute** – If the time unit is set to minute, valid values of the interval are 10 to 525600 minutes and the default value is 1440 minutes.

- **apply-mode** {**manual** | **auto**} – Specifies the mode of applying the flood protection threshold learning result. The mode can be manual or auto. By default, manual is used. To restore to the default mode, use the **no ad threshold-learning apply-mode** command.
    - **manual** – Applies the threshold learning result to the threshold configuration of a flood attack defense item based on your requirements.
    - **auto** – The threshold configuration of all enabled flood attack defense items will be automatically configured with the threshold learning result and these threshold configurations will be automatically applied.
- **coefficient** {**predefine** {**default** | **loose** | **strict**} | **userdefine***number*} – Final threshold learning result=Maximum traffic rate within learning duration * Coefficient. Specifies the coefficient of flood protection threshold learning. Unit: %. To restore to the default coefficient, use the **no ad threshold-learning coefficient** command.
    - **default** – Sets the coefficient to 200.
    - **loose** – Sets the coefficient to 4000.
    - **strict** – Sets the coefficient to 100.
    - **userdefine***number* – Customizes the coefficient, which ranges from 100 to 4000.

To start/stop flood protection threshold learning and apply the flood protection threshold learning result, use the following command in global mode:

exec ad-threshold-learning {**apply** {**syn-flood** | **dns-query-flood** | **dns-query-recursion-flood** | **dns-reply-flood** | **udp-flood** | **icmp-flood** | **sip-flood**} | **start** | **stop**} **zone***zone-name*

- {**apply** {**SYN flood** | **DNS Query flood** | **DNS Recursisve Query flood** | **DNS Reply flood** | **UDP flood** | **ICMP flood** | **SIP flood**} – Applies the flood protection threshold learning result to a specified flood attack defense item, including SYN flood attack item, DNS Query flood attack item, DNS Recursive Query flood attack item, DNS Reply flood attack item, UDP flood attack item, ICMP flood attack item, and SIP flood attack item.
- **start** – Starts flood protection threshold learning.
- **stop** – Stops flood protection threshold learning.
- **zone***zone-name* – Specifies the name of zone that has Flood Attack Defense enabled.

Configuring Large ICMP Packet Attack Defense

You can enable or disable large ICMP packet attack defense for each security zone individually, and configure the packet size threshold and actions for large ICMP packet attacks. To configure large ICMP packet attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad huge-icmp-pak [**threshold** *number* | **action** {**alarm** | **drop**}]

- **ad huge-icmp-pak** – Enables large ICMP packet attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad huge-icmp-pak**.
- **threshold** *number* – Specifies the size threshold for ICMP packets. If the size of any inbound ICMP packet is larger than the threshold, system will identify it as a large ICMP packet and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024. To restore to the default value, use the command **no ad huge-icmp-pak threshold**.
- **action** {**alarm** | **drop**} – Specifies the action for large ICMP packet attacks. **alarm** – Gives an alarm but still allows the packet to pass through; **drop** – Gives an alarm and drop the packet. The default action is drop. To restore to the default action, use the command **no ad udp-flood action**.

Configuring WinNuke Attack Defense

With WinNuke attack defense enabled, system will drop the packets and give an alarm if any WinNuke attack has been detected. To enable WinNuke attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad winnuke

To disable the function, in the security zone configuration mode, use the command **no ad win-nuke**.

Configuring Ping of Death Attack Defense

With Ping of Death attack defense enabled, system will drop the packets and give an alarm if any Ping of Death attack has been detected. To enable Ping of Death attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ping-of-death

To disable the function, in the security zone configuration mode, use the command **no ad ping-of-death**.

Configuring Teardrop Attack Defense

With Teardrop attack defense enabled, system will drop the packets and give an alarm if any Teardrop attack has been detected. To enable Teardrop attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad tear-drop

To disable the function, in the security zone configuration mode, use the command **no ad tear-drop**.

Configuring IP Option Attack Defense

With IP Option attack defense enabled, system will drop the packets and give an alarm if any IP option attack has been detected. You can change the action for the attacks as needed. system will defend against the following types of IP options: Security, Loose Source Route, Record Route,

Stream ID, Strict Source Route and Timestamp. To enable IP Option attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-option [action {alarm | drop}]

- **ad ip-option** – Enables IP Option attack defense for the specified security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-option**.
- **action {alarm | drop}** – Specifies the action for IP Option attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad ip-option action**.

Configuring TCP Option Anomaly Attack Defense

With TCP option anomaly attack defense enabled, system will drop the packets and give an alarm if any TCP option anomaly attack has been detected. You can change the action for the attacks as needed. system identifies the following conditions as TCP option anomaly attack:

- SYN packets are fragmented
- TCP packets are only set with FIN flag
- TCP packets are not set with any flag
- TCP packets are set with both FIN and RST flag
- TCP packets are set with both SYN and URG flag
- TCP packets are set with both SYN and RST flag
- TCP packets are set with both SYN and FIN flag

To enable TCP option anomaly attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad tcp-anomaly [action {alarm | drop}]

- **ad tcp-anomaly** – Enables TCP option anomaly attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad tcp-anomaly**.
- **action {alarm | drop}** – Specifies the action for TCP option anomaly attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad tcp-anomaly action**.

Configuring Land Attack Defense

With Land attack defense enabled, system will drop the packets and give an alarm if any Land attack has been detected. You can change the action for the attacks as needed. To enable Land attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad land-attack [action {alarm | drop}]

- **ad land-attack** – Enables Land attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad land-attack**.
- **action {alarm | drop}** – Specifies the action for the Land attacks.**alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad land-attack action**.

Configuring IP Fragment Attack Defense

When being transmitted among different networks, sometimes the packets need to be fragmented according to the MTU value. Attackers can modify the IP fragments and launch attacks by exploiting the vulnerabilities occurring during reassembling. The modified IP fragments destined to the victims might lead to improper reassembling, or even complete system crash.

system will drop the packets and give an alarm if any IP fragment attack has been detected. You can change the action for the attacks as needed. To enable IP fragment attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-fragment [**action** {**alarm** | **drop**}]

- **ad ip-fragment** – Enables IP fragment attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-fragment**.
- **action** {**alarm** | **drop**} – Specifies the action for IP fragment attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops the packets. The default action is drop. To restore to the default action, use the command **no ad ip-fragment action**.

Configuring Smurf and Fraggle Attack Defense

With Smurf and Fraggle attack defense enabled, system will drop the packets and give an alarm if any Smurf or Fraggle attack has been detected. You can change the action for the attacks as needed. To enable Smurf and Fraggle attack defense for the specified security zone, in the security zone configuration mode, use the following command:

ad ip-directed-broadcast [**action** {**alarm** | **drop**}]

- **ad ip-directed-broadcast** – Enables Smurf and Fraggle attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad ip-directed-broadcast**.
- **action** {**alarm** | **drop**} – Specifies the action for the Smurf and Fraggle attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Gives an alarm and drops all the packets. The default action is drop. To restore to the default action, use the command **no ad ip-directed-broadcast action**.

Configuring ARP Spoofing Attack Defense

ARP spoofing attack defense can protect the Intranet against ARP spoofing attacks. To configure ARP spoofing attack defense of the specified security zone, in the security zone configuration mode, use the following command:

ad arp-spoofing {**reverse-query** | **ip-number-per-mac** *number* [**action** [**drop** | **alarm**]] | **gratuitous-arp-send-rate** *number*}

- **reverse-query** – Enables reverse query. When system receives an ARP request, it will log the IP address and reply with another ARP request; and then system will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP request packet. To disable the function, in the security zone configuration mode, use the command **no ad arp-spoofing reverse-query**.
- **ip-number-per-mac** *number* – Specifies the threshold for the number of IP addresses corresponding to each MAC address in ARP table. The value range is 1 to 1024. The default value is 100. If the number of IP addresses corresponding to a MAC address exceeds the threshold within 30 seconds, system will take the action specified by **action** [**drop** | **alarm**]. The available actions include**drop**(give an alarm and drop the ARP packets) and**alarm**(give an alarm but still allow the packets to pass through). To restore to the default value, use the command **no ad arp-spoofing ip-number-per-mac**.
- **gratuitous-arp-send-rate** *number* – Specifies the number of Gratuitous ARP packets sent per second. The value range is 1 to 10. The default value is 10. To restore to the default value, use the command **no ad arp-spoofing gratuitous-arp-send-rate**.

Configuring DNS Query Flood Attack Defense

DNS (Domain Name System) is used to convert a domain name to an IP address, and resolve an IP address to a domain name. DNS is an application layer protocol, so it can be based on TCP or UDP. DNS Query Flood attacks are based on UDP.

The DNS Query Flood attacks are launched by sending a large number of domain name resolution requests to the target DNS server. Typically the requested domain name is randomly generated, or does not exist at all. When the DNS server being attacked receives the resolution requests, it will first look for the corresponding cache. If the cache is not found and the domain name can not be resolved directly by the server, the DNS server will send a recursive query request to its upper DNS server. The domain name resolution process will bring a heavy load to the DNS server. If the DNS requests per second exceed a certain number, the workload will lead to domain name resolution timeout on the DNS server. .

Hillstone devices support DNS Query Flood attacks defense. You can enable or disable DNS Query Flood attack defense for each security zone individually, and configure the packet number threshold and the actions for DNS Query Flood attacks. To enable DNS Query Flood defense, in the security zone configuration mode, use the following command:

ad dns-query-flood [**recursion**] [**source-threshold** *number*] [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad dns-query-flood** – Enables DNS Query Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad dns-query-flood**.
- **recursion** – Only limits recursive DNS query packets. If this parameter is not specified, system will limit all the DNS query packets.
- **source-threshold** *number* – Specifies a threshold for outbound DNS query packets or recursive DNS query packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, system will identify the traffic as a DNS query flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-query-flood source-threshold**.
- **destination-threshold** *number* – Specifies a threshold for inbound DNS query packets or recursive DNS query packets. If the number of inbound DNS query packets destined to one single IP address per second exceeds the threshold, system will identify the traffic as a DNS

query flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-query-flood destination-threshold**.

- **action** {**alarm** | **drop**} – Specifies the action for DNS Query Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**threshold** *number*) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad dns-flood action**.



Notes: DNS Query Flood attack defense is only applicable to UDP DNS query packets.

Configuring DNS Reply Flood Attack Defense

Hillstone devices support DNS Reply Flood attacks defense. You can enable or disable DNS Reply Flood attack defense for each security zone individually, and configure the packet number threshold and the actions for DNS Reply Flood attacks. To enable DNS Reply Flood defense, in the security zone configuration mode, use the following command:

ad dns-reply-flood [**source-threshold** *number*] [**destination-threshold** *number* | **action** {**alarm** | **drop**}]

- **ad dns-reply-flood** – Enables DNS Reply Flood attack defense for the security zone. To disable the function, in the security zone configuration mode, use the command **no ad dns-reply-flood**.
- **source-threshold** *number* – Specifies a threshold for outbound DNS replypackets or recursive DNS replypackets. If the number of outbound DNS reply packets originating from one single IP address per second exceeds the threshold, system will identify the traffic as a DNS

Reply Flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-reply-flood source-threshold**.

- **destination-threshold***number* – Specifies a threshold for inbound DNS reply packets or recursive DNS reply packets. If the number of inbound DNS reply packets destined to one single IP address per second exceeds the threshold, system will identify the traffic as a DNS Reply Flood and take the specified action. The value range is 0 to 300000. The default value is 1500. To restore to the default value, use the command **no ad dns-reply-flood destination-threshold**.

- **action** {**alarm** | **drop**} – Specifies the action for DNS Reply Flood attacks. **alarm** – Gives an alarm but still allows the packets to pass through; **drop** – Only permits the specified number (**threshold***number*) of recursive DNS reply packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. The default action is drop. To restore to the default action, use the command **no ad dns-flood action**.



Notes: DNS Reply Flood attack defense is only applicable to UDP DNS reply packets.

Configuring IP Verification

After the IP verification function is enabled, for the DNS Reply Flood and DNS Query Flood attack defense functions, when the number of DNS packets exceeds the threshold, the system can dynamically verifies the source IP address and then allows traffic from verified IP addresses over a period of time. For the SYN-Proxy and SYN-Cookie functions, if the number of SYN packets exceeds the threshold, successfully proxy-verified IP addresses are not proxied again over a period of time. Instead, traffic from the IP addresses is directly allowed. To enable the IP verification function, in global configuration mode, use the following command:

ad-ip-certified enable

Use the **no ad-ip-certified enable** command to disable the IP verification function.

After you configure the aging period for the IP verification list, the verified and unverified IP addresses that have exceeded the aging period are deleted. To configure the aging period, in global configuration mode, use the following command:

ad-ip-certified timeout*timeout-value*

- *timeout-value* - Specifies the aging period for the IP verification list. Valid values: 60 to 86400 seconds. Default value: 3600 seconds.

Use the **no ad-ip-certified timeout** command to restore to the default value.

To display the IP verification list, in any mode, use the following command:

show ad ip-certified [**ad-type** { **dns-query-flood** | **dns-query-flood-recursion** | **dns-reply-flood** | **sip-flood** | **syn-cookie** | **syn-proxy**} | **ip-address** {*A.B.C.D* | *X:X:X:X::X*} | **state** {**certified** | **uncertified** | **wait-certified**}]

- **ad-type** { **dns-query-flood** | **dns-query-flood-recursion** | **dns-reply-flood** | **sip-flood** | **syn-cookie** | **syn-proxy**} - Displays the IP verification list of the specified attack defense type.
- **ip-address** {*A.B.C.D* | *X:X:X:X::X*} - Displays the IP verification list of the specified IP address. Both IPv4 and IPv6 addresses are supported.
- **state** {**certified** |**uncertified** | **wait-certified**}- Displays the IP verification list of the specified verification status.

To display the configuration of IP verification, including the status and aging period, in any mode, use the following command:

show ad ip-certified configuration

Configuring TCP Split Handshake Attack Defense

After enabling the TCP split handshake attack defense and this attack is detected, the device will drop the packet and give an alarm by default. You can change the defaul action. To configure the TCP split handshake attack defense, use the following command in the security zone configuration mode:

ad tcp-split-handshake [**action** {**alarm** | **drop**}]

- **ad tcp-split-handshake** – Enable the TCP split handshake attack defense for the security zone. To disable it, use the command **no ad tcp-split-handshake**.
- **action** {**alarm** | **drop**} – Specifies the action for the TCP split handshake attacks. **alarm**- Gives an alarm but still allows the packets to pass through; **drop**- Gives an alarm and drops all the packets. The default action is**drop**. To restore to the default action, use the command **no ad land-attack action**.

Configuring an Attack Defense Whitelist

With attack defense enabled, the system will check all the traffic in the zone. In practical scenario, possibly you do not want to check the traffic originating from certain hosts for test purpose. To solve this problem, you can add the addresses (source address or destination address) to an attack defense whitelist, so that the addresses can be exempted from the attack defense check.

To configure an attack defense whitelist, in the zone configuration mode, use the following command:

ad whitelist [**id** *id*] {**source-ip** | **destination-ip**} {*IPv4-address/M* | *IPv6-address/prefix* | *address-entry*}

- **id** – Specifies an ID for the whitelist rule. The value differs according to different models. If not specified, the system will assign an ID automatically for the rule.
- **source-ip** | **destination-ip**- Specifies the address type in the whitelist: source address(**source-ip**) or destination address (**destination-ip**).
- IPv4-address/M – Specifies the IPv4 address and network that will be added to the whitelist rule.
- *IPv6-address/prefix* - Specifies the IPv6 address and prefix length(value: 120-128) that will be added to the whitelist rule.
- *address-entry* – Specifies the address entry that will be added to the whitelist rule.

To delete the specified whitelist rule, in the zone configuration mode, use the following command:

no ad whitelist [**id** *id*] {**source-ip** | **destination-ip**} {*IPv4-address/M* | *IPv6-address/prefix* | *address-entry*}

Viewing the Attack Defense Configuration and Statistics of the Security Zone

To view the attack defense configuration and statistics of the specified security zone, in any mode, use the following command:

show ad zone*zone-name* {**statistics** | **configuration** | **whitelist** | **threshold-clearning** {**configuration** | **status** | **result**}}

- *zone-name* – Specifies the name of the security zone.
- **statistics** – Shows the attack defense statistics of the specified security zone.
- **configuration** – Shows the attack defense configurations of the specified security zone.
- **whitelist** – Shows the attack defense whitelist configurations of the specified security zone.
- **threshold-clearning** {**configuration** | **status** | **result**} – Shows the flood protection threshold learning configuration, learning status, and learning result of the specified security zone.

Examples of Configuring Attack Defense

This section describes several attack defense configuration examples for your better understanding and helps you configure the attack defense function of the devices.

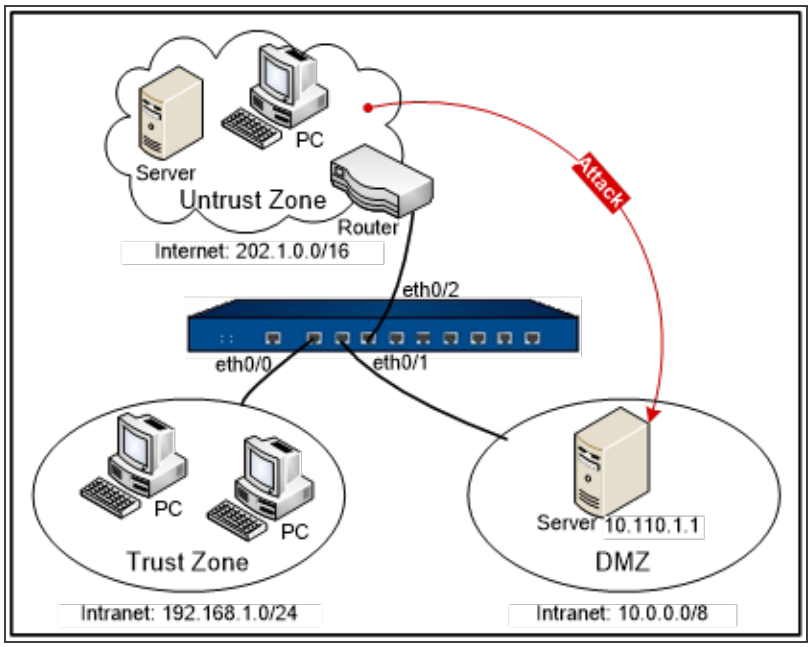
Example of Configuring Land Attack Defense

This section describes a Land attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone

against Land attacks. The network topology is shown below.



Configuration Steps

Step 1: Configure ethernet0/0.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure ethernet0/2.

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule.

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable Land attack defense for the untrust zone.

```
hostname(config)# zone untrust
hostname(config-zone)# ad land-attack
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the Land attack defense configured for the server. Craft a packet with identical source and destination IP address, and send it to 10.110.1.1. The Hillstone device will detect a Land attack, and then give an alarm and drop the packet.

Example of Configuring SYN Flood Attack Defense

This section describes a SYN Flood attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone against SYN Flood attacks.

Configuration Steps

Step 1: Configure ethernet0/0:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure ethernet0/2:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable SYN Flood attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad syn-flood
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the SYN Flood attack defense configured for the server. Send over 1500 packets per second to 10.110.1.1. The Hillstone device will detect a SYN Flood attack, and then give an alarm and drop the packets.

Example of Configuring IP Address Sweep Attack Defense

This section describes an IP address sweep attack defense configuration example.

Requirement

Device's ethernet 0/0 is bound to the trust zone, ethernet 0/2 is bound to the untrust zone, and ethernet 0/1 is bound to the DMZ zone. The goal is to protect the server in the DMZ zone against IP address sweep attacks.

Configuration Steps

Step 1: Configure ethernet0/0:

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configure ethernet0/2:

```
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ip address 202.1.0.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

Step 3: Configure ethernet0/1:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone dmz
hostname(config-if-eth0/1)# ip address 10.0.0.1/8
hostname(config-if-eth0/1)# exit
hostname(config)#
```

Step 4: Configure a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone dmz
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
```

```
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Enable IP address sweep attack defense for the untrust zone:

```
hostname(config)# zone untrust
hostname(config-zone)# ad ip-sweep
hostname(config-if)# exit
hostname(config)#
```

Step 6: Test the IP address sweep attack defense configured for the server. Craft packets via smartbits and launch an IP address sweep attack against ethernet0/2. Send over 10 packets per millisecond to 202.1.0.1. The device will detect an IP address sweep attack, and then give an alarm and drop the packets.

Anti-Virus

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

System is designed with Anti-Virus that is controlled by licenses to provide AV solution featuring high speed, high performance and low delay. With this function configured in system, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, etc., and proceed with the configured actions.

Anti Virus function can detect the common file types and protocol types which are most likely to carry the virus and protect. Hillstone device can detect protocol types of FTP, HTTP, SMTP, IMAP4, POP3, SMB and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE、HTML、MAIL、RIFF、ELF、PDF、MS OFFICE、Raw Data and Others. **Others** means scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc. If SMB protocol type is used, the system supports the detection and controlling of files in break-point resumption scenarios

The virus signature database includes over 10 million signatures, and supports both daily auto update and real-time local update.

If IPv6 is enabled, Anti Virus funtion will detect files and protocols based on IPv6. How to enable IPv6, see IPv6.

Configuring Anti-Virus

To enable the anti-virus function on system, take the following steps:

1. Define an AV profile, and specify the file types, protocol types, the actions for the viruses, and the e-mail label function in the profile.
2. Bind the AV profile to an appropriate policy rule or security zone. To perform the Anti-Virus function on the HTTPS traffic, see Binding an AV Profile to a Policy Rule.

The system also supports binding the anti-virus profile to a ZTNA policy to perform virus detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.



Notes: You need to update the anti-virus signature database before enabling the function for the first time. For more information about how to update, see Updating AV Signature Database. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating.

After installing the anti-virus license and rebooting the device, the anti-virus function will be enabled on the system. To view the status of anti-virus, use the command show version. To enable or disable Anti-Virus, in any mode, use the following command:

exec av {enable | disable}

- **enable** – Enables Anti-Virus.
- **disable** – Disables Anti-Virus.

After executing the above commands, you need to reboot the system to make the modification take effect. After rebooting, system's max concurrent sessions might decrease if the function is enabled, or restore to normal if the function is disabled. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 835.

Configuring Log Aggregation and Aggregation Time

The system can merge anti-virus logs of the same merging type based on the specified time granularity. This way, logs are reduced to prevent the log server from receiving redundant logs. To configure log aggregation and aggregation time granularity, in the global configuration mode, use the following command:

av agg-log enable [**by-src** | **by-dst** | **by-src-dst**] [**aggregation-time** *value*]

- **av agg-log enable** - Merges anti-virus logs of default log aggregation type (**by-src-dst**) and default time granularity (10 seconds).
- **by-src** - Merges anti-virus logs of the same source IP and MD5.
- **by-dst** - Merges anti-virus logs of the same destination IP and MD5.
- **by-src-dst** - Merges anti-virus logs of the same source, the same destination IP and MD5.

- *value* - Specifies the time granularity of log aggregation. With this parameter specified, at the same time granularity, the system stores anti-virus logs of the same merging type in the database only once. Value ranges from 10 to 600 seconds. The default value is 10 seconds.

In the global configuration mode, use the command **no av agg-log enable** to specify the log aggregation type as **Do Not Merge**. This way, the system stores each anti-virus log in the database and does not merge any logs.

Enabling/Disabling Intelligence File Engine Detection Function

The primary target for detection by the intelligence file engine is PE, PDF, OFFICE, and ELF files. This function can be used to perform malware detection on cached files and delay the transmission of detection messages to ensure successful blocking of virus-infected files. This enhances virus detection and filtering capabilities. By default, this function is disabled. To upgrade the intelligence file engine signature database, see Updating AV Intelligence File Engine Database.

To enable/disable the intelligence file engine function, in global configuration mode, use the following command:

av-file-engine {**enable** | **disable**}

- **enable** – Enable the intelligence file engine function of the system.
- **disable** – Disable the intelligence file engine function of the system. By default, the function is disabled.



Notes:

- This function can be configured only after the Anti-Virus function is enabled.
- When the action of a protocol in the antivirus profile is set to Fill Magic, files transferred by using this protocol are not detected by the intelligence file engine.



- When the antivirus profile is configured with the Capture Packets action, no packets are captured even if the intelligence file engine detects threats.
- The following device supports the function:
  - A-series: Devices other than SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200.
  - K-series: SG-6000-K2680, SG-6000-K2380, SG-6000-K6280-GS, SG-6000-K6580, and SG-6000-K9180.
  - X-series: SG-6000-X25803 and SG-6000-X25812.
  - CloudEdge: CloudEdge that is deployed on X86-based server.

To configure the size of cache file, in global configuration mode, use the following command:

av-file-engine cache-file-size*number*

- *number* – Specifies the size of the of the intelligence file engine cache. Valid values: 128 to 10240 KB. Default value: 1024 KB.

To configure the time to delay sending messages, in global configuration mode, use the following command:

av-file-engine pak-hold-time*time-number*

- *time-number* - Specifies the time to delay sending messages. Valid values: 0 to 1000 milliseconds. Default value: 500 milliseconds.

Enhancing Intelligence File Engine Detection Performance

You can configure the performance enhancement function for the intelligence file engine as required. After the function is enabled, the system adopts the multi-core and multi-process

technology for intelligence file engine detection, improving the detection performance.

Specifying the Number of CPU Cores Utilized at the System Data Layer

To enhance the performance of intelligence file engine detection, you need to first specify the number of CPU cores utilized at the system data layer. Once specified, the number of intelligence file engine detection processes will be the total system CPU cores minus the number of CPU cores utilized at the system data layer. To specify the number of CPU cores utilized at the system data layer, in global configuration mode, use the following command:

flow-core-num*number*

- *number* - Specifies the number of CPU cores utilized at the system data later. Valid values: max_core_number/2 to max_core_number-ber, where max_core_number is the total number of CPU cores in the system. Once specified, the formula for calculating the number of intelligence file engine detection processes is as follows: Number of intelligence file engine detection processes = max_core_number (total system CPU cores) - flow-core-number (number of CPU cores utilized at the system data layer).

In global mode, use the **no flow-core-num** command to cancel the configuration of the number of CPU cores utilized at the system data layer.

Enabling/Disabling the Multi-process Function of Intelligence File Engine

By default, the intelligence file engine multi-process function is disabled. To enable this function, in global configuration mode, use the following command:

cp-multi-cores av-file-engine

In global mode, use the **no cp-multi-cores av-file-engine** command to disable the function.



Notes:

- After specifying or unspecifying the number of CPU cores utilized at the system data layer, you need to restart the device to make the configuration take

effect.

- After enabling/disabling the multi-process function of intelligence file engine, you need to restart the device to make the configuration take effect.
- You need to specify the number of CPU cores utilized at the system data layer, enable the intelligence file engine multi-process function, and then restart the device. Only after the device is restarted can the multi-process function of intelligence file engine be fully enabled.
- SG-6000-K6580, SG-6000-K9180, SG-6000-X25803, SG-6000-X25812, and devices with ⩽2 CPU cores do not support this function.

Showing the Intelligence File Engine Detection Information

You can use the show command to view the status, configuration information, and detection number of the intelligence file engine detection function.

To show the information about intelligence file engine detection, in any mode, use the following command:

show av-file-engine status

Example:

```
hostname# show av-file-engine status
AV file engine status : enabled (Shows that the intelligence file engine function is enabled.)
Cache file max size (KB): 1024 (Shows that the cache file size is 1,024 KB.)
Pak hold time (ms) : 500 (Shows that the delay time to send messages is 500 milliseconds.)
Running on core 0 : Yes (Shows that the intelligence file engine function is running only on CPU0.)
Detected: 2 (Shows that 2 viruses are detected by the intelligence file engine.)
```

Creating an AV Profile

The AV profile specifies the file types, protocol types and the actions for viruses. To create an AV Profile, in the global configuration mode, use the following command:

av-profile *av-profile-name*

- *av-profile-name* - Specifies the AV profile name and enters the AV profile configuration mode. If the specified name exists, then the system will directly enter the AV profile configuration mode. To delete the specified AV profile, in the global configuration mode, use the command**no av-profile** *av-profile-name*.

To control the scan accurately, in the AV profile configuration mode, specify the protocol types, actions and file types. Among the above options, the protocol types must be specified, while the file types can be configured as needed. If only the protocol types are configured, but the file types are not configured, the system will only scan the text files transferred over specified protocol; if the scan object is the specified file type transferred over the specified protocol type (for example, a HTML document transferred over the HTTP protocol), you need to specify the HTTP protocol type and HTML file type in the AV profile.

Enabling Malicious Website Detection

System provides the malicious website detection function to protect against attacks from malicious websites if you click maliciously URLs accidentally. With this function enabled, System will detect Trojans, phishing and other malicious behaviors when you are trying to visit URLs, and process malicious URLs according to the actions specified by system.

The Malicious Website Detection is enabled by default. To enable the function, in the global configuration mode, use the following command:

anti-malicious-sites

To disable the function, in the global configuration mode, use the following command:

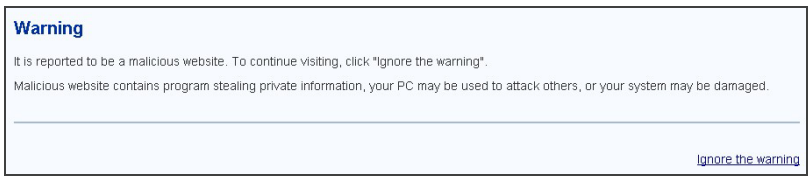
no anti-malicious-sites

Specifying Malicious Website Detection Action

To specify the action for Malicious Website Detection, in the AV profile configuration mode, use the following command:

anti-malicious-sites [action { log-only | reset-conn | warning} | pcap]

- **action {log-only | reset-conn | warning}** – Specifies the action for the Malicious Website Detection
  - **log-only** – Only generates log.
  - **reset-conn** – If virus has been detected, system will reset connections to the files.
  - **warning** – Pops up a warning page to prompt that a virus has been detected. This option is only effective to the messages transferred over HTTP.



    To view the reason for the block, click Why blocks this website, and you will be redirected to the Google Safe Browsing page. To ignore the page and continue to visit the website, click Ignore. In the following hour, you will not be prompted anymore if you visit the website again.

- **pcap** – Enable the Capture Packet function.

To cancel the the action for Malicious Website Detection, in the AV profile configuration mode, use the following command:

no anti-malicious-sites [action { log-only | reset-conn | warning} | pcap]



Notes:

The following platforms support the PCAP function.



- A-series firewalls installed with hard disks (Except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200)
- K-series firewalls installed with hard disks
- X-series firewalls installed with hard disks (Except SG-6000-X10800 and SG-6000-X9180)
- CloudEdge

Specifying a Protocol Type

To specify a protocol type, in the AV profile configuration mode, use the following command:

protocol-type {{**ftp** | **imap4** | **pop3** | **smtp**} [**pcap** | **action** {**fill-magic** | **log-only** | **reset-conn**}] | **http** [**pcap** |**action** {**fill-magic** | **log-only** | **reset-conn** | **warning**}]|**smb** [**pcap** | **action** {**log-only** | **reset-conn**}] }

- **ftp** – Scans the files transferred over FTP.
- **http** – Scans the files transferred over HTTP.
- **imap4** – Scans the files transferred over IMAP4.
- **pop3** – Scans the Emails transferred over POP3.
- **smtp** – Scans the Emails transferred over SMTP.
- **pcap** – Capture the packet for protocol scanning.
- **smb** – Scans the files transferred over SMB.
- **action** {**fill-magic** | **log-only** | **reset-conn** | **warning**} – Specifies the action for the viruses.

- **fill-magic** – Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section.
- **log-only** – Generates logs. This is the default action for FTP, IMAP4, POP3 ,SMTP and SMB.
- **reset-conn** – Resets the connection if any virus has been detected.
- **warning** – Pops up a warning page to prompt that a virus or malicious website download has been detected. There are two kinds of pages: the virus warning page , and malicious website warning page (the malicious website detection is enabled), as shown below. This option is only effective to the messages transferred over HTTP, and is also the default action if any virus or malicious website download has been detected.



To ignore the page and continue to visit the website, click Ignore. In the following one hour, you will not be prompted anymore if you visit the website again.



To ignore the page and continue to visit the website, click Ignore. In the following hour, you will not be prompted anymore if you visit the website again.

Repeat the above command to specify more protocol types.

To cancel the specified protocol type, in the AV profile configuration mode, use the following command:

no protocol-type {ftp | imap4 | pop3 | smtp | http| smb}

SMTP, POP3 and IMAP4 are all mail transfer protocols that are used to send Email files. To scan Emails, you must configure to scan SMTP, POP3 or IMAP4 protocol, and also configure the file types that will be scanned; besides, as the body of the message and attachments are embedded in the mail file, you also need to configure the file types for the attachment.

Specifying a File Type

To specify a file type, in the AV Profile configuration mode, use the following command:

file-type {**bzip2** | **gzip** | **html** | **jpeg** | **mail** | **pe** | **rar** | **riff** | **tar** | **zip** | **elf** | **pdf** | **office** | **raw-data** | **others** }

- **bzip2** – Scans BZIP2 compressed files.
- **gzip** – Scans GZIP compressed files.
- **html** – Scans HTML files.
- **jpeg** – Scans JPEG files.
- **mail** – Scans mail files.
- **pe** – Scans PE files. PE (Portable Executable) is an executable file format supported by Win32 environment. This file format can be used across Win32 platforms. Even if Windows is running on a non-Intel CPU, the PE loader of any Win32 platform can identify and use the file format. Besides, system also supports packed PE files. The supported packing types include ASPack 2.12, UPack 0.399, UPX (all versions), and FSG v1.3, 1.31, 1.33, 2.0.
- **rar** – Scans RAR compressed files.
- **riff** – Scans RIFF files. RIFF (Resource Interchange File Format) is a class of multimedia file formats designed by Microsoft for Windows, mainly consisting of WAV and AVI types.
- **tar** – Scans TAR compressed files.
- **zip** – Scans ZIP compressed files.
- **elf** – Scans the ELF files.

- **pdf** – Scans the PDF files.
- **office** – Scans the Office files.
- **raw-data** – Scans the txt file and unrecognized file.
- **others** – Scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc.

Repeat the above command to specify more protocol types.

To cancel the specified protocol type, in the AV profile configuration mode, use the following command:

no file-type { bzip2 | gzip | html | jpeg | mail | pe | rar | riff | tar | zip | elf | pdf | office | raw-data | others }

Label Email

If an Email transferred over SMTP is scanned, you can enable label Email to scan the Email and its attachment(s). The scanning results will be included in the mail body, and sent with the Email. If no virus has been detected, the message of "No virus found" will be labeled, as shown below:

Body
No virus found. Checked by Hillstone AntiVirus

Otherwise information related to the virus will be displayed in the Email, including the filename, path, result and action, as shown below:

Body
Here are the AntiVirus scanning results: Body: Found virus: virusname1, action: log; Attachment1.zip/virustest1.exe: Found virus: virusname2,

Body
action: log; Attachment2.tar/subfolder/file1.doc: Found virus: virusname3, action: log; Checked by Hillstone AntiVirus



Notes: The Email will display the scan information of up to 3 virus file (including the message body and attachments). You can view all the scan information in the log.

Enabling/Disabling Label Email

By default the label Email function is disabled. To enable the function, in the AV Profile configuration mode, use the following command:

label-mail

To disable the function, in the AV Profile configuration mode, use the following command:

no label-mail

Configuring Email Signature

After enabling the label Email function, you can customize your own Email signature. By default, the signature of the labeled Email is "Checked by Hillstone AntiVirus". To configure an Email signature, in the AV profile configuration mode, use the following command:

mail-sig *signature-string*

- *signature-string* – Configures the signature of the labeled Email.

To restore to the default value, in the AV profile configuration mode, use the following command:

no mail-sig

Configuring Anti-Virus Whitelist

If false positives occur when anti-virus detection is performed on a file MD5 value or URL to an anti-virus whitelist. You can also edit and detect the anti-virus whitelist.

To create or edit an anti-virus whitelist, take the following steps in global configuration mode:

av-whitelist id *id-num* **name** *whilelist-name* {**url** *url-str*|**md5** *md5-str*}

- id-num - Specifies the ID of the anti-virus whitelist.
- whilelist-name - Specifies the name of the anti-virus whitelist.
- *url-str* - Specifies the URL of the anti-virus whitelist.
- *md5-str* - Specifies the file MD5 value of the anti-virus whitelist.

To delete an anti-virus whitelist, take the following steps in global configuration mode:

no av-whitelist id*id-num*

- id-num - Specifies the ID of the anti-virus whitelist.

Binding an AV Profile to a Security Zone

If the AV profile is bound to a security zone, the system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified. If the policy rule is bound with an AV Profile, and the destination zone of the policy rule is also bound with an AV profile, then the AV profile bound to the policy rule will be valid, while the AV profile bound to the security zone will be void.

To bind the AV profile to a security zone, in the security zone configuration mode, use the following command:

av enable *av-profile-name*

- *av-profile-name* – Specifies the name of the AV profile that will be bound to the security zone. One security zone can only be bound with one AV profile.

To cancel the binding, in the security zone configuration mode, use the following command:

no av enable

To view the binding between the security zones and AV Profiles, use the command **show av zone-binding**.

Binding an AV Profile to a Policy Rule

If the AV profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the AV profile to a policy rule, in the policy rule configuration mode, use the following command:

av {*av-profile-name* | **no-av**}

- *av-profile-name* – Specifies the name of the AV profile that will be bound to the policy rule.
- **no-av** – Specifies the predefined AV profile named no-av, which means the anti-virus is disabled. If this profile is bound to any policy rule, even if there are other matched AV profiles, the system still will not detect the traffic.

To cancel the binding, in the policy rule configuration mode, use the following command:**no av**

To perform the Anti-Virus function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. The system will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the Anti-Virus function on the decrypted traffic. According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled Anti-Virus disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the Anti-Virus function on the decrypted traffic.
SSL proxy enabled Anti-Virus	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic.

Policy Rule Configurations	Actions
enabled	
SSL proxy disabled Anti-Virus enabled	The system performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with Anti-Virus as well, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled Anti-Virus disabled	Anti-Virus enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the zone.
SSL proxy enabled Anti-Virus enabled	Anti-Virus enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the policy rule.
SSL proxy disabled Anti-Virus enabled	Anti-Virus enabled	The system performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus rule of the policy rule. The HTTPS traffic will not be decrypted and the system will transfer it.



Tip: For more information about SSL proxy, see the SSL Proxy chapter.

Viewing AV Profile Information

To view the AV profile information, in any mode, use the following command:

show av-profile

Configuring Decompression Control Function

After configuring the decompression control function, StoneOS can decompress the transmitted compressed files, and can handle the files that exceed the max decompression layer as well as the encrypted compressed files in accordance with the specified actions. This function supports to decompress the files in type of RAR, ZIP, TAR, GZIP, and BZIP2. For configuration commands of the decompression global parameters, refer to Configuring Decompression Control Function.

Updating AV Signature Database

By default system updates the AV signature database everyday automatically. You can change the update configuration as needed. The configurations of updating AV signature database include:

- Configuring an AV Signature Update Mode
- Configuring an Update Protocol
- Configure an Update Server
- Specifying an HTTP Proxy Server
- Specifying an Update Schedule
- Updating Now
- Importing an AV Signature File
- Viewing AV Signature Information
- Viewing AV Signature Update Information

Configuring an AV Signature Update Mode

System supports both manual and automatic update modes. To configure an AV signature update mode, in the global configuration mode, use the following command:

av signature update mode {**auto** | **manual**}

- **auto** – Specifies the automatic AV signature update mode. This is the default mode.
- **manual** – Specifies the manual AV signature update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no av signature update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

av signature update protocol HTTP

In the global configuration mode, use the command **no av signature update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hill-stonenet.com. You can also configure another up to three update servers to download the latest AV signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

av signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is

update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs.

To cancel the specified update the server, in the global configuration mode, use the following command:

no av signature update {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the Antivirus signature database updating, use the following command in the global configuration mode:

av signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no av signature update proxy-server** {**main** | **backup**}.

Specifying an Update Schedule

By default, system automatically updates the AV signature database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

av signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the AV signature database immediately as needed. To update the AV signature database now, in any mode, use the following command:

exec av signature update

- **exec av signature update** – Only updates the incremental part between the current AV signature database and the latest AV signature database released by the update server.

Importing an AV Signature File

In some cases, your device may be unable to connect to the update server to update the AV signature database. To solve this problem, system provides the AV signature file import function, i.e., importing the AV signature files to the device from an FTP, TFTP server or USB disk, so that the device can update the AV signature database locally. To import the AV signature file, in the execution mode, use the following command:

import av signature from {{**ftp | ftps |sftp**} **server***ip-address* [**vrouter***vrouter-name*] [**user***user-name***password***password*] | **tftp server***ip-address* [**vrouter***vrouter-name*]} *file-name*

- **ftp | ftps |sftp** - Specifies the type of the server.
- *ip-address* – Specifies the IP address of the FTP, FTPS, SFTP, or TFTP server.

- **vrouter***vrouter-name* – Specifies the VRouter of the FTP, FTPS, SFTP, or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP/FTPS/SFTP server.
- *file-name* – Specifies the name of the AV signature file that be imported.

Viewing AV Signature Information

You can view the AV signature database information of the device as needed, including the AV signature database version, release dates, and the number of the AV signatures. To view AV signature database information, in any mode, use the following command:

show av signature info [**slot***slot-number*]

- **slot***slot-number* - Specifies the slot number,this parameter only support for Hillstone SX series devices.

Viewing AV Signature Update Information

You can view the AV signature update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the AV signature database update. To view the AV signature update information, in any mode, use the following command:

show av signature update

Updating AV Intelligence File Engine Database

By default, the system will automatically update the AV intelligence file engine database every day. You can change the update configuration of the AV intelligence file engine database as needed. Only X86-based devices support the function.

The configurations of updating AV intelligence file engine database include:

- Configuring an AV Intelligence File Engine Database Update Mode
- Configuring an Update Protocol
- Configure an Update Server
- Specifying an HTTP Proxy Server
- Specifying an Update Schedule
- Updating Now
- Importing the AV Intelligence File Engine Database
- Viewing AV Intelligence File Engine Database Version Information
- Viewing AV Intelligence File Engine Database Update Information

Configuring an AV Intelligence File Engine Database Update Mode

System supports both manual and automatic update modes. To configure an AV intelligence file engine database update mode, in the global configuration mode, use the following command:

av-file-engine update mode {**auto** | **manual**}

- **auto** – Specifies the automatic AV intelligence file engine database update mode. This is the default mode.
- **manual** – Specifies the manual AV intelligence file engine database update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no av-file-engine update mode

Configuring an Update Protocol

The system supports to update the AV intelligence file engine database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in

the global configuration mode, use the following command:

av-file-engine update protocol HTTP

In the global configuration mode, use the following command to restore the default value:

no av-file-engine update protocol HTTP

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest AV intelligence file engine database as needed. To configure the update the server, in the global configuration mode, use the following command:

av-file-engine update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of server1 is update1.hillstonenet.com, and the default value of server2 is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an ip-addressor a domain-name, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs.

To cancel the specified update the server, in the global configuration mode, use the following command:

no av-file-engine update {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, the AV intelligence file engine database can update automatically and normally.

To specify the HTTP proxy server for the AV intelligence file engine database, use the following command in the global configuration mode:

av-file-engine update proxy-server {**main** | **backup**} *ip-addressport-number*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no av-file-engine update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the AV intelligence file engine database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

av-file-engine update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly***date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** – Updates the database every week. **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** is used to specify the specific date in a week.
- **monthly***date* - Updates the database every month. Parameter date is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the AV intelligence file engine database immediately as needed. To update the AV intelligence file engine database now, in any mode, use the following command:

exec av-file-engine update

- **exec av-file-engine update** – Only updates the incremental part between the current AV intelligence file engine database and the latest AV intelligence file engine database released by the update server.

Importing the AV Intelligence File Engine Database

In some cases, your device may be unable to connect to the update server to update the AV intelligence file engine database. To solve this problem, system provides the AV intelligence file engine database import function, i.e., importing the AV intelligence file engine database file to the device from an FTP, FTPS, SFTP, TFTP or USB disk, so that the device can update the AV intelligence file engine database locally. To import the AV intelligence file engine database file, in the execution mode, use the following command:

import av-file-engine signature from {{**ftp | ftps |sftp**} **server***ip-address* [**vrouter***vrouter-name*] [**user***user-name***password***password*] | **tftp server***ip-address* [**vrouter***vrouter-name*]} *file-name*

- **ftp | ftps |sftp** - Specifies the type of the server.
- *ip-address* – Specifies the IP address of the FTP, FTPS, SFTP, or TFTP server.
- **vrouter***vrouter-name* – Specifies the VRouter of the FTP, FTPS, SFTP, or TFTP server.
- **user***user-name***password***password* – Specifies the username and password of the FTP/FTPS/SFTP server.

- *file-name* – Specifies the name of the AV intelligence file engine database file that be imported.

Viewing AV Intelligence File Engine Database Version Information

You can view the AV intelligence file engine database information of the device as needed, including the AV intelligence file engine database version and release dates. To view AV intelligence file engine database information, in any mode, use the following command:

show av-file-engine info

Example:

```
hostname# show av-file-engine info
vendor: Hillstone Networks (Shows the company where the AV intelligence file engine database belongs.)
Current version: 3.0.230512 (Shows the current version of the AV intelligence file engine database.)
Release date: 2023/05/12 16:37:09 (Shows the release date of the AV intelligence file engine database.)
```

Viewing AV Intelligence File Engine Database Update Information

You can view the AV intelligence file engine database update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the AV intelligence file engine database update. To view the AV intelligence file engine database update information, in any mode, use the following command:

show av-file-engine update

Example:

```
hostname# show av-file-engine update
av-file-engine signature update options:
protocol: HTTPS (Shows that the transmission protocol of the AV intelligence file engine data-
```

base is HTTPS.)

server1:

server2: update2.hillstonenet.com, 443, trust-vr (Shows the update server information of the AV intelligence file engine database.)

server3:

proxy server status: disable (Shows that no proxy server is specified)

main proxy server:

backup proxy server:

mode: auto (Shows that the update mode of the AV intelligence file engine database is auto.)

schedule: daily 03:51 (Shows the automatic update frequency and time.)

current status: normal (Shows that the update status of the AV intelligence file engine database is normal.)

last update result: Download signature failed; please confirm the servers are reachable (Shows the last update result of the AV intelligence file engine database.)

last update time: Tue Sep 26 03:51:57 2023 (Shows the last update time of the AV intelligence file engine database.)

Examples of Configuring Anti-Virus

Before enabling anti-virus, make sure your device has already been installed with a corresponding anti-virus license.

This section describes an anti-virus configuration example. Devices with this example configured can:

- Scan Emails and its attachments, and display the anti-virus result in the Emails. The Emails are transferred over SMTP and POP3, and the attachments may contain .exe and .jpeg files.
- Scan compressed files. RAR-compressed files contain .jpeg files, and all the compressed files are transferred over FTP.

Configuration Steps

Step 1: Configure the AV profile, and specify the protocol types and file types:

```
hostname(config)# av-profile email-scan
hostname(config-av-profile)# protocol-type smtp action fill-magic
hostname(config-av-profile)# protocol-type pop3 action fill-magic
hostname(config-av-profile)# protocol-type ftp action fill-magic
hostname(config-av-profile)# file-type pe
hostname(config-av-profile)# file-type jpeg
hostname(config-av-profile)# file-type mail
hostname(config-av-profile)# label-mail
hostname(config-av-profile)# mail-sig “Checked by Mail AntiVirus”
hostname(config-av-profile)# exit
hostname(config)#
```

Step 2: Create a policy rule, and reference the AV Profile to the rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# av email-scan
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 3: View the anti-virus status by command show version. If the function is disabled, use following command to enable it and reboot the system to make it take effect:

```
hostname(config)# exec av enable
```

Sandbox

A sandbox executes a suspicious file in a virtual environment, collects the actions of this file, analyzes the collected data, and verifies the legality of the file.

The Sandbox function of the system uses the cloud sandbox and the local sandbox technology. The suspicious file will be uploaded to the cloud sandbox or the local sandbox. The cloud sandbox or the local sandbox will collect the actions of this file, analyze the collected data, verify the legality of the file, give the analysis result to the system and deal with the malicious file with the actions set by system.

The Sandbox function contains the following parts:

- Collect and upload the suspicious file: The Sandbox function parses the traffic, and extracts the suspicious file from the traffic.
    - If there are no analyze result about this file in the local database, system will upload this file to the local sandbox or to the Hillstone cloud service platform, and the local sandbox will analyze the file or the cloud service platform will upload the suspicious file to the cloud sandbox for analysis. For how to connect to the Hillstone cloud service platform, refer to Connecting to Hillsotne Cloud Service Platform.
    - If this file has been identified as an illegal file in the local database of the Sandbox function, system will generate corresponding threat logs and cloud sandbox logs.

  Additionally, you can specify the criteria of the suspicious files by configuring a sandbox profile.
- Check the analysis result and take actions: The Sandbox function checks the analysis results of the suspicious file returned from the cloud sandbox or the local sandbox, verifies the legality of the file, saves the result to the local database. If this suspicious file is identified as an illegal file, you need to deal with the file according to the actions (reset the connection or report logs) set by system. If it's the first time to find malicious file by the cloud sandbox or the local sandbox, system will record threat logs and cloud sandbox logs and cannot stop

the malicious link. When malicious file accesses the cached threat information in the local device, the threat will be effective only by resetting connection.

- Maintain the local database of the Sandbox function: Record the information of the uploaded files, including uploaded time and analysis result. This part is completed by the Sandbox function automatically.



Notes: The cloud sandbox function is controlled by license. To use the cloud sandbox function, install the cloud sandbox license.

Preparation for Configuring Sandbox

Before enabling the Sandbox function, make the following preparations:

1. Make sure your system version supports the Sandbox function.
2. The current device is registered to the Hillstone cloud service platform. For how to connect to the Hillstone cloud service platform, refer to Connecting to Hillsotne Cloud Service Platform.
3. Import the cloud sandbox license and reboot. The cloud sandbox function will be enabled after rebooting.



Notes: After the Sandbox function is enabled, system's max concurrent sessions might decrease. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 835.

Configuring Sandbox

The System supports the zone-based and policy-based Sandbox:

- If a security zone is configured with the Sandbox function, system will perform sandbox detection on the traffic that is sourced from or destined to the binding zone specified in the rule.
- If a policy rule is configured with the Sandbox filtering function, system will perform sandbox detection on the traffic that is destined to the policy rule you specified.
- The sandbox configurations in a policy rule are superior to that in a zone rule if they are specified at the same time, and the sandbox configurations in a destination zone are superior to that in a source zone if they are specified at the same time.

The system also supports binding the sandbox profile to a ZTNA policy to perform sandbox detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To realize the policy-based or the zone-based Sandbox, take the following steps:

1. Enable the cloud sandbox or the local sandbox.
2. Define a sandbox profile, and configure white list settings and file filter settings.
3. Bind the sandbox profile to an appropriate zone or policy rule.

A sandbox profile contains the files types that device scanned, the protocols types that device scanned, and the white list settings.

- **File Type**: Support to detect PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP, ELFand Script file.
- **Protocol Type**: Support to detect HTTP, FTP, POP3, SMTP, IMAP4 and SMB protocol.
- **White list**: A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox or the local sandbox.

There are five built-in sandbox rules with the files and protocols type configured, white list enabled and file filter configured. The three default sandbox rules includes predef_low, predef_middle, predef_high, predef_peand and no_sandbox.

- **predef_low** -- A loose sandbox detection rule, whose file type is PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.
- **predef_middle** -- A middle-level sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.
- **predef_high** -- A strict sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF/SWF/RAR/ZIP/ELF/Script and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.
- **predef_pe**: A sandbox detection rule, whose file type is only PE and protocol types areHTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.
- **no_sandbox**: With this detection rule, the system does not perform any sandbox detection.

Enabling/Disabling the Cloud Sandbox or the Local Sandbox

To enable or disable the cloud sandbox or the local sandbox, in the global configuration mode, use the following command:

sandbox {**cloud-server-check** | **local-server-check**} **enable**

- **cloud-server-check** | **local-server-check** - Specifies to enable the cloud sandbox (**cloud-server-check**) or the local sandbox (**local-server-check**).

To disable the cloud sandbox or the local sandbox, in the global configuration mode, use the command **no sandbox** {**cloud-server-check** | **local-server-check**} **enable**.

Configuring the Local Sandbox

To configure parameters of the local sandbox, in the global configuration mode, use the following command:

sandbox local-server address*ip-address***vrouter***vr-name* [**port** *port*]

- **address** *ip-address* - Specifies the IP address of the local sandbox.
- **vrouter** *vr-name* - Specifies the VRouter of the local sandbox.
- **port** *port*- Specifies the port of the local sandbox, the default value is 443.

To delete the specified parameters, in the global configuration mode, use the command **no sandbox local-server address** .

Creating a Sandbox Profile

To create a sandbox Profile, in the global configuration mode, use the following command:

sandbox-profile*sandbox-profile-name*

- *sandbox-profile-name* - Specifies the sandbox profile name and enters the sandbox profile configuration mode. If the specified name exists, then the system will directly enter the sandbox profile configuration mode.

To delete the specified sandbox profile, in the global configuration mode, use the command **no sandbox-profile** *sandbox-profile-name*.

Enabling White List

The white list includes domain names that are safe. When a file extracted from the HTTP traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox or the local sandbox. To enable the white list function, in the sandbox profile configuration mode, use the following command:

whitelist enable

To disable this function, use **no whitelist enable**.

Configuring Certificate Verification

System supports to enable the verification for the trusted certification. After enabling, system will not detect the PE file whose certification is trusted.

To enable the certificate verification, in the sandbox profile configuration mode, use the following command:

certificate-validation enable

To disable this function, use **no certificate-validation enable**.

Configuring File Filter

The file filter marks the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analyze result from the cloud sandbox or form the local sandbox determines whether this suspicious file is legal or not.

You can set the following criteria:

Mark the file of the specified file type as a suspicious file. The system can mark the PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP, Script, and Others file as a suspicious file now. Use the following command in the sandbox profile to specify the file type:

file-type {**pe** | **apk** | **jar** | **swf** | **ms-office** | **pdf** | **rar** | **zip** | **elf** | **script** | **other**} [**use-server** [**cloud-server** | **local-server**]

- **pe** - Mark the PE file as a suspicious file.
- **apk** - Mark the APK file as a suspicious file.
- **jar** - Mark the JAR file as a suspicious file.
- **swf** - Mark the SWF file as a suspicious file.
- **ms-office** - Mark the MS-Office file as a suspicious file.
- **pdf** - Mark the PDF file as a suspicious file.
- **rar** | **zip** - Mark the RAR or ZIP file as a suspicious file.
- **elf** - Mark the ELF file as a suspicious file.
- **script** - Mark the Script file as a suspicious file.
- **other** - Mark the file of all types other than the types above as a suspicious file.

- **use-server [cloud-server | local-server]** - Specifies to upload the suspicious file to the cloud sandbox **cloud-server**) or to the local sandbox (**local-server**) for detection. By default, the suspicious file will be uploaded to the cloud sandbox for detection.

To cancel the file type setting, use **no file-type {pe | apk | jar | swf | ms-office | pdf | rar | zip | elf | script | other}**.If no file type is specified, the Sandbox function will mark no file as a suspicious one.

Specifies the protocol to scan and directions of the detection. The system can scan the HTTP, FTP, POP3, SMTP, IMAP4 and SMB traffic now. If SMB protocol type is used, the system supports the filtering and blocking of files in break-point resumption scenarios. Use the following command in the sandbox profile to specify the protocol:

protocol {http | ftp | imap4 | pop3 | smtp | smb} direction {download | upload | both}

- **http | ftp | imap4 | pop3 | smtp | smb** - Specifies the protocol to scan.
- **download | upload | both** - Specifies the direction of the detection. Upload means direction from client to server. Download means direction from server to client.

If no protocol is specified, the Sandbox function will not scan the network traffic.

In the sandbox profile, use **no protocol {http | ftp | imap4 | pop3 | smtp | smb}** to delete the protocol specifications.

Specifying Actions for a Sandbox Profile

When system identifies the suspicious files as malicious files, it will deal with them with set actions. To specify the actions, in the Sandbox Profile configuration mode, use the following command:

action {reset | log-only}

- **reset** - Specifies the actions as resetting connections. After detecting the malicious files, system will reset connection of malicious link and record threat logs and cloud sandbox logs.
- **log-only** – Specifies the actions as recording logs. After detecting the malicious files, system will release traffic and record logs (threat logs and cloud sandbox logs) only.

Disabling Suspicious File Uploading

By default, the file will be uploaded to the cloud sandbox when it marks it is classified as suspicious. You can disable the function of suspicious file uploading, which will prevent the suspicious file from being uploaded to the cloud sandbox. In the sandbox profile configuration mode, use the following command:

file-upload-disable

In the global configuration mode, use **no file-upload-disable** command to restore the function of suspicious file uploading.

Binding a Sandbox Profile to a Policy Rule

If the sandbox profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the sandbox profile to a policy rule, in the policy rule configuration mode, use the following command:

sandbox {*sandbox-profile-name* | **predef_low** | **predef_middle** | **predef_high**}

- *sandbox-profile-name* – Specifies the name of the sandbox profile that will be bound to the policy rule.
- **predef_low | predef_middle | predef_high** - Bind the predef_low/ predef_middle/predef_high sandbox profile。

To cancel the binding, in the policy rule configuration mode, use the following command: **no sandbox**

Enabling Benign File

If you enable the Benign File function, system will record cloudsandbox logs of the file when it marks it as a benign file. By default, system will not record logs for the benign files.

To enable the Benign File function, in the global configuration mode, use the following command:

sandbox benign-file report enable

In the global configuration mode, use **no sandbox benign-file report enable**command to disable the Benign File function.

Enabling the Greyware File function

If you enable Greyware File function, system will record cloudsandbox logs of the file when it marks it as a greyware file. A greyware file is the one system cannot judge it is a benign file or a malicious file. By default, system will not record logs for the greyware files.

To enable the Greyware File function, in the global configuration mode, use the following command:

sandbox greyware report enable

In the global configuration mode, use **no sandbox greyware report enable**command to disable the Greyware File function.

Configuring the File Size Limit

The file that is smaller than the specified file size will be marked as a suspicious file. To specify the file size limit, in the global configuration mode, use the following command:

sandbox file-type {**pe** | **apk** | **jar** | **swf** | **ms-office** | **pdf** | **rar** | **zip** | **elf** | **script** | **other**} **max-file-size** *size*

- **pe** - Make the PE file as a detection object.
- **apk** - Make the APK file as a detection object.
- **jar** - Make the JAR file as a detection object.
- **swf** - Make the SWF file as a detection object.
- **ms-office** - Make the MS-Office file as a detection object.
- **pdf** - Make the PDF file as a detection object.
- **rar** | **zip** - Make the RAR or ZIP file as a detection object.
- **elf**- Make the ELF file as a detection object.

- **script** - Make the Script file as a detection object.
- **other** - Mark the file of all types other than the types above as a detection object.
- **max-file-size***size* - Specify the file size. Mark the file that is small than the specified file size as a detection object.

To cancel the file size limit setting, use the command **no sandbox file-type** {**pe** | **apk** | **jar** | **swf** | **ms-office** | **pdf** | **rar** | **zip** | **elf** | **script** | **other**} **max-file-size** *size*.

Adding Items to the Trust List

The threat list means the list of threat items in the Hillstone device. There are three sources of the threat items:

- The Hillstone device finds suspicious file and upload this file to the local sandbox or to the cloud sandbox. After verifying the file is malicious, the cloud sandbox or the local sandbox will send the analysis results and MD5 to the device, and the threat item will be listed in the threat list.
- The Hillstone device finds suspicious file and successfully queries MD5 of the threat in the cloud sandbox or the local sandbox, the threat item will be listed in the threat list.
- The Hillstone device receives the synchronous threat MD5 from the Hillstone cloud service platform and matches the threat, the threat item will be listed in the threat list.

You can add the sandbox threat items to the trust list. Once the item in the trust list is matched, the corresponding traffic will be released and not controlled by the actions of sandbox rule.

To add or remove a sandbox threat item, in any mode, use the following command:

exec sandbox-threat*value* {**trust** | **untrust**}

- *value* – Specifies the name of the sandbox threat item.
- **trust** – Add the sandbox threat item to the trust list.
- **untrust** – Remove the sandbox threat item from the trust list.

Viewing Sandbox Information

To view the sandbox profile information, in any mode, use the following command:

show sandbox-profile [*sandbox-profile-name*]

To view the sandbox status and statistic information, in any mode, use the following command:

show sandbox status

To view the sandbox threat items in the treat list, in any mode, use the following command:

show sandbox threat-entry info

To view the sandbox global configuration information, including , in any mode, use the following command:

show sandbox configuration

Updating Sandbox Whitelist Database

By default system updates the sandbox whitelist database everyday automatically. You can change the update configuration as needed. The configurations of updating sandbox whitelist database include:

- Configuring a sandbox whitelist update mode
- Configuring an Update Protocol
- Configuring an update server
- Specifying a HTTP proxy server
- Specifying an update schedule

- Updating now
- Importing a sandbox whitelist file
- Viewing sandbox whitelist information
- Viewing sandbox whitelist update information

Configuring a Sandbox Whitelist Update Mode

System supports both manual and automatic update modes. To configure a sandbox whitelist update mode, in the global configuration mode, use the following command:

sandbox whitelist update mode {**auto** | **manual**}

- **auto** – Specifies the automatic sandbox whitelist update mode. This is the default mode.
- **manual** – Specifies the manual sandbox whitelist update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no sandbox whitelist update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

sandbox whitelist update protocol HTTP

In the global configuration mode, use the command **no sandbox whitelist update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hill-stonenet.com. You can also configure another up to three update servers to download the latest

sandbox whitelist as needed. To configure the update the server, in the global configuration mode, use the following command:

sandbox whitelist update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hill-stonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no sandbox whitelist update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the sandbox whitelist signature database updating, use the following command in the global configuration mode:

sandbox whitelist update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no sandbox whitelist update proxy-server** {**main** | **backup**}command.

Specifying an Update Schedule

By default, system automatically updates the sandbox whitelist database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

sandbox whitelist update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the sandbox whitelist database immediately as needed. To update the sandbox whitelist database now, in any mode, use the following command:

exec sandbox whitelist update

- **exec sandbox whitelist update** – Only updates the incremental part between the current sandbox whitelist database and the latest sandbox whitelist database released by the update server.

Importing a Sandbox Whitelist File

In some cases, your device may be unable to connect to the update server to update the sandbox whitelist database. To solve this problem, StoneOS provides the sandbox whitelist file import function, i.e., importing the sandbox whitelist files to the device from an FTP, TFTP server or USB disk, so that the device can update the sandbox whitelist database locally. To import the sandbox whitelist file, in the execution mode, use the following command:

import sandbox whitelist from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the sandbox whitelist file that be imported.

Viewing Sandbox Whitelist Information

You can view the sandbox whitelist database information of the device as needed, including the sandbox whitelist database version, and release dates. To view sandbox whitelist database information, in any mode, use the following command:

show sandbox whitelist info

Viewing Sandbox Whitelist Update Information

You can view the sandbox whitelist update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the sandbox whitelist database update. To view the sandbox whitelist update information, in any mode, use the following command:

show sandbox whitelist update

IPS

IPS (Intrusion Prevention System) is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration. StoneOS supports license-controlled IPS, i.e., the IPS function will not work unless an IPS license or TP license has been installed on a StoneOS that supports IPS.

The IPS on StoneOS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, StoneOS will update the signature database automatically everyday to assure its integrity and accuracy.

IPS Detection and Submission Procedure

The protocol detection procedure of IPS consists of two stages: protocol parsing and signature matching.

- Protocol parsing: IPS analyzes the protocol part of the traffic. If the analyze results shows the protocol part contains abnormal contents, the system will process the traffic according to the action configuration. And it can generate logs for the administrator if any anomaly has been detected. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information in Threat log details.
- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration and it can generate logs for the administrator. Each Threat log contains "Threat ID", the signature ID in the signature database. You can view detailed information about the error according to the ID.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "05001" is

the attacking signature ID. The mappings between IDs and protocols are shown in the table below:

ID	Protocol	ID	Protocol	ID	Protocol	ID	Protocol
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Updating IPS Signature Database

By default StoneOS updates the IPS signature database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. StoneOS supports auto update and local update. Non-root VSYS does not support this feature. For more information about the signature database configurations, please refer to the table below.

Configuration	CLI
To configure an update mode (auto by default)	In the global configuration mode, use the following command: • Specifying the update mode: **ips signature update mode {auto | manual}** • Restoring to the default: **no ips signature update mode**
To configure an update protocol	In the global configuration mode, use the following command: • Specifying the update protocol: **ips signature update protocol**

Configuration	CLI
(HTTPS by default)	**HTTP** • Restoring to the default: **no ips signature update protocol HTTP**
To configure an update server	In the global configuration mode, use the following command. The IPv4 and IPv6 address are supported for configuring the update server address. • Specifying the update server: **ips signature update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} • Canceling the server: **no ips signature update** {**server1** | **server2** | **server3**}
To configure an update schedule	In the global configuration mode, use the following command to make the IPS signature database update daily or weekly: **ips signature update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*] In the global configuration mode, use the following command to make the IPS signature database update hourly: **ips signature update schedule hourly** *minute* • *minute* – Specifies the minute that the update starts.
To update now	In the execution mode, use the following command: **exec ips signature update**
To update locally	In the execution mode, use the following command: **import ips signature from** {{**ftp** | **ftps** | **sftp**} **server** *ip-address* [**user** *user-name* **password** *password* | **vrouter** *vr-name*] | **tftp server** *ip-address* [**vrouter** *vr-name*]} *file-name*
To view signature statistics	**show ips signature info**
To view sig-	**show ips signature update**

Configuration	CLI
nature database configurations	

Specifying the HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the IPS signature database updating, use the following command in the global configuration mode:

ips signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the **main** parameter to specify the main proxy server and use the **backup** parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the command **no ips signature update proxy-server** {**main** | **backup**}.

IPS Working Modes

System supports two IPS working modes: log only mode and IPS mode. In log only mode, system only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections; while in IPS mode, system not only generates protocol anomaly alarms and attacking behavior logs, but also blocks attackers or resets connections. By default, system works in IPS mode.

To switch to the IPS mode, in the global configuration mode, use the command **ips mode** {**ips-logonly** | **ips**}.

Configuring IPS

Before enabling IPS, make the following preparations:

1. Make sure your StoneOS version supports IPS.
2. Import an IPS license or TP license and reboot. The IPS will be enabled after the rebooting.

The configuration of IPS includes the following contents:

- Signature set configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- Protocol configurations: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, the system will process the traffic according to the action configuration.
- IPS profile: contains signature set configurations, protocol configurations, and packet capture configurations. You can bind an IPS profile to different directions of the security zone (inbound, outbound, bi-direction) to apply the IPS function to the specified direction, or bind an IPS profile to a policy rule to apply the IPS function to the traffic that matches the specified policy rule.

If a policy rule is bound with an IPS profile and the source and destination security zone are also bound with an IPS Profile, the priority of the IPS detection will be: IPS profile for the policy rule > IPS profile for the destination zone > IPS profile for the source zone.

The system also supports binding the IPS profile to a ZTNA policy to perform IPS detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

With IPS configured, StoneOS will generate an Threat log if any intrusion has been detected. Each Threat log contains a signature ID. You can view detailed information about the signature according to the ID in IPS online help pages. To view Threat logs, use the command **show logging ips**.

Configuration Suggestions

All the IPS rules configured for different attacks and intrusions will eventually affect the final actions. When determining the final action, the system will follow the principles below:

- The IPS working mode has the highest priority. When the working mode is set to log only, no matter what action is specified in other related configurations, the final action will always be log only.
- If you create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature , the system will adopt the following rules:
    - Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only > Deault. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s
    - If one signature set is configured with Capture Packet, the system will capture the packets.
    - The action of the signature set created by Search Condition has high priority than the action of the signature set created by Filter.
- For the IPS Profile that is bound to a security zone or policy rule, you can modify the signature sets for the IPS Profile, or a specific signature and its corresponding action. If any IPS profile has been modified, the system will process the related sessions following the principles below:
    - If the IPS profile reference has been changes, the modification will not take effect on the existing sessions immediately. For example, if the IPS profile bound to the trust zone is IPS-pro1 and then is replaced by IPS-pro2, the existing session will continue to

use IPS-pro1, and only new sessions will use IPS-pro2. To make the IPS profile reference take effect on the existing sessions immediately, use the command **clear session**.

- If the signature set of the referenced IPS profile has been changed, the modification will take effect on the existing sessions immediately.



Notes: The IPS Capture Packets function is supported for A-series devices (except A1605/A1805/A2205) that are installed with SSD, K-series devices that are installed with SSD, X-series devices X8180/X20803/X20812 that are installed with SSD, CloudEdge.

Performing IPS Detection on HTTPS Traffic

To perform the IPS detection on the HTTPS traffic, you need to enable the SSL proxy function for the security policy rule that the HTTPS traffic is matched. The system will decrypt the HTTPS traffic that matches the security policy rule according to the SSL proxy profile and then perform the IPS detection on the decrypted traffic.

According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled IPS disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the IPS detection on the decrypted traffic.
SSL proxy enabled IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic.
SSL proxy disabled IPS enabled	The system performs the IPS detection on the HTTP traffic according to the IPS profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with IPS as well, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled IPS disabled	IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic according to the IPS profile of the zone.
SSL proxy enabled IPS enabled	IPS enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS detection on the decrypted traffic according to the IPS profile of the policy rule.
SSL proxy disabled IPS enabled	IPS enabled	The system performs the IPS detection on the HTTP traffic according to the IPS profile of the policy rule. The HTTPS traffic will not be decrypted and the system will transfer it.



Tip: For more information about SSL proxy, see the SSL Proxy chapter.

IPS Commands

action

When the traffic matches the signatures configured by filter rule and/or search rule, specify the corresponding actions.

Command:

action {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset** | **default**}

Description:

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies that when the signature is hit, the system blocks the IP address of the attacker, and also specifies the block time.

- **permanent** - Specifies that the attacker IP is permanently blocked.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the attacker IP. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies that when the signature is hit, the system blocks the service of the attacker, and also specifies the block time.

- **permanent** - Specifies that the attacker service is permanently blocked.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the attacker service. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

default- Execute the action specified in the signature rule.

Default values:

log-only

Mode:

Filter rule configuration mode;

Search rule configuration mode.

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **action log-only**

affected-software

Configure the affected-software parameter to include signatures, related to the specified software, in the filter rule.

Command:

affected-software {**Apache** | **IE** | **Firefox** | …}

no affected-software {**Apache** | **IE** | **Firefox** | …}

Description:

Apache | **IE** | **Firefox** | … – Enter the name of the software. You can press the Tab key after the**affected-software**parameter to see the entire software list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# ips profile test

hostname(config-ips-profile)# filter-class 1

hostname(config-ips-filter-class)# affected-software Apache

attack-type

Configure the attack-type parameter to include signatures, related to the specified attack type, in the filter rule.

Command:

attack-type {Access-Control | SPAM | Mail | …}

no attack-type {Access-Control | SPAM | Mail | …}

Description:

Access-Control | SPAM | Mail | … - Enter the name of the attack type. You can press the Tab key after the attack-typeparameter to see the entire attack type list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# ips profile test

hostname(config-ips-profile)# filter-class 1

hostname(config-ips-filter-class)# attack-type WEB-PHP

banner-protect enable

Enable the function that protects the banner information of FTP/Web/POP3/SMTP servers and set the new banner information to replace the original one. Use the no form of the command to

disable the function.

Command:

banner-protect enable replace-with *string*

no banner-protect enable

Description:

string - Specifies the banner information.

Default values:

None

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset test template ftp**

hostname(config-ftp-sigset)# **banner-protect enable replace-with vsftp2.0**

brute-force

Enter the brute-force configuration mode, where you can make configurations to block brute-force attacks on FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP/HTTP protocol.

Command:

brute-force

{**ftp** | **imap** | **ldap** | **msrpc** | **pop3** | **rdp** | **smb** | **smtp** | **ssh** | **sunrpc** | **telnet** | **vnc**| **http**} *times***block** {**ip** | **service**} {**permanent** | **second** *timeout* | **hour***timeout* | **day***timeout*}

no {**ftp** | **imap** | **ldap** | **msrpc** | **pop3** | **rdp** | **smb** | **smtp** | **ssh** | **sunrpc** | **telnet** | **vnc** | **http**}

Description:

ftp | **imap** | **ldap** | **msrpc** | **pop3** | **rdp** | **smb** | **smtp** | **ssh** | **sunrpc** | **telnet** | **vnc**| **http** - Specifies the name of the protocol on which the system blocks brute-force attacks.

times - Specifies the number of authentication/login failures allowed within the default five minutes. The value range is from 1 to 100000.

ip | **service** - Specifies the IP address or service of the attacker whose authentication/login attempts fail more than the specified limits. The system will block this specified IP address or service.

permanent - Specifies that the IP address or service of the attacker is blocked permanently.

second *timeout* | **hour***timeout* | **day***timeout* - Specifies the duration (by second/hour/day) for blocking the IP address or service of the attacker. The value range is 60 to 3600 seconds/ 1 to 24 hours/ 1 to 15 days.

Default:

None

Mode:

brute-force configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **brute-force**

hostname(config-ips-profile-bruteforce)# **ftp 100 block ip second 61** (Block the IP address of the attacker, whose authentication/login attempts over the FTP protocol fail more than 100 times, for 61 seconds)

password-protect

In IPS Profile configuration mode, enter the HTTP password protection configuration mode. This way, you can configure the HTTP password protection information and enable/disable the HTTP plaintext password check function.

password-protect

Configuring HTTP Password Protection Information

The system determines whether there is weak password and brute-force decryption by parsing relevant information such as user name, password and login result in the HTTP login message, and provides a default list of fields for user name, password and login result. However, because the content of HTTP protocol relies on the negotiation between the user and the server, to avoid omission, you can customize the configuration of the fields representing user name, password, login success or failure in the actual message, detecting weak password and brute-force decryption of HTTP protocol, and process accordingly based on the configured rules.

In HTTP password protection configuration mode, use the following commands:

- Configure the username: **http-username***username*
    - *username* - Specifies the field of the username in the HTTP login message, which is case-insensitive. Multiple fields are separated by ";". The username needs to be 1 to 512 characters in length. The system provides the following five default username fields: username, user, usrname, j_username, and login.
- Configure the password: **http-userpassword***password*
    - *password* - Specifies the field of the password in the HTTP login message, which is case-insensitive. Multiple fields are separated by ";". The password needs to be 1 to 512 characters in length. The system provides the following five default password fields: password, passwd, pass, pwd, and j_password.
- Configure the login success response code: **http-success-code***success-code*
    - *success-code* - Specifies the response code for login success in the HTTP login message. Multiple codes are separated by ";". The response code needs to be 1 to 512 characters in length. The system provides the following three default login success response codes: 200, 302, and 201.
- Configure the login failure response code: **http-fail-code***fail-code*

- *fail-code* - Specifies the response code for login failure in the HTTP login message. Multiple codes are separated by ";". The response code needs to be 1 to 512 characters in length. The system provides the following four default login success response codes: 200, 302, 201, and 303.

- Configure the login success field: **http-custom-success-login***custom-success-login*
  - *custom-success-login* - Specifies the field of login success in the HTTP login message, which is case-insensitive. Multiple fields are separated by ";". The field needs to be 1 to 512 characters in length. The system provides the following four default fields of login success: loginsuccess, login-success, OK=1, and "successful"."true".
- Configure the login failure field: **http-custom-fail-login***custom-fail-login*
  - *custom-fail-login* - Specifies the field of login failure in the HTTP login message, which is case-insensitive. Multiple fields are separated by ";". The field needs to be 1 to 512 characters in length. The system provides the following six default fields of login failure: loginerror, login-error, loginerr, OK=0, "successful"."fail", and "result"=[].



Notes: When you configure the username, password, login success, login success field, login failure response code, and login failure field, you need to enter the field value in hexadecimal notation after you run the corresponding command. For example, to configure the username as "hillstone; login", you need to enter the **http-username 68696C6C73746F6E653B6C6F67696E** command.

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **password-protect**

hostname(config-ips-profile-pwd-protect)# **http-username 68696C6C73746F6E653B6C6F67696E**

Enabling/Disabling the HTTP Plaintext Check Function

The system supports to enable/disable HTTP plaintext password check function. By default, this function is disabled. With this function enabled, the system will check the password field in the HTTP message. If the password field is not encrypted, an alarm log is generated.

In HTTP password protection configuration mode, use the following commands:

- Enable the HTTP plaintext password check function: **http-plain-text-check enable**
- Disable the HTTP plaintext password check function: **http-plain-text-check disable**

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **password-protect**

hostname(config-ips-profile-pwd-protect)# **http-plain-text-check enable**

bulletin-board

Configure the bulletion-board parameter to include signatures, related to the specified bulletin board, in the filter rule.

Command:

bulletin-board {**CVE** | **BID** | **OSVDB** | …}

no bulletin-board {**CVE** | **BID** | **OSVDB** | …}

Description:

CVE | **BID** | **OSVDB** | … Enter the name of the bulletin board. You can press the Tab key after the **bulletin-board**parameter to see the entire bulletion board list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **bulletin-board CVE**

command-injection-check

Enable the function of detecting the HTTP protocol command injection attack. Use the no form to disable this function.

Command:

command-injection-check enable

no command-injection-check enable

Description:

None

Default values:

None

Mode:

protocol configuration mode

Guidance:

None.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **command-injection-check enable**

confidence

Configure the confidence parameter to include signatures, related to the specified confidence level, in the filter rule.

Command:

confidence {**low** | **medium** | **high**}

no confidence {**low** | **medium** | **high**}

Description:

low | **medium** | **high** – Enter the level of the confidence.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **confidence low**

cc-url

Configure the URL path for the CC URL constraint. After the configuration, the system will make statistics on the frequency of the HTTP requests that access the path. If the frequency exceeds the threshold, the system will block the source IP of the request and the IP will not be able to access the Web server. Use the no form to delete the url configuration.

Command:

cc-url *url_string*

no cc-url *url_string*

Description:

url_string - Specifies the URL path of CC URL constraint. System will check the frequency of the HTTP requests that access the specified paths, includingthe whole or part of the paths. For example, if the configuration is /home/ab, system will check and calculate the HTTP requests like /home/ab/login and /home/abc/login. If the frequency of requests exceeds the threshold,

system will block the source IP of the request and deny its access to the web server. URL path does not support the path format which contains the host name or domain name, for example: the configuration should be / home / login.html, instead of www.baidu.com/home/login.html, while www.baidu.com should be configured in the domain name settings of the Web server. System allows up to 32 URL paths configuration. The length range of each path is 1 to 255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

Non-root VSYS does not support the CC URL constraint.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **domain www.abc.com**

hostname(config-web-server)# **cc-url /home/login.php**

cc-url-limit

Configure t threshold value of visiting frequency of URL path and the time to block IP for the CC URL constraint. After the configuration, the system will make statistics on the frequency of the HTTP requests that access the path. If the frequency exceeds the threshold, the system will block the source IP of the request and the IP will not be able to access the Web server. The system will release the blocked IP and the IP can revisit the Web server after the blocking time.Use the no form to delete the domain name configuration.

Command:

cc-url-limit threshold *value* **action block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day** *timeout*}

no cc-url-limit

Description:

value-Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, the system will block the flow of the IP. The value ranges from 1 to 65535 times per minute.

action block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block time.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the attacker IP. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

Default values:

value – 1 times per minute.

block-ip_time – 60 seconds

Mode:

Web server configuration mode

Guidance:

Non-root VSYS does not support the CC URL constraint.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **domain www.abc.com**

hostname(config-web-server)# **cc-url /home/login.php**

hostname(config-web-server)# **cc-url-limit threshold 1500 action block-ip 100**

check-weakpassword

When configuring an IPS rule, with the Weak Password Detection function, the system checks the strength of the plaintext password which is set under the FTP/Telnet/POP3/IMAP/SMTP protocols in this profile. The password is detected as weak if it meets the conditions configured

in the Weak Password Detection section. In this case, the system issues an alarm log to prevent potential security risks caused by a weak password. Use this command to enter the Weak Password Detection configuration mode to configure parameters including Password Length, Password Character Type, User Name Equals Password, Continuous Character Detection, FTP Anonymous Login Detection, and Specify Weak Password.

Use the no form of this command to restore to the default Weak Password Detection configurations. Default configurations: password length criterion is 6 characters; two character types are covered in a password; User Name Equals Password is enabled; Continuous Character Detection is enabled; FTP Anonymous Login Detection is disabled; Specify Weak Password has no default value.

Commands:

check-weakpassword

no check-weakpassword

Description:

None

Default values:

None

Mode:

IPS Profile configuration mode

Guidance:

Weak password detection function is enabled by default.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-password**

hostname(config-ips-profile-weakpass)#

custom-password add

Add a specified weak password to the weak password dictionary of the Weak Password Detection function. If a password matches the specified weak password, the system will consider it as a

weak one. You can specify up to 100 weak passwords.

Command

custom-password add *weakpassword*

Description

weakpassword - Specifies the weak password to be added into the weak password dictionary.

Default values:

None

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **custom-password add password123**

custom-password delete

Delete a specified weak password from the weak password dictionary of the Weak Password Detection function.

Command:

custom-password delete *weakpassword*

Description:

weakpassword - Specifies the weak password to be deleted from the weak password dictionary.

Default values:

None

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **custom-password delete password123**

deny-method

Specify the HTTP method that is refused by the system. Use the no form to allow the specified HTTP method.

Command:

deny-method {**connect** | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav**| **others**}

no deny-method {**connect** | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav**| **others**}

Description:

connect | **delete** | **get** | **head** | **options** | **post** | **put** | **trace** | **webdav** | **others**- Specifies the refused/allowed HTTP method.

Default values:

All methods are allowed by default.

Mode:

protocol configuration mode

Guidance:

When the system discovers the requested method is not allowed, it will disconnect the connection.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **deny-method post**

disable

Disable the Weak Password Detection function.

Command:

disable

Description:

None

Default values:

By default, the Weak Password Detection function is enabled.

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **disable**

disable protocol-anomaly

Disable a signature rule in a profile. Use the no form to re-enable this signature rule.

Command:

disable protocol-anomaly *id*

no disable protocol-anomaly *id*

Description:

id - Specifies the ID of the enabled/disabled signature rule.

Default values:

None

Mode:

Protocol configuration mode

Guidance:

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **disable protocol-anomaly 360002**

disable signature

Disable a certain signature in a profile. Use the no form to re-enable this signature.

Command:

disable signature *id*

no disable signature *id*

Description:

id - Specifies the ID of the enabled/disabled signature.

Default values:

None

Mode:

IPS profile configuration mode

Guidance:

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **disable signature 160009**

domain

Configure the domain name for the Web server. Use the no form to delete the domain name configuration.

Command:

domain *domain_name*

no domain *domain_name*

Description:

domain_name -Specifies the domain name of the Web server. You can specify up to 255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

Cannot configure the domain name for the default Web server.

You can configure up to 5 domain names for each Web server.

The domain name of the Web server follows the longest match principle as shown below:

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **domain abc.com**

hostname(config-web-server)# **exit**

hostname(config-http-sigset)# **web-server web_server2**

hostname(config-web-server)# **domain email.abc.com**

With the above configurations, the traffic that accesses the news.abc.com will be matched to the web_server1, the traffic that accesses the www.email.abc.com will be matched to the web_server2, and the traffic that accesses the www.abc.com.cn will be matched to the default Web server.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **domain www.abc.com**

dst-ip

Configure the destination IP address for the IPS white list. Use the no form to delete the IP address.

Command:

dst-ip *A.B.C.D | A.B.C.D/M*

no dst-ip

Description:

A.B.C.D | A.B.C.D/M-Specifies the destination address IP address for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

hostname(config)# **ips whitelist white1**

hostname(config-ips-whitelist)# **dst-ip 10.1.1.2**

enable

Enable the Web server. Use the no form to disable the Web server.

Command:

enable

no enable

Description:

None

Default values:

Enable the Web server.

Mode:

Web server configuration mode

Guidance:

The default Web server is enabled by default and it cannot be disabled

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **enable**

enable

Enable the Weak Password Detection function.

Command:

enable

Description:

None

Default values:

By default, he Weak Password Detection function is enabled.

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

equal-username-check

Enable/disable the weak password detection function of User Name Equals Password. With this function enabled, the password that equals the user name will be detected as a weak password.

Commands:

Enable: **equal-username-check enable**

Disable**equal-username-check disable**

Description:

None

Default values:

None

Mode:

Weak Password Detection configuration mode

Guidance:

By default, User Name Equals Password function is enabled.

Examples

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **equal-username-check enable**

exec ips

Enable/disable the IPS function.

Command:

Enable the function: **exec ips enable**

Disable the function: **exec ips disable**

Description:

None

Default values:

None

Mode:

execution mode

Guidance:

- This command is valid for the platforms with the IPS license installed.
- After executing the **exec ips enable**command or the**exec ips disable**command, you must restart the device to enable or disable the IPS function. After restarting, system's max concurrent sessions might decrease if the function is enabled, or restore to normal if the function is disabled. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 835.
- Non-root VSYS does not support this command.

Example:

hostname# **exec ips enable**

external-link

Configure the URL of external link. The URL must be an absolute path, which indicates that you must enter the protocol, i.e. http://, https:// or ftp://. For example, http://www.-abc.com/script represents that all files located under this path can be referenced by the Web server. Use the no form to delete the specified URL of the external link.

Command:

external-link *url*

no external-link *url*

Description:

url - Specifies the URL of external link.

Default values:

None

Mode:

Web server configuration mode

Guidance:

For each Web server, you can configure up to 32 URLs of external link.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **external-link http://www.abc.com/script**

external-link-check

Enable the function of external link check to control the referenced actions performed by the Web server. Use the no form to disable this function.

Command:

external-link-check enable action {reset | log}

no external-link-check enable

Description:

reset | log - Specifies the actions performed to the behavior of Web site external link.

- reset - If discovering the behavior of Web site external link, reset the connection (TCP) or send the packets (UDP) to notify the unreachable destination and generate the logs.
- log - If discovering the behavior of Web site external link, only generate the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-http-web-server)# **external-link-check enable action reset**

filter-class

When configuring a signature set, you can create a filter rule. And in this filter rule, you can specify the desired signatures by using filter conditions. Use the following command to create a filter rule and enter into the filter rule configuration mode. Use the no form to delete this rule.

Command:

filter-class id [**name** *name*]

no filter-class id

Description:

id - Specifies the ID of the filter rule.

name *name*- Specifies the name of the filter rule.

Default values:

None

Mode:

IPS Profile configuration mode.

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-http-sigset)# **filter-class 1 name test2**

ftp-anonymous-login-check

Enable / disable FTP Anonymous Login Detection. When you log in anonymously through FTP, the system identifies your password as a weak password.

Commands:

Enable: **ftp-anonymous-login-check enable**

Disable: **ftp-anonymous-login-check disable**

Description:

None

Default values:

None

Mode:

Weak Password Detection configuration mode

Guidance:

By default, FTP Anonymous Login Detection is disabled.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **ftp-anonymous-login-check enable**

http-request-flood auth

Configure the authentication method for the HTTP request flood protection. The system judge whether the source IP address of the HTTP request is valid or not by authentication, thus identifying the attack traffic and executing the protection. If it is failed to authenticate a certain source IP address, the system will block the HTTP request generated by the source IP address. Use the no form to cancel the configurations.

Command:

http-request-flood auth {**auto-js-cookie** | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**} [**crawlers-friendly**]

no http-request-flood auth

Description:

auto-js-cookie | **auto-redirect** | **manual-CAPTCHA** | **manual-confirm**

Specifies the authentication method:

- **auto-js-cookie** – Automatic (JS Cookie). This authentication method is automatically completed by the Web browser.
- **auto-redirect** – Automatic (Redirect). This authentication method is automatically completed by the Web browser.
- **manual-CAPTCHA** – Manual (Access confirmation). When using this authentication method, the user that initiates the HTTP requests must click the OK button to complete the authentication.
- **manual-confirm** – Manual (Verification code). When using this authentication method, the user that initiates the requests must enter the verification code to complete the authentication.

crawlers-friendly - With this parameter entered, the system will not authenticate the crawlers.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood auth auto-js-cookie**

http-request-flood enable

Enable the HTTP request flood protection function and set the request threshold. When the HTTP request rate reaches the configured threshold, the system concludes that the HTTP

request flood happens and it enable the HTTP request flood protection function. Use the no form to disable the function.

Command:

http-request-flood enable [**threshold request** *value*]

no http-request-flood enable

Description:

threshold request *value* - Specifies the request threshold. The value ranges from 0 to 1000000 per second.

Default values:

The default value is 2000 per second.

Mode:

Web server configuration mode

Guidance:

Non-root VSYS does not support the HTTP request flood protection function.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood enable**

http-request-flood proxy-limit

Configure the proxy rate limit. After configuring the proxy rate limit, the system checks whether each source IP belongs to the proxy server. If it belongs to the server, the system limits the proxy rate based on the proxy rate limit. Use the no form to cancel the proxy rate limit.

Command:

http-request-flood proxy-limit threshold*value* {**blockip timeout**{**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*}| **reset**} [**nolog**]

no http-request-flood proxy-limit

Description:

threshold *value* - Specifies the threshold for the request rate. If the received request rate exceeds the configured threshold and the http request flood protection is enabled, the system will perform the corresponding limitations. The value ranges from 0 to 1000000.

blockip timeout {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **reset** - Specifies the limitations that the system is to perform when the request rate exceeds the configured threshold.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the attacker IP. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.
- **reset** – Reset the requests that exceed the configured threshold.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood proxy-limit threshold 10000 reset nolog**

http-request-flood request-limit

Configure the access rate limit. After configuring the access rate limit, the system limits the access rate for each source IP address. Use the no form to cancel the access rate limit.

Command:

http-request-flood request-limit threshold*value* {**blockip timeout**{**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*}| **reset**} [**nolog**]

no http-request-flood request-limit

Description:

threshold *value* - Specifies the threshold for the access rate. If the received request rate exceeds the configured threshold and the http request flood protection is enabled, the system will perform the corresponding limitations. The value ranges from 0 to 1000000.

blockip timeout{**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*}| **reset** - Specifies the limitations that the system is to perform when the request rate exceeds the configured threshold.

- **permanent** - Specifies that the IP address or service of the attacker is blocked permanently.
- **second** *timeout* |**hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP or service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.
- **reset** – Reset the requests that exceed the configured threshold.

nolog - Do not record logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood request-limit threshold 10000 blockip timeout 60**

http-request-flood statistics

Enable the URL request statistics function. Use the no form to cancel the URL request statistics function.

Command:

http-request-flood statistics enable

no http-request-flood statistics enable

Description:

None

Default values:

None

Mode:

Web server configuration mode

Guidance:

Only after executing the **http-request-flood statistics enable**command, the **show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**command can take effect.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood statistics enable**

http-request-flood white-list

Configure the white list for the HTTP request flood protection function. The system will not check the source IP addresses that are added to the white list. Use the no form to cancel the white list configurations.

Command:

http-request-flood white-list *address_entry*

no http-request-flood white-list

Description:

address_entry - Specifies the address entry that will not be checked.

Default values:

None

Mode:

Web server configuration mode

Guidance:

- The address entry cannot be domain names and IPv6 addresses
- If the traffic of the source IP addresses in the white list exceeds the request threshold, the HTTP request flood protection function will be enabled

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood white-list addr1**

http-request-flood x-forward-for

Configure the value of the x-forward-for field of HTTP for HTTP request flood protection. After the configuration, the system will make a statistics of the access frequency of the above field. When the number of HTTP connecting request per second towards this URL reaches the threshold and this lasts 20 seconds, the system will treat it as a HTTP request flood attack.Use the no form to cancel the value configuration of the x-forward-for field.

Command:

http-request-flood x-forward-for {**first** | **last** | **all**}

no http-request-flood x-forward-for

Description:

first | last | all - Specifies the value of the x-forward-for field of HTTP for HTTP request flood protection. **first** is the first value of the x-forwarded-for field, and **last**is the last value of the x-forwarded-for field, and **all**is the all value of the x-forwarded-for field.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood x-forward-for first**

http-request-flood x-real-ip

Enable the x-real-for field statistics for HTTP request flood protection. When enabled, the system calculates the value of the x-real-for field.Use the no form to cancel the configuration.

Command:

http-request-flood x-real-ip enable

no http-request-flood x-real-ip

Description:

None

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **http-request-flood x-real-ip enable**

iframe-check

Enable the function of hides iframe check and configure the function. Through the iframe check, the system recognizes whether there is a hidden iframe HTML page, so as to log or reset the connection. Use the no form to disable this function.

Command:

iframe-check enable action {**log** | **reset**}

no iframe-check enable

Description:

reset | **log** - Specify the action for the HTTP request that hides iframe behavior.

- **reset** – If discovering the behavior of hides iframe, reset the connection (TCP) or send the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the behavior of hides iframe, only generate the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **iframe-check enable action log**

iframe width

Configure the limits of height and width for the iframe check function. Then System will check the iframe of HTML page according to the given height and width.When one value of the height or width in HTML page is less than or equal to the given value, system will identify the happening of hidden iframe attack. and then log or reset the connection. Use the no form to cancel the configurations.

Command:

iframe width *width_value* **height** *height_value*

no iframe

Description:

width *width_value* - Specifies the height value for the iframe, range from 0 to 4096.

height *height_value* - Specifies the width value of the iframe, range from 0 to 4096.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **iframe width 0 height 1**

ips buffer-capture enable

For threats detected by the Intrusion Prevention System, the system can capture the threat data and you can view how the threats occur in threat logs. By default, the function is enabled. After this function is enabled, you can view ASCII and hex information of the threat in the Log Details tab. With the help of data in the **Threat Data** section, you can analyze the whole development

process of the threat. If the **Capture Threat Data** function is not enabled, the **Threat Data** option will not be displayed on the **Threat Log** page.

Command:

ips buffer-capture enable

ips buffer-capture disable

Description:

None

Default values:

Enabled

Mode:

global configuration mode

Guidance:

The Capture Threat Data function is supported for A-series devices (except A1605/A1805/A2205) that are installed with SSD, K-series devices that are installed with SSD,X-series devices X8180/X20803/X20812 that are installed with SSD, CloudEdge

Example:

hostname(config)# **ips buffer-capture enable**

hostname(config)#

ips enable

Enable the IPS function for a certain security zone and specify the IPS Profile to be used. Use the no form to disable the IPS function.

Command:

ips enable {**no-ips** | **predef_default** | **predef_loose** | **predef_critical** | **DMZ-server** | **General-server** | **web-server** | **Unix-like-server** | **Windows-server** | *profile-name*} {**egress** | **ingress** | **bidirectional**}

no ips enable

Description:

no-ips - Use the predefined IPS profile named **no ips**. The**no ips** includes no IPS signatures.

predef_default - Use the predefined IPS profile named **predef_default**. The **predef_default** rule is configured with IPS signatures of medium and high confidence levels, this rule can be used to detect threats and perform the default rule action.

predef_loose - Use the predefined IPS profile named **predef_loose**. The**predef_loose** rule is configured with all the IPS signatures and its default action is log only.

predef_critical - Use the predefined IPS profile named **predef_critical**. The **predef_critical** rule is configured with IPS signatures of the latest high-risk attacks and its default action is reset.

DMZ-server - Use the predefined IPS profile named **DMZ-server**. The **DMZ-server** rule is configured with all detections except TFTP and NETBIOS protocols to detect threats and its default action is log only.

General-server - Use the predefined IPS profile named **General-server**. The **General-server** rule is configured with detections for vulnerability scanning, denial of service attacks and back-door/Trojan-type attacks to detect threats and its default action is log only.

web-server - Use the predefined IPS profile named **web-server**. The **web-server** rule is configured with all Web-type attack detections and enables XSS injection and SQL injection detections to detect threats and its default action is log only.

Unix-like-server - Use the predefined IPS profile named **Unix-like-server**. The **Unix-like-server** rule is configured with all detections in Linux and Solaris system to detect threats and its default action is log only.

Windows-server - Use the predefined IPS profile named **Windows-server**. The **Windows-server** rule is configured with all detections in Windows to detect threats and its default action is log only.

profile-name - Specifies a IPS profile for the current security zone.

egress - Performs the IPS check for the egress traffic of the current security zone.

ingress - Performs the IPS check for the ingress traffic of the current security zone.

bidirectional - Performs the IPS check for both the ingress and egress traffic of the current security zone.

Default values:

None

Mode:

security zone configuration mode

Guidance:

- If the policy rule has been bound with an IPS Profile and the source and destination security zones have been bound with an IPS Profile simultaneously, the system will perform the IPS check according to the following order of priority: IPS Profile bound to the policy rule, IPS Profile bound to the destination security zone, IPS Profile bound to the source security zone.
- For each security zone, you can only bind one IPS Profile with it.

Example:

hostname(config)# **zone trust**

hostname(config-zone-trust)# **ips enable test bidirectional**

ips log aggregation

System can merge IPS logs which have the same protocol ID, the same VSYS ID, the same Signature ID, the same log ID, and the same merging type.Thus it can help reduce logs and avoid to receive redundant logs.

Command:

ips log aggregation {**by-src** | **by-dst** | **by-src-dst**}

Description:

by-src - Merge the IPS logs with the same Source IP.

by-dst - Merge the IPS logs with the same Destination IP.

by-src-dst - Merge the IPS logs with the same Source IP and the same Destination IP.

Default values:

Disabled

Mode:

global configuration mode

Guidance:

- Only support to merge IPS logs.
- Non-root VSYS does not support this command.

Example:

hostname(config)# **ips log aggregation by-src**

ips log http-proxy-ip

System will only record the IP address of the HTTP proxy and not the real IP address of the threat source in threat log. After disabled, system will parse the HTTP header to obtain the real IP address of the threat source, and display the real IP address of the threat source in threat log.

Command:

ips log http-proxy-ip {**enable** | **disable**}

Description:

enable - Enable the device to record HTTP proxy IP.

disable - Disable the device to record HTTP proxy IP.

Default values:

Enabled

Mode:

global configuration mode

Guidance:

Example:

hostname(config)# **ips log http-proxy-ip enable**

ips mode

Specify the IPS work mode. The system supports the IPS online emulation mode and IPS mode.

Command:

ips mode {**ips** | **ips-logonly**}

Description:

ips - Uses the IPS mode. Besides providing the warnings and logs for the abnormal protocols and network attacks, the system can perform the block or reset operation to the discovered attacks.

ips-logonly - Uses the IPS online emulation mode. The system provides the warnings and logs for the abnormal protocols and network attacks, and cannot perform the block or reset operation to the discovered attacks.

Default values:

IPS mode

Mode:

global configuration mode

Guidance:

Non-root VSYS does not support this command.

Example:

hostname(config)# **ips mode ips-logonly**

ips profile

Create an IPS profile and enter the IPS Profile configuration mode. If the specified name already exists, the system will enter the IPS Profile configuration mode directly. Use the no form to delete the specified IPS Profile.

Command:

ips profile {**no-ips** | **predef_default** | **predef_loose**| **predef_critical** | **DMZ-server** | **General-server** | **web-server** | **Unix-like-server** | **Windows-server** | *profile-name*}

no ips profile *profile-name*

Description:

no-ips - Use the predefined IPS profile named **no ips**. The**no ips** includes no IDS signatures

predef_default - Use the predefined IPS profile named **predef_default**. The **predef_default** rule is configured with IPS signatures of medium and high confidence levels, this rule can be used to detect threats and perform the default rule action.

predef_loose - Use the predefined IPS profile named **predef_loose**. The**predef_loose** rule is configured with all the IPS signatures and its default action is log only.

predef_critical - Use the predefined IPS profile named **predef_critical**. The **predef_critical** rule is configured with IPS signatures of the latest high-risk attacks and its default action is reset.

DMZ-server - Use the predefined IPS profile named **DMZ-server**. The **DMZ-server** rule is configured with all detections except TFTP and NETBIOS protocols to detect threats and its default action is log only.

General-server - Use the predefined IPS profile named **General-server**. The **General-server** rule is configured with detections for vulnerability scanning, denial of service attacks and back-door/Trojan-type attacks to detect threats and its default action is log only.

web-server - Use the predefined IPS profile named **web-server**. The **web-server** rule is configured with all Web-type attack detections and enables XSS injection and SQL injection detections to detect threats and its default action is log only.

Unix-like-server - Use the predefined IPS profile named **Unix-like-server**. The **Unix-like-server** rule is configured with all detections in Linux and Solaris system to detect threats and its default action is log only.

Windows-server - Use the predefined IPS profile named **Windows-server**. The **Windows-server** rule is configured with all detections in Windows to detect threats and its default action is log only.

profile-name - Specifies the name of the IPS Profile. The system supports up to 64 user-defined IPS rules and each non-root VSYS supports up to 4 user-defined IPS rules.

Default values:

None

Mode:

global configuration mode

Guidance:

Non-root VSYS also supports predefined IPS Profiles.

Example:

```
hostname(config)# ips profile test
hostname(config-ips-profile)#
```

ips signature

Disable a certain signature. Use the no form to re-enable this signature.

Command:

ips signature id disable

no ips signature id disable

Description:

id - Specifies the ID of the enabled/disabled signature.

Default values:

None

Mode:

global configuration mode

Guidance:

- When a certain signature is disabled, it is the disabled status in the signature set as well.
- Non-root VSYS does not support this command.

Example:

hostname(config)# **ips signature 160009 disable**

ips sigset

Use the existing pre-defined protocol as a template and create a user-defined protocol based on this template. Enter the protocol configuration mode. If the specified name already exists, the system will enter the protocol configuration mode directly. Use the no form to delete the specified protocol.

Command:

ips sigset *sigset-name* [**template** {**dhcp** | **dns** | **finger** | **ftp** | **http** | **imap** | **ldap** | **msrpc** | **mssql** | **mysql** | **netbios** | **nntp** | **oracle** | **other-tcp** | **other-udp** | **pop3** | **smtp** | **snmp** | **sun-rpc** | **telnet** | **tftp** | **voip**}]

no ips sigset *sigset-name*

Description:

sigset-name - Specifies the name of the protocol.

dhcp | dns … | voip - Selects a predefined protocol as the template.

Default values:

None

Mode:

global configuration mode

Guidance:

- The predefined protocol cannot be deleted and edited.
- The user-defined protocol cannot have the same name as the predefined protocol.
- Cannot create signature set based on the user-defined signature set.
- Protocols of the same type cannot be added to one IPS Profile. For example, two protocols created based on the HTTP template cannot be added to one IPS Profile.

Example:

```
hostname(config)# ips sigset http1 template http
hostname(config-http-sigset)#
```

ips suspicious-ua-detection whitelist

Create the UA whitelist entry for the Suspicious UA Detection function. When a whitelist entry is created, the system will not perform suspicious UA detection for traffic matching the UA string in the whitelist. You can add both predefined and user-defined UA strings to the UA whitelist. Use the no form of the command to delete specified UA whitelist entry.

Commands:

ips suspicious-ua-detection whitelist *string*

no ips suspicious-ua-detection whitelist *string*

Description:

string - Specifies the UA string that is to add to the whitelist. The value range is 1-31 characters.

Default values:

None

Mode:

global configuration mode

Guidance:

None

Command:

hostname(config)# **ips suspicious-ua-detection whitelist abc**

ips suspicious-ua-detection user-define

Add the customized User-Agent string for the Suspicious UA Detection function. When a user-defined UA string is added, the system checks for the added UA string and applies corresponding action if it is detected as suspicious. You can add up to 16 pieces user-defined UAs. Use the no form of the command to delete specified user-defined UA string.

Commands:

ips suspicious-ua-detection user-define *string*

no ips suspicious-ua-detection user-define *string*

Description:

string - Specifies the customized UA string. The value range is 1-31 characters.

Default values:

None

Mode:

global configuration mode

Guidance:

None

Example:

hostname(config)# **ips suspicious-ua-detection user-define abc**

ips whitelist

Configure the white list for IPS. The system will release data packets that match the IPS whitelist, no longer detect and defend, thereby reducing the rate of false reports of threats. IPS whitelist matching criteria include source address, destination address, signature ID, and VRouter. The user needs to configure at least one condition; when the user configure multiple conditions, the data packets need to meet all the conditions and then the system will release. Use the no form to delete the specified white list.

Command:

ips whitelist *list-name*

no ips whitelist *list-name*

Description:

list-name- Specifies the name of IPS whitelist.The length of it ranges from 1 to 255.

Default values:

None

Mode:

global configuration mode

Guidance:

None

Example:

hostname(config)# **ips whitelist white1**

hostname(config-ips-whitelist)#

issue-date

Configure the issue-date parameter to include signatures, issued in the specified year, in the filter rule.

Command:

issue-date *year*

no issue-date *year*

Description:

year - Enter the year when the vulnerability was issued. The range varies from 2000 to 2004.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **issue-date 2006**

length

Specify the length criterion of the password. If a password is shorter than the length criterion, it will be detected as a weak password.

Command:

length*number*

Description:

number - Specify the length criterion of the password. The range of length criterion is from 6 to 50 characters.

Default values:

number - 6 characters

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **length 8**

max-arg-length

Specify the maximum length for the POP3 client command parameters and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-arg-length *length* **action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-arg-length (Restore the length to the default value)

Description:

length - Specifies the maximum length for the POP3 client command parameters (in byte).

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the service of the attacker is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 40 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset pop3-cus template pop3**

hostname(config-pop3-sigset)# **max-arg-length 30 action log-only**

max-bind-length

Specify the allowed maximum length for the MSRPC binding packet and the action performed when discovering this kind of anomaly . Use the no form to restore the length setting to the default value.

Command:

max-bind-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-bind-length- Restore the length to the default value.

Description:

length - Specifies the maximum length for the binding packet (in byte). The value ranges from 16 to 65535.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 2048 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset msrpc-cus template msrpc**

hostname(config-msrpc-sigset)# **max-bind-length 3000 action log-only**

max-black-list

Specify the maximum number of URLs that a Web server black list can contain. When a user accesses a statistic page, the system will add the URL of this page to the black list if the system discovers that the contents in this page violate the external link check and the uploading path check. When a user accesses this statistic page again, the URL will hit the black list, thus, improving the processing speed of the system. Use the no form to cancel the above setting.

Command:

max-black-list *size*

no max-black-list

Description:

size - Specifies the maximum length of URLs that a Web server black list can contain.

Default values:

0

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-http-web-server)# **max-black-list 4096**

max-cmd-line-length

Specify the maximum length of the FTP command line/POP3 client command line/SMTP client command line and the action performed when discovering this kind of anomaly . When calculating the length, both the line feed and carriage return are calculated. Use the no form to restore the length setting to the default value.

Command:

max-cmd-line-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-cmd-line-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the command line (in byte). The maximum length of FTP command line ranges from 5 to 1024. The maximum length of POP/SMTP client command line ranges from 64 to 1024.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset test1 template ftp**

hostname(config-ftp-sigset)# **max-cmd-line-length 80 action log-only**

max-content-filename-length

Specify the allowed maximum length of the attachment name of SMTP emails and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-content-filename-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*}| **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*}| **log-only** | **reset**}

no max-content-filename-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the attachment name of SMTP emails (in byte). The value ranges from 64 to 1024.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only Record a log.

resetReset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset smtp-cus template smtp**

hostname(config-smtp-sigset)# **max-content-filename-length 512 action log-only**

max-content-type-length

Specify the allowed maximum length of the SMTP Content-Type value and the action performed when discovering this kind of anomaly. Use the no form to restore the length setting to the default value.

Command:

max-content-type-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-content-type-length- Restore the length to the default value.

Description:

length - Specifies the maximum length of the SMTP Content-Type value (in byte). The value ranges from 64 to 1024.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

resetReset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset smtp-cus template smtp**

hostname(config-smtp-sigset)# **max-content-type-length 256 action log-only**

max-failure

For each POP3/SMTP session, specify the allowed maximum number of times of errors returned from POP3/SMTP server and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-failure*times***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-failure- Restore the number of times to the default value.

Description:

times - For each POP3 session, specifies the allowed maximum number of times of errors returned from the POP3 server. The value ranges from 0 to 512.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

times – 0 (no limitation)

Mode:

protocol configuration mode

Guidance:

For each POP3/SMTP session, specifying the allowed maximum number of times of errors returned from POP3/SMTP server can prevent the invalid attempts effectively.

Example:

hostname(config)# **ips sigset pop3-cus template pop3**

hostname(config-pop3-sigset)# **max-failure 8 action log-only**

max-input-length

Specify the allowed maximum length of Telnet username and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-input-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-input-length- Restore the number of times to the default value

Description:

length - Specifies the maximum length of Telnet username and password (in byte). The value ranges from 6 to 1024.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 128 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset telnet-cus template telnet**

hostname(config-telnet-sigset)# **max-input-length 30 action log-only**

max-path-length

Specify the allowed maximum length of two SMTP client commands, i.e. reverse-path and forward path and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-path-length *length* **action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **block-service** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-path-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of two SMTP client commands, i.e. reverse-path and forward path (in byte). The value ranges from 16 to 512, including punctuation marks.

block-ip {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 256 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset smtp-cus template smtp**

hostname(config-smtp-sigset)# **max-path-length 128 action log-only**

max-reply-line-length

Specify the allowed maximum length of SMTP server responses and the action performed when discovering this kind of anomaly. When calculating the length, both the carriage return and line feed are calculated. Use the no form to restore the setting to the default value.

Command:

max-reply-line-length *length* **action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **block-service** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-reply-line-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of SMTP server responses (in byte). The value ranges from 64 to 1024.

block-ip {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset smtp-cus template smtp**

hostname(config-smtp-sigset)# **max-reply-line-length 1024 action log-only**

max-request-length

Specify the allowed maximum length of MSRPC request packets and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-request-length *length* **action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **block-service** {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-request-length- Restore the length setting to the default value

Description:

length - Specifies the maximum length of MSRPC request packets (in byte). The value ranges from 16 to 65535.

block-ip {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 65535 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset msrpc-cus template msrpc**

hostname(config-msrpc-sigset)# **max-request-length 60000 action log-only**

max-rsp-line-length

Specify the allowed maximum length of FTP responses and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-rsp-line-length *length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-rsp-line-length- Restore the length setting to the default value.

Description:

length - Specifies the maximum length of FTP responses (in byte). The value ranges from 5 to 1024.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 512 bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset test1 template ftp**

hostname(config-ftp-sigset)# **max-rsp-line-length 100 action log-only**

max-scan-bytes

Specify the maximum length of scanning. Use the no form to restore the setting to the default value.

Command:

max-scan-bytes *length*

no max-scan-bytes

Description:

length - Specifies the maximum length of scanning (in byte).

Default values:

length – 4096

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset test1 template other-tcp**

hostname(config-other-tcp-sigset)# **max-rsp-line-length 1000**

max-text-line-length

Specify the allowed maximum length of the email text in SMTP client and the action performed when discovering this kind of anomaly. When calculating the length, both the carriage return and line feed are calculated. Use the no form to restore the setting to the default value.

Command:

max-text-line-length*length***action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-text-line-length- Restore the length setting to the default value

Description:

length - Specifies the allowed maximum length of the email text in SMTP client (in byte). The value ranges from 64 to 2048.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length – 1000 byte

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset smtp-cus template smtp**

hostname(config-smtp-sigset)# **max-text-line-length 1024 action log-only**

max-uri-length

Specify the allowed maximum length of the HTTP URL and the action performed when discovering this kind of anomaly. Use the no form to restore the setting to the default value.

Command:

max-uri-length*length* **action** {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

no max-uri-length- Restore the length setting to the default value

Description:

length - Specifies the allowed maximum length of URL (in byte). The value ranges from 64 to 4096.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset- Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

length - 4096bytes

Mode:

protocol configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **max-uri-length 1000 action log-only**

max-white-list

Specify the maximum number of URLs that a Web server white list can contain. When a user accesses a statistic page, the system will add the URL of this page to the white list if the system discovers that the contents in this page do not violate the external link check and the uploading path check. When a user accesses this statistic page again, the URL will hit the white list, thus, improving the processing speed of the system. Use the no form to cancel the above setting.

Command:

max-white-list *size*

no max- white-list

Description:

length- Specify the maximum number of URLs that a Web server white list can contain. The value ranges from 0 to 4096.

Default values:

0

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-http-web-server)# **max-white-list 4096**

min-character-type

Specify how many character types should be covered in the password. If the character types covered in a password are less than the specified number, the password will be detected as a weak password.

Command:

min-character-type*number*

Description:

number - Specify how many character types should be covered in the password. Value range is from 1 to 4 types.

Default values:

number - 2 types

Mode:

Weak Password Detection configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **min-character-type 3**

pcap

When the traffic matches the signatures configured in a filter rule or a search rule, the system will capture the packets of the traffic.

Command:

pcap enable

pcap disable

Description:

enable - Capture the abnormal packets. You can view them in the threat log.

disable -Do not capture the abnormal packets.

Default values:

disable

Mode:

Filter rule configuration mode;

search rule configuration mode.

Guidance:

The IPS Capture Packets function is supported for A-series devices (except A1605/A1805/A2205) that are installed with SSD, K-series devices that are installed with SSD,X-series devices X8180/X20803/X20812 that are installed with SSD, CloudEdge.

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **pcap enable**

protocol-check

Enable the protocol legality check for the signature set and configure the strictness level for the protocol legality check.

Command:

protocol-check disable

protocol-check enable action {{ **block-service**{**permanent** | **second***timeout* | **hour***timeout* | **day** *timeout*}| **block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*}| **log-only** | **reset**} **pcap** {**disable** | **enable**}

Description:

enable -Enable the protocol legality check.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset -Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

pcap {disable | enable} enable- Use enable to capture the abnormal packets. You can view them in the threat log. Use **disable**to not capture the abnormal packets.

Default values:

The system disables the protocol legality check.

Mode:

protocol configuration mode.

Guidance:

The IPS Capture Packets function is supported for A-series devices (except A1605/A1805/A2205) that are installed with SSD, K-series devices that are installed with SSD,X-series devices X8180/X20803/X20812 that are installed with SSD, CloudEdge.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **protocol-check strict**

hostname(config-http-sigset)# **protocol-check enable action log-only**

protocol

Configure the protocol parameter to include signatures, related to the specified protocol, in the filter rule.

Command:

protocol {**DNS** | **FTP** | **HTTP** | …}

no protocol { **DNS** | **FTP** | **HTTP** | …}

Description:

DNS | FTP | HTTP | … - Enter the protocol name. You can press the Tab key after the **protocol**parameter to see the entire protocol list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **protocol Telnet**

referer-white-list

Configure the exception URL for the Web server. Once configured, the URL can refer to the Web site, and the other unadded cannot reference the Web site. Use the no form to delete the URL.

Command:

referer-white-list *url_string*

no referer-white-list *url_string*

Description:

url_string - Specifies tht exception URL for Web server. The length of URL is in the range of 1-255 characters.

Default values:

None

Mode:

Web server configuration mode

Guidance:

You can configure up to 32 URL paths.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **referer-white-list www.abc.com**

referer-white-list-check

Enable the referer checking function and configure it. After the configuration, the system can reset the connection or record log for the HTTP Request of the hotlinking and CSRF (Cross Site Request Forgery) attack.Use the no form to disable the function.

Command:

referrer-white-list-check enable action {**log** | **reset**}

no referrer-white-list-check enable

Description:

reset | log Specifies the action for the hotlinking and CSRF attack check for HTTP protocol:

- **reset**: If discovering the hotlinking and CSRF attack, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log**: If discovering the hotlinking and CSRF attack, the system only generates the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

```
hostname(config)# ips sigset test_http template http
hostname(config-http-sigset)# web-server web_server1
hostname(config-web-server)# referrer-white-list-check enable action log
```

response-bypass

Specify does not scan the HTTP server data packets.

Command:

response-bypass

no response-bypass

Description:

None

Default values:

None

Mode:

protocol configuration mode

Guidance:

Only for HTTP protocol

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **response-bypass**

reverse-shell

Enable the rebound shell detection function. With this function enabled, the system detects and defends against rebound shell attacks. If a rebound shell attack is detected, the system will defend it based on user-defined actions. Use the no form of this command to disable the rebound shell detection function.

Command:

reverse-shell enable

no reverse-shell enable

Description:

None

Default values:

By default, this function is disabled.

Mode:

IPS Profile configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **reverse-shell enable**

reverse-shell action

Specifies the defend action against the rebound shell attacks. With the rebound shell detection function enabled, the system detects and defends against rebound shell attacks. If a rebound shell attack is detected, the system will defend it based on user-defined actions.

Command:

reverse-shellaction {**log-only** | **reset** | **block-ip** {**permanent** | **second***timeout* | **hour***timeout* | day*timeout*}}

Description:

action {**log-only** | **reset** | **block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*}}- Specifies the defend action against the rebound shell attacks.

- **log-only** - With this parameter specified, the system only generate logs when it detects the rebound shell attacks.
- **reset** - With this parameter specified, when a rebound shell attack is detected, the system resets connection (TCP) or sends destination unreachable packets (UDP), and then generates logs.
- **block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*} - With this parameter specified, the system blocks the IP address of the rebound shell attacker and the block time is configured.**permanent** - Specifies that the attacker IP is blocked permanently. **second***timeout* | **hour***timeout* | **day***timeout* - Specifies the duration (by second/hour/day) for blocking the attacker IP. The value range is 60 to 3600 seconds/ 1 to 24 hours/ 1 to 15 days.

Default values:

log-only

Mode:

IPS Profile configuration mode

Guidance:

After configuring the defense action against the rebound shell attacks, make sure the rebound shell detection function is enabled. Otherwise, the configuration is only saved but will not take effect.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **reverse-shell enable**

hostname(config-ips-profile)# **reverse-shell action log-only**

reverse-shell level

Specifies the defend mode for the rebound shell attacks. With the rebound shell detection function enabled, the system scans to detect keywords of the rebound shell attack and you need to specify the defend mode for the rebound shell attacks.

Command:

reverse-shelllevel {**high** | **low**}

Description:

level {**high** | **low**}- Specifies the defend mode for the rebound shell attacks.

- **high** - With this parameter specified, when the system scans to detect keywords of the rebound shell attack, logs are reported when the keywords are hit more than twice. This mode can be used in scenarios with high requirements for attack detection.
- **low** - With this parameter specified, when the system scans to detect keywords of the rebound shell attack, logs are reported only when the keywords are hit more than four time. This mode can be used in scenarios where high system performance is required.

Default values:

low

Mode:

IPS Profile configuration mode

Guidance:

After configuring the defense action against the rebound shell attacks, make sure the rebound shell detection function is enabled. Otherwise, the configuration is only saved but will not take effect.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **reverse-shell enable**

hostname(config-ips-profile)# **reverse-shell level high**

search-class

When configuring a signature set, you can create a search rule. And in this search rule, you can specify the desired signatures by using search conditions. Use the following command to create a search rule and enter into the search rule configuration mode. Use the no form to delete this rule.

Command:

search-class *id* **name** *name*

no search-class *id*

Description:

id -Specifies the ID of the search rule.

name *name* -Specifies the name of the search rule.

Default values:

None

Mode:

IPS Profile configuration mode.

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **search-class 1 name test1**

search-condition

When using a search condtion to search signatures, you can specify the information of the signature. The system will perform the fuzzy searching among the following fields: signature ID, signature name, CVE-ID, and signature description:

Command:

search-condition *description*

no search-condition *description*

Description:

description - Enter the information of the desired signatures.

Default values:

None

Mode:

Search rule configuration mode.

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **search-class 1**

hostname(config-ips-filter-class)# **search-condition DNS**

sensitive-file-scan action

Specify the protection action against the Sensitive File Scan attacks on Web servers. If an attacker attempts to scan sensitive files on the Web server, the Web server returns a large number of response packets with the status code "404". In this case, the system counts the number of 404 responses returned by the Web server per minute and conduct corresponding protection actions.

Command:

sensitive-file-scan action {**block-ip**{**permanent**|**second** *timeout*|**hour***timeout*|**day***timeout*} | **block-service**{**permanent**|**second***timeout*|**hour***timeout*| **day***timeout*} | **log-only** | **reset**}

Description:

block-ip {**permanent**|**second** *timeout*|**hour***timeout*|**day***timeout*}- Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second***timeout* | **hour***timeout*| **day***timeout*- Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service{**permanent**|**second***timeout*|**hour***timeout* | **day***timeout*}- Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the service of the attacker is blocked permanently.
- **second***timeout* | **hour***timeout*| **day***timeout*- Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only - Only generate logs when the signature of Sensitive File Scan is matched.

reset - When the signature of Sensitive File Scan is matched, reset the connection (TCP) or send unreachable destination packets, and then generate logs.

Default value:

log-only

Mode:

Web server configuration mode

Guidance:

If the Sensitive File Scan function for Web servers is enabled following the configurations made with this command, the configuration still takes effect. However, if the Sensitive File Scan function for Web servers is disabled, you can make configurations with this command but the configuration does not take effect.

Examples:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **sensitive-file-scan action block-ip second 61**

sensitive-file-scan enable

Enable the Sensitive File Scan function for Web servers. In Sensitive File Scan attacks, an attacker traverses the sites in the Web server by using a file scanning tool. This way, the attacker can obtain sensitive information of the Web server, such as the directory structure, background files, and backup files. Use the no form of this command to disable the Sensitive File Scan function for Web servers.

Commands:

sensitive-file-scan enable

no sensitive-file-scan enable

Description:

None

Default values:

The Sensitive File Scan function for Web servers is disabled by default.

Mode:

Web server configuration mode

Guidance:

None

Examples:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **sensitive-file-scan enable**

sensitive-file-scan warning-value

Specifies the threshold for the system to defend against sensitive file scanning attacks. If the number of times that URL paths match sensitive file dictionaries per minute exceeds the threshold, the system performs the user-specified protection actions.

Command:

sensitive-file-scan warning-value*value*

Description:

value - Specifies the threshold for URL paths to match sensitive file dictionaries per minute. The value range is from 10 to 100 times/min.

Default values:

10 times/ min

Mode:

Web server configuration mode

Guidance:

If the Sensitive File Scan function for Web servers is enabled following the configurations made with this command, the configuration still takes effect. However, if the Sensitive File Scan function for Web servers is disabled, you can make configurations with this command but the configuration does not take effect.

Examples:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **sensitive-file-scan warning-value 20**

serial-character-check

Enable /disable Continuous Character Detection. After this detection is enabled, a password that has less than 10 characters, among which at least 8 characters are the same or in consecutive sequence, will be detected as a weak password, such as 1aaaaaaaa, 1abcdefgh, a87654321.

Commands:

Enable: **serial-character-check enable**

Disable: **serial-character-check disable**

Description:

None

Default values:

None

Mode:

Weak Password Detection configuration mode

Guidance:

By default, Continuous Character Detection is enabled.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **check-weakpassword**

hostname(config-ips-profile-weakpass)# **enable**

hostname(config-ips-profile-weakpass)# **serial-character-check enable**

severity

Configure the severity parameter to include signatures, related to the specified severity, in the filter rule.

Command:

severity {**Low** | **Medium** | **High**}

no severity {**Low** | **Medium** | **High**}

Description:

Low | Medium | High - Enter the severity.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **severity Low**

signature id

Configure the signature id parameter to include signatures, related to the specified id, in the search rule.

Command:

signature id *id*

no signature id *id*

Description:

id - Enter the signature ID.

Default values:

None

Mode:

search rule configuration mode

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **search-class 1**

hostname(config-ips-filter-class)# **signature id 105001**

signature-id

Configure the signature ID for the IPS white list. Use the no form to delete the signature ID.

Command:

signature-id *id*

no signature-id *id*

Description:

id - Specifies the signature ID for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

hostname(config)# **ips whitelist white1**

hostname(config-ips-whitelist)# **signature-id 105002**

sigset

Add the protocol configurations to the IPS Profile. Use the no form to delete the protocol congurations from the IPS Profile.

Command:

sigset *user-defined-profile*

no sigset *user-defined-profile*

Description:

user-defined-profile - Adds the user-defined signature set to the IPS Profile.

Default values:

None

Mode:

IPS Profile configuration mode

Guidance:

None

Example:

hostname(config)# **ips profile ips-profile1**

hostname(config-profile)# **sigset test**

sql-injection

Disable the SQL injection check. Use the no form to enable the SQL injection check.

Command:

sql-injection {**cookie** | **post** | **referer** | **uri**} **disable**

no sql-injection {**cookie** | **post** | **referer** | **uri**} **disable**

Description:

{**cookie** | **post** | **referer** | **uri**} **disable** - Disables the specified SQL injection check, namely HTTP Cookie, HTTP Post, HTTP Refer, or HTTP URI.

Default values:

The SQL injection check is enabled by default.

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **sql-injection cookie disable**

sql-injection-check

Enable the SQL injection check for HTTP protocol.

Command:

sql-injection-check enableaction {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

sql-injection-check disable

Description:

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only - Only generate logs when the signature of SQL injection is matched.

reset - When the signature of SQL injection is matched, reset the connection (TCP) or send unreachable destination packets, and then generate logs.

Default values:

By default, the sensitivity level is low.

Mode:

Web server configuration mode

Guidance:

The severity level of the SQL injection attack is critical. Without configuring actions, the system will only generate logs when discovering SQL injection attack.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **sql-injection-check enable**

src-ip

Configure the source IP address for the IPS white list. Use the no form to delete the IP address.

Command:

src-ip *A.B.C.D | A.B.C.D/M*

no src-ip

Description:

A.B.C.D | A.B.C.D/M - Specifies the source IP address for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

hostname(config)# **ips whitelist white1**

hostname(config-ips-whitelist)# **src-ip 10.1.1.1**

suspicious-ua-detection

Enable /disable Suspicious UA Detection function. With this function enabled, the system can detect suspicious information by identifying the User-Agent string in the HTTP packet.

Commands:

Enable: **suspicious-ua-detection enable**

Disable: **suspicious-ua-detection disable**

Description:

None

Default values:

This function is disabled by default.

Mode:

IPS Profile configuration mode

Guidance:

None

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **suspicious-ua-detection enable**

suspicious-ua-detection action

With the Suspicious UA Detection function enabled, use this command to specify corresponding actions when the User-Agent string in the HTTP packet is detected as suspicious.

Command:

suspicious-ua-detection action {**block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*} |**block-service** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*} | **log-only** | **reset**}

Description:

block-ip - Specifies the protection action is to block the IP address of the attacker.

block-service - Specifies the protection action is to block the service of the attacker.

permanent - Specifies that the IP address or service of the attacker is blocked permanently.

second*timeout* | **hour***timeout* | **day***timeout* - Specifies the duration (by second/hour/day) for blocking the IP address or service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only - Record a log.

reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

Default values:

log-only

Mode:

IPS Profile configuration mode

Guidance:

If Suspicious UA Detection function is enabled following the configuration of this command, the configuration still takes effect. If Suspicious UA Detection function is disabled, you can configure this command but the configuration does not take effect.

Examples:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **suspicious-ua-detection action block-ip day 1**

system

Configure the system parameter to include signatures, related to the specified system, in the filter rule.

Command:

system {Windows | Linux | FreeBSD | …}

no system { Windows | Linux | FreeBSD | …}

Description:

Windows | Linux | FreeBSD | … - Enter the OS name. You can press the Tab key after the **system**parameter to see the entire system list.

Default values:

None

Mode:

Filter rule configuration mode;

Guidance:

None

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **filter-class 1**

hostname(config-ips-filter-class)# **system Linux**

vr

Configure the VRouter for the IPS white list. Use the no form to delete the IP address.

Command:

vr *vr-name*

no vr

Description:

vr-name - Specifies the VRouter for the IPS white list to match.

Default values:

None

Mode:

IPS white list configuration mode

Guidance:

None

Example:

hostname(config)# **ips whitelist white1**

hostname(config-ips-whitelist)# **src-ip 10.1.1.1**

hostname(config-ips-whitelist)# **vr trust-vr**

web-acl

Configure the Web site path and specify the attributes. Use the no form to disable the function.

Command:

web-acl *url* {**static** | **deny**}

no web-acl *url*

Description:

url- Specifies Web site path.

static | **deny** - Specifies the attributes of Web site path:

- **static**- With this attribute specified, the resources in this Web site path can only be accessed as static resources (pictures and text). Otherwise, the system will perform the actions based on the configurations of the uploading path check function (**web-acl-check enable action** {**reset** | **log**}).
- **deny**- With this attribute specified, the resources in this Web site path cannot be accessed.

Default values:

None

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-http-web-server)# **web-acl /eee deny**

web-acl-check

Enable the uploading path check function to prevent the attacker from uploading malicious codes to the Web server. Use the no form to disable the function.

Command:

web-acl-check enable action {**reset** | **log**}

no web-acl-check enable

Description:

reset | **log** - Specifies the control action for the Web site uploading behavior:

- **reset**- If discovering the Web site uploading behavior, the system resets the connection (TCP) or sends the packets (UDP) to notify the unreachable destination and generate the logs.
- **log** – If discovering the Web site uploading behavior, the system only generates the logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

The severity level of the Web site uploading behavior is warnings.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-http-web-server)# **web-acl-check enable action reset**

web-server

Create a Web server and enters the Web server configuration mode. If the name already exists, the system will enter the Web server configuration mode directly. Use the no form to delete the Web server.

Command:

web-server {**default** | *server_name*}

no web-server *server_name*

Description:

default - Configure the default Web server. When creating a HTTP signature set, the system will create a default Web server.

server_name - Specifies the name for the created Web server. You can specify up to 21 characters.

Default values:

None

Mode:

protocol configuration mode

Guidance:

- The default Web server cannot be deleted or edited. The default Web server can detect the following attacks: Sensitive File Scan, SQL injection, XSS injection, iframe attack, ACL, and HTTP request flood.
- You can configure up to 32 Web servers (excluding the default Web server) for each signature set.

Example:

hostname(config)# **ips sigset test_http template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)#

xss-injection

Disable the XSS injection check. Use the no form to enable the XSS injection check.

Command:

xss-check {cookie | post | referer | uri} disable

no xss-injection {cookie | post | referer | uri} disable

Description:

{cookie | post | referer | uri} disable - Disables the specified XSS injection check, namely HTTP Cookie, HTTP Post, HTTP Refer, or HTTP URI.

Default values:

The XSS injection check is enabled by default.

Mode:

Web server configuration mode

Guidance:

None

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server web_server1**

hostname(config-web-server)# **xss-injection uri disable**

xss-check enable

Enable the XSS injection check for HTTP protocol.

Command:

xss-check enableaction {**block-ip** {**permanent** | **second** *timeout* | **hour** *timeout* |**day** *timeout*} | **block-service** {**permanent** |**second** *timeout* | **hour** *timeout* | **day** *timeout*} | **log-only** | **reset**}

xss-check disable

Description:

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only - Only generate logs when this signature is matched.

reset - When this signature is matched, reset the connection (TCP) or send destination unreachable packets (UDP), and then generate logs.

Default values:

None

Mode:

Web server configuration mode

Guidance:

The severity level of the XSS injection attack is Critical. If you configure no action, the system will only record the logs.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **web-server www.abc.com**

hostname(config-web-server)# **xss-check enable**

ips http-multi-decode

In global configuration mode, enter the IPS HTTP multi-decode configuration mode. This way, you can configure the IPS HTTP multi-decode function, including enabling/disabling URL decoding and Unicode decoding function. You can also configure the maximum number of times of HTTP multiple decoding.

ips http-multi-decode

Configuring the IPS HTTP Multi-decode Function

To enhance the detection and protection capacities of the system, the system supports to configure the IPS HTTP Multi-decode function. You can perform multiple decoding on URL or Unicode-encoded HTTP packets, and then detect and protect decoded messages.

URL encoding and Unicode encoding are common encoding formats of HTTP. You can select to enable the corresponding decoding function based on the actual condition.

Perform the following steps:

1. Enable/Disable URL Decoding
2. Enable/Disable Unicode Decoding
3. Configure the Maximum Number of Times of HTTP Multiple Decoding

Enable/Disable URL Decoding

After you enable this function, the system can decode URL-encoded HTTP packets. By default, this function is enabled.

In IPS HTTP multi-decode configuration mode, use the following command to enable and disable URL decoding:

- Enable URL decoding: **url-decode enable**
- Disable URL decoding: **url-decode disable**

Example:

hostname(config)# **ips http-multi-decode**

hostname(config-ips-http-decode)# **url-decode disable**

Enable/Disable Unicode Decoding

After you enable this function, the system can decode Unicode-encoded HTTP packets. By default, this function is enabled.

In IPS HTTP multi-decode configuration mode, use the following command to enable and disable Unicode decoding:

- Enable Unicode decoding: **unicode-decode enable**
- Disable Unicode decoding: **unicode-decode disable**

Example:

hostname(config)# **ips http-multi-decode**

hostname(config-ips-http-decode)# **unicode-decode disable**

Configuring the Maximum Number of Times of HTTP Multiple Decoding

The same HTTP message carrying intrusion attacks may be encoded multiple times. When URL decoding or Unicode decoding is enabled, the system will only decode the HTTP message encoded once, and the HTTP message encoded twice or more will not be fully decoded. You can configure the maximum number of HTTP multiple decoding times to solve the problem that HTTP messages encoded multiple times cannot be fully decoded.

In IPS HTTP multi-decode configuration mode, use the following command:

multi-decode-limit*number*

- *number* - Specifies the maximum number of times the system can decode. Valid values: 1 to 5. Default value: 1. When the number of times the HTTP message has been encoded is greater than the specified maximum number of times to decode, only the data corresponding to the number of times the message has been encoded will be decoded. For example, if the HTPP message has been encoded 3 times and the maximum number of decoding times is specified as 2, only the data encoded in the first two times of the message will be decoded.

Use the following command to restore the default value:

no multi-decode-limit

Example:

hostname(config)# **ips http-multi-decode**

hostname(config-ips-http-decode)# **multi-decode-limit 3**

show ips

Display the configurations about IPS.

Command:

show ips configuration – Shows all information of IPS configurations.(Non-root VSYS does not support this command)

show ips profile [*profile-name*] [**signature-class** *signature-class-id*]- Shows all information of IPS Profile.

show ips sigset [*sigset-name*] – Shows all information of IPS protocol configurations.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood auth-ck** – Shows the corresponding information of the authentication of HTTP request flood protection.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood ip-top** {**max-rate** | **total**} – For HTTP request flood protection, shows the maximum rate ranking of the source IP addresses and the total number ranking.

show ips sigset *sigset-name* **web-server** *server-name* **http-request-flood req-stat** {**overview** {**by-day** | **by-hour** | **by-minute** | **by-second**} | **protect** {**by-day** | **by-hour** | **by-minute** | **by-second**} | **top**} – For HTTP request flood protection, shows the overview, protection information, and requested URL ranking.

show ips status – Shows the status of IPS.

show ips zone-binding – Shows the binding between the security zones and IPS Profiles.

Description:

sigset-name - Specifies the name of the protocol that you want to display.

profile-name - Specifies the name of the IPS profile that you want to display.

signature-class-id - Specifies the ID of the search rule or filter rule that you want to display.

web-server *server-name* - Specifies the name of the Web server that you want to display.

ip-top {**max-rate** | **total**} - Shows the maximum rate ranking of source IP addresses and the total number ranking.

req-stat {**overview** {**by-day** | **by-hour** | **by-minute** | **by-second**} - Shows the overview of the packets, including request numbers, request numbers of different methods (GET and POST), response numbers, response numbers of different status number (4XX and 5XX). You can show the information by days, hours, minutes, or seconds.

protect {**by-day** | **by-hour** | **by-minute** | **by-second**} - Shows the protection information of the packets, including request numbers, response numbers, and other information.

top - Shows the requested URL ranking.

Default values:

None

Mode:

any mode

Guidance:

After executing the **http-request-flood statistics enable**command, the **show ips sigset** *sigset-name* **web-server** *server-name* **http-request-flood req-stat top**command can take effect.

Example:

hostname(config)# **show ips sigset**

Total count: 53

==========

=====

IPS signature set dhcp

Default actions:

Attack-level Action Block Seconds

INFO log noblock 0

WARNING log noblock 0

CRITICAL log noblock 0

Max scan bytes per direction: 0(Unlimited)

Used by 1 IPS profiles:

test

Abnormal Behavior Detection

Overview

There are various threat attacks in networks, such as Web server attacks ,DoS Flood attacks, application layer attacks , Port/Server scan attacks , Amplification attacks, SSL attacks etc. These threats have demonstrated a wide variety of abnormal behaviors. System provide an abnormal behavior detection function based on security zones. This function inspects the sessions of the detected object in multiple factors. When one detected object has multiple abnormal parameters, system will analyze the relationship among the abnormal parameters to see whether an abnormal behavior formed. If there is an abnormal behavior, system will send the alarm message and generate the threat log(s).

The followings are the concept description of the Abnormal Behavior Detection:

- Detected object: The protected objects configured in the Host Defender in this chapter and the protected objects configured in critical assets.
- Parameter: The basic statistical factor of a session, for example, the received bytes of inbound sessions per second. The statistical values of the parameters are used by the system to judge whether the detected object is abnormal or not.
- Baseline: The baseline is the benchmark for the parameters. Value of the baseline is calculated by the system according to the historical data.
- Abnormal behavior model database: The abnormal behavior model database includes the abnormal information of the traffic, which are detecting rules, description of the abnormalities, the reason for the abnormalities, and the suggestions. The information in the database helps you analyze and resolve the abnormal problems. By default, System will update the database at the certain time everyday, and you can modify the update the updating settings according to your own requirements. For more information about how to update, see Updating Abnormal Behavior Model Database. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating

Configuring Abnormal Behavior Detection

To enable the abnormal behavior detection function on system, take the following steps:

1. Make sure your system version supports abnormal behavior detection.
2. Import a StoneShield license and reboot. The abnormal behavior detection will be enabled after the rebooting.

Enabling/Disabling Abnormal Behavior Detection

To enable the zone-based abnormal behavior detection function, in the zone configuration mode, use the following command. By default, the abnormal behavior detection function will detect the entire network covered by this security zone.

anomaly-detection [**host-enable** [**advanced-protection**] [**ddos-protection**]] | [**forensic**]

- **host-enable** – Enable the Host Defender function for the specific zone, for each host which is identified host name, establish a data model for each host which is identified host name, analyze the network behavior of host, and define the corresponding signature dimension for different network behavior, and then detect the abnormal behavior of the host based on the signature dimension, to find the more hidden threat attack. When enabling the Host Defender function, both the DDoS protection function and the abnormal behavior detection of the HTTP factor are not enabled by default. To enable the abnormal behavior detection of the HTTP factor, use the advanced-protection parameter. To enable the DDoS protection, use the ddos-protection parameter, currently, you can defend against the following types of DDoS attacks: Zip of Death, SSL DDoS, DDoS Flood, DDoS Sockstress, DDoS Reflect, Application DDoS, and DNS Query Flood.
- **forensic** – Capture packets. If this parameter is specified, the system will save the evidence messages.

To disable the function, in the zone configuration mode, use the following command:

no anomaly-detection [**host-enable** [**advanced-protection** | **ddos-protection**]][**forensic**]

DNS Mapping

DNS as the domain name resolution protocol,is designed to resolve fixed domain names to IP addresses.Due to the use of domain name is convenient, and is widely used, so the attacker will take different means to use the domain name to generate attack. For example, A IP address can correspond to multiple domain name, the server according to the Host field of HTTP packet to find the Goal URL, the malware will use this feature by modifying the Host field to disguise the domain name, and generate the abnormal behavior. DGA, is the domain generation algorithm, this algorithm will generate a large number of pseudo random domain name, and will be used by malware. ISP DNS hijack, add some of the malicious domain name used by the malicious software to its blacklist.

To solve these problem, DNS domain name analysis can be used as an important basis to determine the malicious behavior. System will monitor the DNS response packets after the abnormal behavior detection function function is enabled, and establish the DNS mapping list, The DNS mapping list is used to store domain names and IP addresses, the pseudo random domain name generated by DGA algorithm, and the black and white domain name updated from the cloud. The device can detect the malware and abnormal behavior attack according the DNS mapping, and generate the threat logs.

Viewing the Entry of DNS Mapping

To view the number of domain name entries in DNS mapping, in any mode,use the following commands:

show dns-mapping

Viewing Detection Status of Dos Attacks

To view the detection status of DOS attacks, in any mode,use the following commands:

show anomaly-detection ddos status

Updating Abnormal Behavior Model Database

By default system updates the abnormal behavior model database everyday automatically. You can change the update configuration as needed. The configurations of updating abnormal behavior

model database include:

- Configuring an abnormal behavior model update mode
- Specifying an automatic update period
- Updating now
- Importing an abnormal behavior model file
- Viewing abnormal behavior model update information

Configuring an Abnormal Behavior Model Update Mode

System supports both manual and automatic (periodicity) update modes. To configure an abnormal behavior model update mode, in the global configuration mode, use the following command:

on mode {1 | 2}

- 1 – **manual**, Specifies the manual update mode.
- 2 – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command:

cloud abnormal-behavior-detection period *period*

- *period* - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the abnormal behavior model database immediately as needed. To update the abnormal behavior model database now, in any mode, use the following command:

exec cloud abnormal-behavior-detection update

- **exec cloud abnormal-behavior-detection update** – Only updates the incremental part between the current abnormal behavior model database and the latest abnormal behavior model database released by the update server.

Importing an Abnormal Behavior model File

In some cases, your device may be unable to connect to the update server to update the abnormal behavior model database. To solve this problem, system provides the abnormal behavior model file import function, i.e., importing the abnormal behavior model files to the device from an FTP, TFTP server or USB disk, so that the device can update the Abnormal Behavior model database locally. To import the abnormal behavior model file, in the execution mode, use the following command:

import cloud abnormal-behavior-detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the abnormal behavior model file that be imported.

Viewing Abnormal Behavior Model Update Information

To view the abnormal behavior model update information, in any mode, use the following command:

show cloud abnormal-behavior-detection update

Advanced Threat Detection

Overview

Advanced Threat Detection , is on the basis of learning advanced threat detection signatures, to analysis the suspicious traffic of host, detect malicious behavior to identify APT (Advanced Persistent Threat) attack and generate the threat logs.

You need to update the malware behavior model database before enabling the function for the first time. For more information about how to update, see Updating Malware Behavior Model Database.

Configuring Advance Threat Detection

To enable the advance threat detection function on system, take the following steps:

1. Make sure your system version supports advance threat detection.
2. Import a StoneShield license and reboot. The advance threat detection will be enabled after the rebooting.

To configure the advance threat detection based on zone, in zone configuration mode, use the following command:

malware-detection [**forensic**]

- **malware-detection** – Enabling the advance threat detection for specific zone.
- **forensic** – Capture packets. If this parameter is specified , the system will save the evidence messages, and support to download it.

To disable the function, in the zone configuration mode, use the following command:

no malware-detection [**forensic**]

Updating Malware Behavior Model Database

By default system updates the malware behavior model database everyday automatically. You can change the update configuration as needed. The configurations of updating malware behavior model database include:

- Configuring a malware behavior model update mode
- Specifying a automatic update period
- Updating now
- Importing a malware behavior model file.
- Viewing malware behavior model update information.

Configuring a Malware Behavior Model Update Mode

System supports both manual and automatic (periodicity) update modes. To configure a malware behavior model update mode, in the global configuration mode, use the following command:

cloud advanced-threat-detection mode {1 | 2}

- 1 – **manual**, Specifies the manual update mode.
- 2 – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command

cloud advanced-threat -detection period *period*

- **period** - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the malware behavior model database immediately as needed. To update the malware behavior model database now, in any mode, use the following command:

exec cloud advanced-threat -detection update

- **exec cloud advanced-threat-detection update** – Only updates the incremental part between the current malware behavior model database and the latest malware behavior model database released by the update server.

Importing a Malware Behavior Model File

In some cases, your device may be unable to connect to the update server to update the malware behavior model database. To solve this problem, system provides the malware behavior model file import function, i.e., importing the malware behavior model files to the device from an FTP, TFTP server or USB disk, so that the device can update the malware behavior model database locally. To import the malware behavior model file, in the execution mode, use the following command:

import cloud advanced-threat -detection from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the malware behavior model file that be imported.

Viewing Malware Behavior Model Update Information

To view the malware behavior model update information, in any mode, use the following command:

show cloud advanced-threat -detection update

Perimeter Traffic Filtering

Overview

Perimeter Traffic Filtering can filter the perimeter traffic based on known risk IP, MAC or Service list, and take logging/block action on the malicious traffic that hits the risk IP, MAC or Service list.

The risk IP list includes the following three types:

- IP Blacklist: The system supports Static IP Blacklist, Blacklist Library, Dynamic IP Blacklist, Real IP Blacklist, and Hit Statistics.
- Service Blacklist: After adding the services to the service blacklist, system will perform the block action to the service until the block duration ends.
- MAC Blacklist: After adding the MAC of the host to the blacklist to prevent users from accessing the network during the specified period.
- IP Reputation list: Retrieve the risk IP (such as Botnet, Spam, Tor nodes, Compromised, Brute-forcer, and so on.) list from the Perimeter Traffic Filtering signature database.
- Configuration: Blacklist global configuration, including Blacklist Log and Session Rematch.

You need to update the IP reputation database before enabling the IP Reputation function for the first time. For more information about how to update, see Updating IP Reputation Database.

Configuring Perimeter Traffic Filtering

Before enabling the Perimeter Traffic Filtering function on system, make sure your StoneOS version supports Perimeter Traffic Filtering.

Enabling/Disabling Perimeter Traffic Filtering

To enable the perimeter traffic filtering and enter the perimeter traffic filtering configuration mode, in config configuration mode, use the following command:

perimeter-traffic-filtering

Configuring Static IP Blacklist

The static IP blacklist will block specified IP address or prevent hosts from accessing the network during the specified period.

To configure the static IP blacklist, in the perimeter traffic filtering configuration mode, use the following command:

blacklist ip [**id***id*] { **address** { **address-book** *address-book* | *start-ip end-ip* | *ip-prefix/mask* } | **user** {{**user** | **group**} *server-name* | **role**} *user-name* } [**vrouter***vrouter-name* | **zone***zone-name*] [**schedule***schedule-name*] {**enable** | **disable**}

- **id** *id* - Specify the ID of static IP blacklist.
- **address-book** *address-book* - Specify the reference address book name of the static IP blacklist.
- *start-ip end-ip* - Specify the IPv4/IPv6 address range of the static IP blacklist.
- *ip-prefix/mask* - Specifies the IP address and the netmask of the static IP blacklist.
- **user** [**user** | **group** | **role**]- Specifies the user type of the static IP blacklist, include user, user group or role.
- *server-name*- Specifies the AAA server name that the user belongs to.
- *user-name*- Specifies the user name of the static IP blacklist.
- **vrouter** *vrouter-name*] | [**zone***zone-name* - Specify the blacklist applied to zone or Virtual Router. If not specified, the blacklist will apply to global.
- **schedule** *schedule-name* - Specifies the schedule that has been configured in the system. If this parameter is specified, the system will block the host from accessing the network during the specified period; if this parameter is not specified, the system will permanently block the

host from accessing the network. For more information about how to create a schedule, see "Creating a Schedule" of "System Management".

- **enable** | **disable** – Enables or disables the static IP blacklist.

To delete the static IP blacklist entry, in the perimeter traffic filtering configuration mode, use the following command:

no blacklist ip id *id*

To view the static IP blacklist information, in any mode, use the following command:

show perimeter-traffic-filtering blacklist ip

Configuring Redundancy Check of Static IP Blacklist

The system supports to check the conflicts among blacklists. You can check whether the blacklists overshadow each other.

To configure redundancy check ofthe static IP blacklist, in any mode,use the following command:

exec perimeter-traffic-filtering blacklist-ip redundancy-check start

To stop redundancy check of the static IP blacklist, in any mode, use the following command:

exec perimeter-traffic-filtering blacklist-ip redundancy-check stop

To view the result of redundancy check, in any mode, use the following command:

show perimeter-traffic-filtering blacklist-ip redundancy

To clear the the result of redundancy check, in any mode, use the following command:

exec perimeter-traffic-filtering blacklist-ip redundancy-check clear

Configuring MAC Blacklist

After adding the MAC of the host to the blacklist to prevent users from accessing the network during the specified period.

To configure the MAC blacklist, in the perimeter traffic filtering configuration mode, use the following command:

blacklist mac [**id** *id*] **address***address* [**schedule** *schedule-name*] {**enable** | **disable**}

- **id** *id* - Specify the ID of MAC blacklist.
- **address** *address* - Specifies the MAC address of the host that will be added to the blacklist.
- **schedule** *schedule-name* - Specifies the schedule that has been configured in the system. If this parameter is specified, the system will block the host from accessing the network during the specified period; if this parameter is not specified, the system will permanently block the host from accessing the network. For more information about how to create a schedule, see "Creating a Schedule" of "System Management".
- **enable** | **disable** – Enables or disables the MAC blacklist.

To delete the blacklist entry, in the perimeter traffic filtering configuration mode, use the following command:

no blacklist mac id *id*

To view the MAC blacklist information, in any mode, use the following command:

show perimeter-traffic-filtering blacklist ip



Notes: The configuration of multicast MAC addresses and broadcast MAC addresses is not supported.

Configuring Blacklist Library

The system support to import/export the blacklist library file or update the blacklist from the specified server, and specify the rule of the blacklist library.

To configure the blacklist library, in the perimeter traffic filtering configuration mode, use the following command:

blacklist lib [**vrouter***vrouter-name* | **zone***zone-name*] {**enable** | **disable**}

- [**vrouter** *vrouter-name* | **zone** *zone-name*] - Specify the blacklist applied to zone or Virtual Router. If not specified, the blacklist will apply to global.
- **enable** | **disable** – Enables or disables the blacklist library.

To import the blacklist library file , in the execution mode, use the following command:

import blacklist-lib {**add** | **cover**} **from** {{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vrouter-name*] *file-name*

- **add** | **cover** - Specify the update mode of blacklist library, **add** means Incremental Import, **cover** means Overwrite Import.
- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**user** *user-name* **password** *password*] - Specifies the IP address, username and password of the FTP, FTPS or SFTP server.
- **tftp server** *ip-address* - Specifies the IP address of the TFTP server.
- **vrouter** *vrouter-name*] - Specifies the VRouter of the FTP, FTPS, SFTP and TFTP server.
- *file-name* – Specifies the name of the blacklist library file that will be imported by using the FTP or TFTP server.
- **http** | **https** – Specifies to use the HTTP or HTTPS server to update the blacklist library.
- **url** *url* – Specifies the URL of the HTTP or HTTPS server. The URL needs to be 1 to 255 characters in length. The URL of the HTTP server needs to start with "http://" and the URL of the HTTPS server needs to start with "https://".
- **vrouter** *vrouter-name* - Specifies the VRouter to which the HTTP or HTTPS server belongs.



Notes:

- The blacklist library file to be imported or automatically updated needs to be in the TXT or CSV format. (This limit applies only to the FTP or TFTP

server).

- The size of the blacklist file to be imported or automatically updated cannot be larger than 40 MB.
- The blacklist library files to be imported or automatically updated will be checked for redundancy in the order of import. If the imported entries are completely covered by the first imported entries, the import will be failed.

To export the blacklist library file , in the execution mode, use the following command:

export blacklist-libto {{**ftp** | **ftps** | **sftp**} **server** *ip-address* [**user** *user-name***password** *password*] | **tftp server** *ip-address*} [**vrouter** *vrouter-name*] *file-name*

- {**ftp** | **ftps** | **sftp**} **server** *ip-address* [**user** *user-name* **password** *password*] - Specifies the IP address, username and password of the FTP, FTPS or SFTP server.
- **tftp server** *ip-address* - Specifies the IP address of the TFTP server.
- **vrouter** *vrouter-name*] - Specifies the VRouter of the FTP, FTPS, SFTP and TFTP server.
- *file-name* – Specifies the name of the blacklist library file that will be exported.

To configure an blacklist library auto update mode, in the perimeter traffic filtering configuration mode, use the following command:

blacklist lib update {**add** | **cover**} **from** { {**ftp server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} *file-name* | {**http** | **https**} **url** *url*} [**vrouter** *vrouter-name*]

- **add** | **cover** - Specify the update mode of blacklist library, **add** means Incremental Import, **cover** means Overwrite Import.
- **ftp server** *ip-address* [**user** *user-name* **password** *password*] - Specifies the IP address, username and password of the FTP server.

- **tftp server** *ip-address* - Specifies the IP address of the TFTP server.
- **vrouter** *vrouter-name*] - Specifies the VRouter of the FTP, TFTP, HTTP and HTTPS server.
- *file-name* – Specifies the name of the blacklist library file that will be imported.
- **http** | **https** – Specifies to update the blacklist library from the HTTP or HTTPS server.
- **url** *url* – Specifies the URL of the HTTP or HTTPS server, which needs to be 1 to 255 characters in length. The URL of the HTTP server needs to start with "http://" and the URL of the HTTPS server needs to start with "https://".

To configure the frequency and time of auto update of the blacklist library, in the perimeter traffic filtering configuration mode, use the following command:

blacklist lib update schedule {**daily** [HH:MM] | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} [HH:MM] | **interval** *time-value*}

- **daily** – Updates the blacklist library every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the blacklist library every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** is used to specify the specific date in a week.
- *HH:MM* – Specifies the time of update, for example, 09:00.
- **interval** – Updates the blacklist library according to the specified period.
- *time-value* – Specifies the period, the range is 30 to 10080 mins.

To clear the current blacklist library file and the current VSYS blacklist library loaded in memory, in any mode, use the following command:

clear perimeter-traffic-filtering blacklist lib

To view the blacklist library information, in any mode, use the following command:

show perimeter-traffic-filtering blacklist lib

To view the configuration information of auto updating blacklist library, in any mode, use the following command:

show perimeter-traffic-filtering blacklist lib update

Configuring Dynamic IP Blacklist

After adding the IP addresses to the global blacklist, system will perform the block action to the IP address and service until the block duration ends.

To configure the dynamic IP blacklist, in any mode, use the following command:

exec block-ip add {{**ip** | **ipv6**} *ip-address*| **user** {**user** | **group**} *server-name* | **role** } *user-name*} [**vrouter** *vrouter-name*] [**timeout** *timeout-value*]

- {**ip** | **ipv6**} *ip-address* - Specifies the IP address to be blocked. Both IPv4 and IPv6 addresses are supported.
- **user** [**user** | **group** | **role**] *user-name* - Specifies the user type to be blocked, including user, user group, or role.
- *server-name*- Specifies the AAA server name to which the user belongs.
- *user-name*- Specifies the user name.
- **vrouter** *vrouter-name* - Specifies the virtual router to which the IP address belongs.
- **timeout** *timeout-value* - Specifies the duration during which the IP address will be blocked. The value ranges from 60 to 1,296,000 seconds. If block duration is not configured, by default, the IP address will be blocked permanently.

To delete the blacklist entry, in any mode, use the following command:

exec block-ip remove {**all** | {{**ip** | **ipv6**} *ip-address*| **user** {{**user** | **group**} *server-name* | **role** } *user-name*} [**vrouter***vrouter-name*] }

To view the dynamic IP blacklist information, in any mode, use the following command:

show block-ip [{**ip** | **ipv6**} *ip-address*]

Configuring Real IP Blacklist

Generally, you can determine the IP address of the client by checking the HTTP packet. However, if the proxy is configured on the client, the source IP contained in the HTTP packet will be the IP address of the proxy server, rather than the real client IP address. In this case, when an attack is detected, the system blocks the IP address of the proxy server, making all services unavailable. To solve this problem, you can determine the real IP address of the client by parsing the X-Forwarded-For and X-Real-IP fields in the HTTP packet. The X-Forwarded-For field is used to record the real IP address of the client and the IP addresses of the proxy servers of different levels. The X-Real-IP field is only used to record the real IP address of the client.

After adding the real IP address of the client to the Real IP Blacklist, the system will perform the block action to that IP address until the block duration ends.

To configure the real IP blacklist, in any mode, use the following command:

exec block-real-ip add {**ip** | **ipv6**} *ip-address* [**vrouter** *vrouter-name*] [**timeout** *timeout-value*]

- {**ip** | **ipv6**} *ip-address* - Specifies the IP address to be blocked. Both IPv4 and IPv6 addresses are supported, but the IPv6 address can be specified only when the system version is IPv6.
- **vrouter** *vrouter-name* - Specifies the virtual router where the blocked IP belongs.
- **timeout** *timeout-value* - Specifies the duration during which the IP address will be blocked. The value ranges from 60 to 1,296,000 seconds. If block duration is not configured, by default, the IP address will be blocked permanently.

To delete the real IP blacklist entry, in any mode, use the following command:

exec block-real-ip remove {**all** | {**ip** | **ipv6**} *ip-address* [**vrouter***vrouter-name*] }

To view information about the real IP blacklist, in any mode, use the following command:

show block-real-ip [{**ip** | **ipv6**} *ip-address*]

- {**ip** | **ipv6**} *ip-address* - Displays the real IP blacklist entry of the specified IP address. Both IPv4 (**ip**) and IPv6 (**ipv6**) addresses are supported, but the IPv6 address can be specified only

when the system version is IPv6. If this parameter is not specified, all real IP blacklist entries will be displayed.

Configuring Static Service Blacklist

The static service blacklist blocks entries in the blacklist within a specified time range by configuring IP masks, IP prefixes, IP ranges, or address book types of IP addresses.

To configure the static service blacklist, in the perimeter traffic filtering configuration mode, use the following command:

blacklist service [**id***id*] **src-ip** {*min-ipv4-address max-ipv4-address* | *ipv4-address/Mask* | *min-ipv6-address max-ipv6-address* | *ipv6/Mask* | **address-book** *address-name*} **dst-ip** {*ipv4-address* | *ipv6-address*} **drt-port** *port-number* **prot** {**tcp** | **udp**} [**schedule** *schedule-name*| **vrouter** *vrouter-name*] {**enable** | **disable**}

- **id** *id* - Specify the ID of the blocked service, range is 1 to 3000.
- **src-ip** {*min-ipv4-address max-ipv4-address* | *ipv4-address/Mask* | *min-ipv6-address max-ipv6-address* | *ipv6/Mask* | **address-book** *address-name*} - Specify the source IP address of the blocked service.
- **dst-ip** {*ipv4-address* | *ipv6-address*} - Specify the destination IP address of the blocked service.
- **vrouter** *vrouter-name* - Specify the virtual router that the IP address belongs to.
- **drt-port** *port-number* - Specify the port number of the blocked service, range is 1 to 65535.
- **proto** {**tcp** | **udp**} - Specify the protocol of the blocked service.
- **schedule** *schedule-name* - Specify the schedule for the blacklist to take effect. The blacklist takes effect in the period specified by the schedule. If the schedule is not configured, the blacklist will always be effective.
- **enable** | **disable** - Specify the status of the blacklist, enable or disable.

To delete the service blacklist, in the perimeter traffic filtering configuration mode, use the following command:

no block-service id *id*

To view the service blacklist information, in any mode, use the following command:

show block-service vrouter *vrouter-name*

Configuring Dynamic Service Blacklist

After adding the services to the service blacklist, system will perform the block action to the service until the block duration ends.

To configure the service blacklist, in any mode, use the following command:

exec block-service add [**src-ip** *src-ip* | **src-ipv6** *src-ipv6*] [**dst-ip** *dst-ip* | **dst-ipv6** *dst-ipv6*] [**vrouter** *vrouter-name*] **drt-port** *port-number* **proto** *protocol*[**timeout** *timeout-value*]

- **src-ip** *src-ip* | **src-ipv6** *src-ipv6* - Specify the source IP address of the blocked service.
- **dst-ip** *dst-ip* | **dst-ipv6** *dst-ipv6* - Specify the destination IP address of the blocked service.
- **vrouter** *vrouter-name* - Specify the virtual router that the IP address belongs to.
- **drt-port** *port-number* - Specify the port number of the blocked service, range is 1 to 65535.
- **proto** *protocol* - Specify the protocol of the blocked service.
- **timeout** *timeout-value* - Specify the blocking duration of the blacklist. The value range is 60 to 1296000 seconds. When the duration is not configured, the default is permanent.

To delete the service blacklist, in any mode, use the following command:

exec block-service remove [**src-ip** *src-ip* | **src-ipv6** *src-ipv6*] [**dst-ip** *dst-ip* | **dst-ipv6** *dst-ipv6*] [**vrouter** *vrouter-name*] **drt-port** *port-number* **proto** *protocol*

To view the service blacklist information, in any mode, use the following command:

show block-service [**ip***ip-address*] [**ipv6***ipv6-address*] [**vrouter***vrouter-name*]

Enabling the Logging Function of Blacklist

To enable the logging function of blacklist, in the perimeter traffic filtering configuration mode, use the following command:

- Enable: **log enable**
- Disable: **log disable**

Configuring Session Rematch of Blacklist

When you add or modify the blacklist, the session will match the optimal blacklist again.

To configure session rematch of blacklist, in the perimeter traffic filtering configuration mode, use the following command:

- Enable: **session rematch ptf enable**
- Disable: **session rematch ptf disable**

Configuring Cache Time For The Hit Count Statistics Data of Blacklist

The storage time of default hit count statistics data of blacklist is short, which causes users fail to view statistics data over longer period. To meet user requirements, the system supports to configure the cache time for the hit count statistics data of blacklist. By default, the system will store the hit count statistics data of blacklist for 6 hours.

To configure cache time for the hit count statistics data of blacklist, in the perimeter traffic filtering configuration mode, use the following command:

blacklist ip hit-age-period *time-value*

- *time-value* - Specify the cache time for IP blacklist hit count statistics data, with the range of 1-72 hours and the default of 6 hours.

To restore the default cache time of the system, in the perimeter traffic filtering configuration mode, use the following command:

no blacklist ip hit-age-period

Viewing the Hit Count Statistics of Blacklist

To view the hit count statistics information of blacklist, in any mode, use the following command:

show perimeter-traffic-filtering blacklist hit-info {{**all** | **top***top-number* | {**ip** | **ipv6**} *ip-address* [**vrouter***vrouter-name* | **zone***zone-name*]}

Clearing the Hit Count Statistics of Blacklist

To clear the hit count statistics information of blacklist, in any mode, use the following command:

clear perimeter-traffic-filtering blacklist hit-info {**all** | **ip** *ip-address* [**vrouter** *vrouter-name* | **zone** *zone-name*]}

Viewing the Enabled Status of the Blacklist Logging Function

To view the enabled status of the blacklist logging function, in any mode, use the following command:

show perimeter-traffic-filtering log

Enabling/Disabling IP BlackList TCP Reset

After the IP BlackList TCP Reset function is enabled, the system will send a TCP-RST packet to the IP address of TCP traffic that hits the blacklist, thus blocking the IP address

To enable the IP BlackList TCP Reset function, in the perimeter traffic filtering configuration mode, use the following command:

blacklist ip tcp-reset enable

To disable the IP BlackList TCP Reset function, in the perimeter traffic filtering configuration mode, use the following command:

no blacklist ip tcp-reset enable

Viewing the Status of IP BlackList TCP Reset

To view the status of the IP BlackList TCP Reset function, in any mode, use the following command:

show perimeter-traffic-filtering blacklist ip tcp-reset

Configuring IP Reputation Filtering

By default StoneOS updates the IP reputation database everyday automatically. You can change the update configuration as needed. The configurations of updating IP reputation database include:

- Enabling IP Reputation Filtering
- Configuring an IP reputation update mode
- Configuring an Update Protocol
- Configuring an update server
- Specifying an update schedule
- Updating now
- Importing an IP reputation file
- Viewing IP reputation information
- Viewing categories of IP reputation
- Viewing IP reputation update information



Notes: To upgrade the IP reputation database, install the IP reputation license and reboot. The IP reputation database upgrade function is available only after the device is reboot.

Enabling IP Reputation Filtering

To enable the IP reputation filtering and enter the IP reputation filtering configuration mode, in the perimeter traffic filtering configuration mode, use the following command:

ip-reputation

To configure the IP reputation filtering function of each category and specify an action for the malicious traffic that hits the IP reputation category, in the IP reputation filtering configuration mode, use the following command:

category *category-type* **action** {**drop** | **log-only** | **block-ip** *timeout*}

- *category-type*- Specifies the category of IP reputation. Valid values: **bot**, **brute-forcer**, **compromised**, **ddos-attacker**, **proxy**, **scanner**, **spam**, **tornode**, and **ioc** (this category is applicable to the IP blacklist in attack and defense drills).
- **action** {**drop** | **log-only** | **block-ip** *timeout*}- Specifies the action for the system hitting the malicious traffic of the specified IP reputation category.
  - **drop** – The system drops the data packet after the system hits the malicious traffic of the specified IP reputation category.
  - **log-only** – The system logs only after the system hits the malicious traffic of the specified IP reputation category. This action is the default action.
  - **block-ip** *timeout*- The system blocks the IP address for a specific period of time after the system hits the malicious traffic of the specified IP reputation category. *timeout* indicates the blocking duration. Valid values: 60 to 1296000. Unit: seconds.

To disable the IP reputation filtering function, in IP reputation filtering configuration mode, use the following command:

no category*category-type*

Configuring an IP Reputation Update Mode

System supports both manual and automatic update modes. To configure an IP reputation update mode, in the global configuration mode, use the following command:

ip-reputation update mode {**auto** | **manual**}

- **auto** – Specifies the automatic IP reputation update mode. This is the default mode.
- **manual** – Specifies the manual IP reputation update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no ip-reputation update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

geolocation-IP-signature update protocol HTTP

In the global configuration mode, use the command **no geolocation-IP-signature update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hill-stonenet.com. You can also configure another up to three update servers to download the latest IP reputation as needed. To configure the update the server, in the global configuration mode, use the following command:

ip-reputation update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hill-stonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-addresss*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no ip-reputation signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the IP reputation signature database updating, use the following command in the global configuration mode:

ip-reputation update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- **ip-address** *port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no perimeter-traffic-filter update proxy-server** {**main** | **backup**}command.

Specifying an Update Schedule

By default, system automatically updates the IP reputation database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

ip-reputation update schedule {**daily** [*HH:MM*] | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} [*HH:MM*] | **hourly** *minute* | **monthly** *date* [*HH:MM*] }

- **daily** [*HH:MM*] – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun**is used to specify the specific date in a week.
- **hourly** *minute* – Updates the database every three hours. This option is the default update schedule *minute*is used to specify the specific minute in one hour.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Importing an IP Reputation File

In some cases, your device may be unable to connect to the update server to update the IP reputation database. To solve this problem, system provides the IP reputation file import function, i.e., importing the IP reputation files to the device from an FTP, TFTP server or USB disk, so that the device can update the IP reputation database locally. To import the IP reputation file, in the execution mode, use the following command:

import ip-reputation from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the IP reputation file that be imported.

Viewing IP Reputation Information

You can view the IP reputation database information of the device as needed, including the IP reputation database version, release dates, and the number of the IP reputation. To view IP reputation database information, in any mode, use the following command:

show ip-reputation info

Viewing Categories of IP Reputation

To view the categories of IP reputation in the IP reputation database, in any mode, use the following command:

show perimeter-traffic-filtering ip-reputation category

Sample command of viewing categories of IP reputation:

```
hostname(config-ptf-iprep-scope)# show perimeter-traffic-filtering ip-reputation category
IP-reputation config table, total num: 10
============================================================
ID                  NAME
------------------------------------------------------------
0                   bot
1                   spam
2                   tornode
3                   compromised
4                   proxy
5                   scanner
6                   brute-forcer
```

```
7               ddos-attacker

8               ioc

================================
================================
====
```

Viewing IP Reputation Update Information

You can view the IP reputation update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the IP reputation database update. To view the IP reputation update information, in any mode, use the following command:

show ip-reputation update

Mitigation

Overview

The system can identify the potential risks and network attacks dynamically, and take action on the risk that hits the mitigation rules.

Mitigation Rule

Tack auto mitigation action on the risk that hits the mitigation rules.

Mitigation rules includes the following two types:

- Predefined rule: this rule is retrieved from the Mitigation signature database. The predefined rules may vary by different mitigation signature databases. About updating the signature database, see Updating Mitigation Rule Database.
- User-defined rule: According to user needs, specify the trigger condition and action.



Notes:

- Mitigation rules only for the threat types of Scan,Dos and Spam
- Predefined rule can not be edited or deleted.

The configurations of auto mitigation rule include:

- Enabling/Disabling auto mitigation
- Configuring the mitigation rule
- Viewing the status of auto mitigation

Enabling/Disabling Auto Mitigation

After enabling auto mitigation , mitigation rules (user-defined rule and predefined rule) to be able to take effect.

To enable/disable auto mitigation, in global command mode, use the following command:

mitigation-status {enable | disable}

- **enable** – Enable the auto mitigation.
- **disable** – Disable the auto mitigation.

Configuring the Mitigation Rule

Only supports to use WebUI to configuring the mitigation rule, see StoneOS_WebUI_User_Guide.

Viewing the Status of Auto Mitigation

To view the status of auto mitigation, in any mode, use the following command:

show mitigation-status

Updating Mitigation Rule Database

By default system updates the mitigation rule database everyday automatically. You can change the update configuration as needed. The configurations of updating malware behavior model database include:

- Configuring a mitigation rule update mode
- Specifying a automatic update period
- Updating now
- Importing a mitigation rule file
- Viewing mitigation rule update information

Configuring a Mitigation Rule Update Mode

System supports both manual and automatic (periodicity) update modes. To configure a mitigation rule update mode, in the global configuration mode, use the following command:

cloud mitigation mode {1 | 2}

- 1 – **manual**, Specifies the manual update mode.
- 2 – **period**, Specifies the automatic (periodicity) update mode.

Specifying an Automatic Update Period

To specify an automatic update period, in the global configuration mode, use the following command:

cloud mitigation period *period*

- **period** - Specifies the automatic update period, the range is 600 to 86400 seconds.

Updating Now

For both manual and automatic update modes, you can update the mitigation rule database immediately as needed. To update the mitigation rule database now, in any mode, use the following command:

exec cloud mitigation update

- **exec cloud mitigation update** – Only updates the incremental part between the current mitigation rule database and the latest mitigation rule database released by the update server.

Importing a Mitigation Rule File

In some cases, your device may be unable to connect to the update server to update the mitigation rule database. To solve this problem, StoneOS provides the malware behavior model file import function, i.e., importing the mitigation rule files to the device from an FTP, TFTP server

or USB disk, so that the device can update the A mitigation rule database locally. To import the mitigation rule file, in the execution mode, use the following command:

import cloud mitigation from {**ftp server** *ip-address* [**user** *user-name* **password** password] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the username and password of the FTP server.
- *file-name* – Specifies the name of the mitigation rule file that be imported.

Viewing Mitigation Rule Update Information

To view the mitigation rule update information, in any mode, use the following command:

show cloud mitigation update

Correlation Analysis

System provides the correlation analysis engine and this engine makes the correlation analysis of the threat events generated by each modules of threat prevention. According to the defined correlation analysis rules, this engine analyzes the happened threat events, try to find the correlation of these threat events and the threats that crosss hosts, and discover the potential threats with high severity. You view the correlation analysis results in WebUI > iCenter > Threat.

Updating Correlation Analysis Engine/Rules

The updating of correlation analysis engine/rule is merged into the updating of abnormal behavior model database. For information of updating abnormal behavior model database, see the Updating Abnormal Behavior Model Database section.

Critical Assets

Critical assets refer to IT assets owned by a company that are essential to its ability to operate and make profit. Those assets include key servers, networking devices, data storage server etc. Since critical assets are essential for business day-to-day operations, they are grown to targets of cyber-attacks. Therefore, the critical assets in a company need to be secured and protected with even stronger defense mechanisms comparing with other individual host machines.

After configuring critical asset object, the system will automatically enable the advanced threat detection and abnormal behavior detection functions in the select security zone, protect the priority and resource for critical asset monitoring, and display the related threat and traffic of the critical asset in the Critical Assets page in iCenter.

Configuring critical assets includes the following items:

- Specifying the name of the critical asset
- Specifying the IP address of the critical asset
- Speicifying the security zone of the critical asset
- View the critical asset configurations

Specifying Critical Asset Name

To specify the critical asset name, in the global configuration mode, use the following command:

critical-asset name *name*

- *name* – Specify the critical asset name and enter into the critical asset object configuration mode. If the name already exists, the system will enter into the critical asset object configuration mode directly.

To delete a critical asset, use the command **no critical-asset name** *name*.

Specifying Critial Asset IP Address

To specify the critical asset IP address, in the critical asset object configuration mode, use the following command:

ip *ip-address*

- *ip-address* – Specify the IP address of the critical asset.

To cancel the IP setting, use the command **no ip**.

Specifying Critial Asset Zone

To specify the security zone where the critical asset locates, in the critical asset object configuration mode, use the following command:

zone *zone-name*

- *zone-name* – Specify the security zone where the critical asset locates. The system will automatically enable the advanced threat detection and abnormal behavior detection functions of this security zone.

To cancel the security zone setting, use the command **no zone**.

Enabling/Disabling Web Server Advanced Protection

Web Server Advanced Protection function to detect HTTP protocol type of Web server attacks, and find the abnormal behavior immediately and correctly. Enable this function, can detect the following types of attacks and behavior:

- Web Vulnerability Scan: A web vulnerability scanner is a program which communicates with a web application through the web front-end in order to identify potential security vulnerabilities in the web application and architectural weaknesses.
- Http-based DoS Attack: Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server

with requests and data. As the name suggests, Http-Based DoS Attack is based on http protocol.

- Web Spider : A Web spider is an internet bot that systematically browses the World Wide Web, typically for the purpose of Web indexing. Web search engines and some other sites use web spider to update their web content or indexes of others sites' web content. Web spider s can copy all the pages they visit for later processing by a search engine that indexes the downloaded pages so that users can search them much more quickly.

To enable the function, in the critical asset object configuration mode, use the following command:

mark-webserver

To disable the function, in the critical asset object configuration mode, use the following command:

no mark-webserver

Renaming a Critical Asset

To rename a critical asset, in the critical asset object configuration mode, use the following command:

rename *new-name*

- *new-name* – Specifies the new name for the critical asset.

Viewing Critical Asset Object Configurations

Use the **show critical-asset object**command to view the critical asset object configurations.

Hot Threat Intelligence

Hillstone Cloud server can push the latest hot threat intelligence to system. Hot threat intelligence page displays this intelligence of hot threats, including IPS vulnerability, virus and threats detected by the cloud sandbox. You can view the details of the hot threats, or carry out protection operations to prevent them via WebUI in iCenter Page.

Enabling /Disabling Hot Threat Intelligence Pushing

Hillstone Cloud server can push the latest hot threat intelligence to system , and once system gets threat intelligence from the Hillstone Cloud server, it will notice and update the list of threat intelligence in WebUI. When the pushing is disabled, Hillstone cloud platform will no longer push the latest hot threat intelligence. Meanwhile, the previously received threat intelligence can only be viewed, and relevant protective operations are not allowed.

To enable the Hot Threat Intelligence Pushing , in the global configuration mode, use the following commands:

- **threat-intelligence push enable**

To disable the Hot Threat Intelligence Pushing , in the global configuration mode, use the following commands:

- **threat-intelligence push disable**

Updating Hot Threat Intelligence Manually

You can manual update the hot Threat Intelligence. System will immediately synchronizes the hot threat intelligence information on the Hillstone cloud platform, and downloads and updates the latest information to the local hot Threat Intelligence list. To update the hot threat intelligence manually, in any mode, use the following command:

exec threat-intelligence update

Geolocation Information Database

Overview

System can display the incoming threat map via WebUI. You can view the selected threat or risky host region. You need to update the geolocation information database before use this function for the first time.

Updating Geolocation Information Database

By default StoneOS updates the geolocation information database everyday automatically. You can change the update configuration as needed. The configurations of updating geolocation information database include:

- Configuring a geolocation information database update mode
- Configuring an Update Protocol
- Configuring an update server
- Specifying an update schedule
- Updating now
- Importing a geolocation information database file
- Viewing geolocation information database information
- Viewing geolocation information database update information

Configuring a Geolocation Information Database Update Mode

System supports both manual and automatic update modes. To configure a geolocation information database update mode, in the global configuration mode, use the following command:

geolocation-IP-signature update mode {**auto** | **manual**}

- **auto** – Specifies the automatic geolocation information database update mode. This is the default mode.
- **manual** – Specifies the manual geolocation information database update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no geolocation-IP-signature update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

geolocation-IP-signature update protocol HTTP

In the global configuration mode, use the command **no geolocation-IP-signature update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest geolocation informations as needed. To configure the update the server, in the global configuration mode, use the following command:

geolocation-IP-signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1 | server2 | server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no geolocation-IP-signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the geolocation information database updating, use the following command in the global configuration mode:

geolocation-ip-signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main | backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no geolocation-ip-signature update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the geolocation information database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

geolocation-IP-signature update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun**is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the geolocation information database immediately as needed. To update the geolocation information database now, in any mode, use the following command:

exec geolocation-IP-signature update [full]

- **exec geolocation-IP-signature update** – Only updates the incremental part between the current geolocation information database and the latest geolocation information database released by the update server.
- **full** – Force to upgrade the current geolocation information database

Importing a Geolocation Information Database File

In some cases, your device may be unable to connect to the update server to update the geolocation information database. To solve this problem, StoneOS provides the geolocation information database file import function, i.e., importing the geolocation information database files to the device from an FTP, TFTP server or USB disk, so that the device can update the geolocation information database locally. To import the geolocation information database file, in the execution mode, use the following command:

import geolocation-IP-signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the geolocation information database file that be imported.

Viewing Geolocation Information Database Information

You can view the geolocation information database information of the device as needed, including the geolocation information database version, release dates, and the number of the geolocation informations. To view geolocation information database information, in any mode, use the following command:

show geolocation-IP-signature info

Viewing Geolocation Information Database Update Information

You can view the geolocation information database update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the geolocation information database update. To view the geolocation information database update information, in any mode, use the following command:

show geolocation-IP-signature update

MITRE ATT&CK® Knowledge Base

MITRE ATT&CK®(Adversarial Tactics, Techniques, and Common Knowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The system supports to map detected suspicious activities to the MITRE ATT&CK® framework and display MITRE ATT&CK® tactics and techniques details on the WebUI. This helps you better identify suspicious behaviors. To ensure the use of the latest MITRE ATT&CK® knowledge base during detection, we recommend that you upgrade the MITRE ATT&CK® knowledge base to the latest version.

Updating MITRE ATT&CK® Knowledge Base

By default StoneOS updates the MITRE ATT&CK® knowledge base everyday automatically. You can change the update configuration as needed. The configurations of updating MITRE ATT&CK® knowledge base include:

- Configuring a MITRE ATT&CK® Knowledge Base Update Mode
- Configuring an Update Protocol
- Configuring an Update Server
- Specifying an HTTP Proxy Server
- Specifying an Update Schedule
- Updating Now
- Importing a MITRE ATT&CK® Knowledge Base File
- Displaying MITRE ATT&CK® Knowledge Base Information
- Displaying MITRE ATT&CK® Knowledge Base Update Information

Configuring a MITRE ATT&CK® Knowledge Base Update Mode

System supports both manual and automatic update modes. To configure a MITRE ATT&CK® knowledge base update mode, in the global configuration mode, use the following command:

ATT&CK update mode {**auto** | **manual**}

- **auto** – Specifies the automatic MITRE ATT&CK® knowledge base update mode. This is the default mode.
- **manual** – Specifies the manual MITRE ATT&CK® knowledge base update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no ATT&CK update mode

Configuring an Update Protocol

The system supports to update the knowledge base through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

ATT&CK update protocol HTTP

In the global configuration mode, use the following command to restore the default value:

no ATT&CK update protocol HTTP

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest MITRE ATT&CK® knowledge base as needed. To configure the update server, in the global configuration mode, use the following command:

ATT&CK update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1 | server2 | server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address* or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update server, in the global configuration mode, use the following command:

no ATT&CK update {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the MITRE ATT&CK® knowledge base, use the following command in the global configuration mode:

ATT&CK update proxy-server {**main** | **backup**} *ip-address port-number*

- **proxy-server {main | backup}** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no att&CK update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the MITRE ATT&CK® knowledge base every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

ATT&CK update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun** is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg,

there is no 30th in February), the database will not be automatically upgraded this month.

- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the MITRE ATT&CK® knowledge base immediately as needed. To update the MITRE ATT&CK® knowledge base now, in any mode, use the following command:

exec ATT&CK update [**full**]

- **exec ATT&CK update** – Only updates the incremental part between the current MITRE ATT&CK® knowledge base and the latest MITRE ATT&CK® knowledge base released by the update server.
- **full** – Force to upgrade the current MITRE ATT&CK® knowledge base

Importing a MITRE ATT&CK® Knowledge Base File

In some cases, your device may be unable to connect to the update server to update the MITRE ATT&CK® knowledge base. To solve this problem, StoneOS provides the MITRE ATT&CK® knowledge base import function, i.e., importing the MITRE ATT&CK® knowledge base files to the device from an FTP, TFTP server or USB disk, so that the device can update the MITRE ATT&CK® knowledge base locally. To import the MITRE ATT&CK® knowledge base file, in the execution mode, use the following command:

import attck signature from {{**ftp** | **ftps** | **sftp**} **server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* [**vrouter** *vrouter-name*]} *file-name*

- **ftp** | **ftps** | **sftp** - Specifies the type of the server.
- *ip-address* – Specifies the IP address of the FTP, TFTP, SFTP, or TFTP server.
- **vrouter** *vrouter-name* – Specifies the VRouter of the FTP, FTPS, SFTP, or TFTP server.

- **user** *user-name* **password** *password* – Specifies the username and password of the FTP/FTPS/SFTP server.
- *file-name* – Specifies the name of the MITRE ATT&CK® knowledge base file to be imported.

Viewing MITRE ATT&CK® Knowledge Base Information

You can view the MITRE ATT&CK® knowledge base information of the device as needed, including the MITRE ATT&CK® knowledge base version and release dates. To view the MITRE ATT&CK® knowledge base information, in any mode, use the following command:

show ATT&CK info

Example:

```
hostname# show ATT&CK info
Signature vendor: Hillstone Networks (Shows the company where the MITRE ATT&CK® knowledge base belongs.)
Current version: 3.0.2 (Shows the current version of the MITRE ATT&CK® knowledge base.)
Release date: 2022/11/08 14:36:16 (Shows the release date of the MITRE ATT&CK® knowledge base.)
```

Viewing MITRE ATT&CK® Knowledge Base Update Information

You can view the MITRE ATT&CK® knowledge base update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the MITRE ATT&CK® knowledge base update. To view the MITRE ATT&CK® knowledge base update information, in any mode, use the following command:

show ATT&CK update

Example:

```
hostname# show ATT&CK update
ATT&CK knowledge base signature update options:
```

protocol: HTTPS (Shows the that the transmission protocol of the MITRE ATT&CK® knowledge base is HTTPS.)

server1:

server2: update2.hillstonenet.com, 443, trust-vr (Shows the update server information of the MITRE ATT&CK® knowledge base.)

server3:

proxy server status: disable (Shows that no proxy server is specified.)

main proxy server:

backup proxy server:

mode: auto (Shows that the update mode of the MITRE ATT&CK® knowledge base is auto.)

schedule: daily 22:34 (Shows the automatic update frequency and time.)

current status: normal (Shows that the update status of the MITRE ATT&CK® knowledge base is normal.)

last update result: not update yet from system up (Shows the last update result of the MITRE ATT&CK® knowledge base.)

Botnet Prevention

Botnet refers to a kind of network that uses one or more means of communication to infect a large number of hosts with bots, forming a one-to-many controlled network between the controller and the infected host, which will cause a great threat to network and data security.

The botnet prevention function can detect botnet host in the internal network timely, as well as locate and take other actions according to the configuration, so as to avoid further threat attacks.

The botnet prevention configurations are based on security zones or policies. If the botnet prevention profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the botnet prevention profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration.



Notes: The botnet prevention function is controlled by license. To use the botnet prevention function, install the Botnet C&C Prevention license.

Preparing

Before enabling botnet prevention, make the following preparations:

1. Make sure your system version supports botnet prevention.
2. Import a botnet C&C prevention license and reboot. The botnet prevention will be enabled after the rebooting.

To view the status of the botnet prevention function, use the command **show version**. To enable or disable the botnet prevention function, in any mode, use the following command:

exec botnet-c2-prevention {**enable** | **disable**}

- **enable** – Enables the botnet prevention function.
- **disable** – Disables the botnet prevention function.

Configuring Botnet Prevention

To configure the botnet prevention function, take the following steps:

1. Enable the botnet prevention function.
2. Define a botnet prevention profile, and specify the protocol types, the actions for the botnet in the profile.
3. Bind the botnet prevention profile to an appropriate policy rule or security zone.



Notes: You need to update the botnet prevention signature database before enabling the function for the first time. For more information about how to update, see Updating Botnet Prevention Signature Database. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating.

You can use default botnet prevention rules or create custom rules. The system provides 3 default botnet prevention rules: predef_critical, predef_default, and no-botnet-c2-prevention.

- **predef_critical** - The strict botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, malicious connection is reset and threat logs will be recorded.
- **predef_default** - The loose botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, traffic is allowed and the system only records threat logs.
- **no-botnet-c2-prevention** – This rule does not implement any botnet prevention check.

Creating a Botnet Prevention Profile

The botnet prevention profile specifies the protocol types and the actions for botnet. To create a botnet prevention Profile, in the global configuration mode, use the following command:

botnet-c2-prevention profile *profile-name*

- *profile-name* - Specifies the botnet prevention profile name and enters the botnet prevention profile configuration mode. If the specified name exists, then the system will directly enter the botnet prevention profile configuration mode.

To delete the specified botnet prevention profile, in the global configuration mode, use the command **no botnet-c2-prevention** *profile-name*.

Specifying the Outreach Type of Threat Prevention and the Corresponding Action

After you specify the outreach type (i.e., IOC tag type) that needs to be protected, when traffic hits the predefined/custom blocking list or cloud query cache blacklist, the IOC tag of the traffic data will be detected and processed based on the specified outreach type and the corresponding action; if not enabled, traffic will be detected and processed based on the protocol configuration of the common type.

To specify the outreach type of Threat Prevention and the corresponding action, in Profile configuration mode of Botnet Prevention, use the following command:

botnet-c2-prevention threat-type {**APT** | **CnC** | **DDNS** | **Malware** | **Miner** | **Phishing** | **Proxy** | **Ransomware** | **Trojan** | **DGA** | **Dns-tunnel** } **protocol** {**tcp** | **http** | **dns** }**action** {**reset**| **log-only** | **sinkhole-replace**} [**intelligent-algorithm** {**enable** | **disable**}]

- **APT** | **CnC** | **DDNS** | **Malware** | **Miner** | **Phishing** | **Proxy** | **Ransomware** | **Trojan** | **DGA** | **Dns-tunnel** – Specifies the outreach type, including APT detection (**APT**) , CnC server detection (**CnC**), dynamic DNS domain detection (**DDNS**), malware detection (**Malware**), miner detection (**Miner**), phishing detection (**Phishing**), proxy server detection (**Proxy**), ransomware detection (**Ransomware**), Trojan detection (**Trojan**), DGA detection (**DGA**), DNS tunnel detection (**Dns-tunnel**).
- **tcp** | **http** | **dns** – Specifies to enable scanning detection for different protocols (TCP, HTTP, DNS) for the selected outreach type.

- **action** { **reset** | **log-only** | **sinkhole-replace**} – Specifies the action to be taken.
  - **reset** – When this parameter is specified, the system resets malicious connections and records threat logs after threat events of the corresponding outreach type occur.
  - **log-only** – When this parameter is specified, the system allows traffic and records only log information (threat logs) after threat events of the corresponding outreach type occur. This is the default action.
  - **sinkhole-replace** - When the protocol type is DNS, you can specify the processing action as "Sinkhole Address Replacement". After the threat is discovered, the system will replace the IP address in the DNS response packet with the Sinkhole IP address.
- [**intelligent-algorithm** {**enable** | **disable**} – Enable (**enable**)/Disable (**disable**) the local intelligent algorithm. For the DGA Detection type (**DGA**) and DNS Tunnel Detection (**Dns-tunnel**) type, the Local Intelligent Algorithm function is enabled by default. You can use this function to improve the accuracy rate of detection and reduce the false positive rate.

Use the following command to delete the outreach type:

no botnet-c2-prevention threat-type {**APT** | **CnC** | **DDNS** | **Malware** | **Miner** | **Phishing** | **Proxy** | **Ransomware** | **Trojan** | **DGA** | **Dns-tunnel** } **protocol** {**tcp** | **http** | **dns** }

Specifying a Protocol Type

To specify a protocol type, in the botnet prevention profile configuration mode, use the following command:

botnet-c2-prevention protocol {**tcp** | **http** | **dns** }**action** {**reset**| **log-only** | **sinkhole-replace**}

- **tcp** – Check for information transferred over TCP.
- **http** – Check for information transferred over HTTP.
- **dns** – Check for information transferred over DNS.

- **action { reset | log-only }** – Specifies the action for the botnets.
  - **reset** – Resets the connection if any botnet has been detected.
  - **log-only** – Generates logs if any botnet has been detected.
  - **sinkhole-replace** - When the protocol type is DNS, you can specify the processing action as "Sinkhole Address Replacement". After the threat is discovered, the system will replace the IP address in the DNS response packet with the Sinkhole IP address.

To cancel the specified protocol type, in the botnet prevention profile configuration mode, use the following command:

no botnet-c2-prevention protocol {tcp | http | dns }

Enabling/Disabling DGA Detection

DNS as the domain name resolution protocol, is designed to resolve fixed domain names to IP addresses. Due to the use of domain name is convenient, and is widely used, so the attacker will take different means to use the domain name to generate attack. For example, A IP address can correspond to multiple domain name, the server according to the endpoint field of HTTP packet to find the Goal URL, the malware will use this feature by modifying the endpoint field to disguise the domain name, and generate the abnormal behavior. DGA, is the domain generation algorithm, this algorithm will generate a large number of pseudo random domain name, and will be used by malware.

To solve these problem, system supports to enable DGA detection function to detect DNS response messages and detect whether the device is attacked by DGA domain name. If a DGA domain name is detected, the system will perform the specified processing actions on the detected DGA domain name according to the configuration of the botnet prevention rules (record the related threat log or reset the connection).

To enable the DGA detection, in the botnet prevention profile configuration mode, use the following command:

dga-detect enable [action {reset| log-only }]

- **enable** - Enable the DGA detection function.
- **action** { **reset** | **log-only**} – Specifies the action for the DGA domain name.
    - **reset** – Resets the connection if any DGA domain name has been detected.
    - **log-only** – Generates logs if any DGA domain name has been detected.

To disable the DGA detection, in the botnet prevention profile configuration mode, use the following command:

dga-detect disable



Notes: DGA detection function only supports X series devices, A series devices and K9180 devices.

Enabling/Disabling the DNS Tunnel Detection

DNS tunnel is a kind of covert channel, which establishes communication by encapsulating other protocols in DNS protocol for transmission. However, most firewalls and detection devices release DNS traffic, and DNS tunnel attacks formally use the features of the release to implement operations such as remote control and file transfer, which cause harm to users' network security and data security. Therefore, the detection, warning, and processing of DNS tunnels are particularly important.

System provides the DNS tunnel detection function. Through the detection of DNS request messages and the monitoring of DNS traffic, the feature extraction and comprehensive analysis of the DNS tunnel can be realized. At the same time, the specified processing action can be performed on the detected DNS tunnel (Record the relevant threat log or reset the connection) to prevent the threat brought by the DNS tunnel.

By default, the DNS tunnel detection function is disabled.

To enable the DNS tunnel detection function, in the botnet prevention profile configuration mode, use the following command:

dns-tunnel-detect enable [**action** {**reset**| **log-only** }]

- **enable** - Enable the DNS tunnel detection function
- **action** { **reset** | **log-only**} – Specifies the action for the DNS tunnel.
  - **reset** – Resets the connection if any DNS tunnel has been detected.
  - **log-only** – Generates logs if any DNS tunnel has been detected.

To disable DNS tunnel detection function, in the botnet prevention profile configuration mode, use the following command:

dns-tunnel-detect disable

Specifying Log Aggregation Type and Aggregation Time

The system can merge botnet prevention logs of the same merging type based on the specified time granularity. This way, logs are reduced to prevent the log server from receiving redundant logs. To configure log aggregation and aggregation time granularity, in the global configuration mode, use the following command:

botnet-c2-prevention agg-log enable [**by-src** | **by-dst** | **by-src-dst** | **by-src-ioc** | **by-dst-ioc** | **by-src-dst-ioc**] [**aggregation-time** *value*]

- **botnet-c2-prevention agg-log enable** - Merges botnet prevention logs of default log aggregation type (**by-src-ioc**) and default time granularity (10 seconds).
- **by-src** - Merges botnet prevention logs of the same source IP.
- **by-dst** - Merges botnet prevention logs of the same destination IP.
- **by-src-dst** - Merges botnet prevention logs of the same source and destination IP.
- **by-src-ioc** - Merges botnet prevention logs of the same source IP and IOC. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.

- **by-dst-ioc** - Merges botnet prevention logs of the same destination IP and IOC. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.
- **by-src-dst-ioc** - Merges botnet prevention logs of the same source IP, destination IP, and IOC. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.
- *value* - Specifies the time granularity of log aggregation. With this parameter specified, at the same time granularity, the system stores botnet prevention logs of the same merging type in the database only once. Value ranges from 10 to 600 seconds. The default value is 10 seconds.

In the global configuration mode, use the command **no botnet-c2-prevention agg-log enable** to specify the log aggregation type as **Do Not Merge**. This way, the system stores each botnet-prevention log in the database and does not merge any logs.

Configuring the DNS Tunnel Log Interval

To specify the minimum time interval for logging after the system detects the DNS tunnel, in the global configuration mode, use the following command:

dns-tunnel-detect log-interval*time-interval*

- *time-interval* - Specifies the minimum time interval for logging after the system detects the DNS tunnel. The range is 1 to 3600 seconds, the default value is 60 seconds.

To restore the default value, in the global configuration mode, use the following command:

no dns-tunnel-detect log-interval



Notes: DNS tunnel detection function only supports X series devices, A series devices and K9180 device.

Address Library Management

The address library includes a predefined address library and a custom address library, each of which contains a block list and an exclude list, which are described as follows:

- Predefined exclude list: It contains domains automatically obtained through the botnet prevention signature database. When the traffic matches to the domain name in the list, system will not control the traffic with botnet prevention function.
- Custom exclude list: It contains IPs, domains and URLs manually added by the user. When the traffic matches to the IP address, domain name or URL in the list, system will not control the traffic with botnet prevention function.
- Predefined block list: It contains IPs, domains and URLs automatically obtained through the botnet prevention signature database. When the traffic matches to the IP address, domain name or URL in the list, system will control the traffic with botnet prevention function.
- Custom block list: It contains IPs, domains and URLs manually added by the user. When the traffic matches to the IP address, domain name or URL in the list, system will control the traffic with botnet prevention function.

The traffic matching sequence will be: Custom exclude list > Custom block list > Predefined exclude list > Predefined block list.

Configuring the Custom Block List

To configure a custom blocklist entry, in the global configuration mode, use the following command:

botnet-c2-prevention signature {**ip***ip-address* [**port***port-number* | **domain***domain-name* [**wildcard**] | **url***url*}

- **ip***ip-address* [**port***port-number* - Specifies the IP address of the custom blocklist entry. If not specified the port,it will be any port.
- **domain***domain-name* [**wildcard**] - Specifies the domain name of the custom blocklist entry. **wildcard** means the domain is a wildcard domain.

To delete the custom blocklist entry, in the global configuration mode, use the following command:

no bot net-c2-prevention signature {**ip***ip-address* [**port***port-number* | **domain***domain-name* [**wildcard**] | **url***url*}

Configuring the Custom Exclude List

To configure a custom exclude list entry, in the global configuration mode, use the following command:

botnet-c2-prevention whitelist {**ip***ip-address* [**port***port-number* | **domain***domain-name* [**wildcard**] | **url***url*}

- **ip***ip-address* [**port***port-number* - Specifies the IP address of the custom exclude list entry.If not specified the port,it will be any port.
- **domain***domain-name* [**wildcard**] - Specifies the domain name of the custom exclude list entry. **wildcard** means the domain is a wildcard domain.

To delete the custom exclude list entry, in the global configuration mode, use the following command:

no bot net-c2-prevention whitelist {**ip***ip-address* [**port***port-number* | **domain***domain-name* [**wildcard**] | **url***url*}

Viewing Custom Signature Entry

To view the custom blocklist entry, in any mode, use the following command:

show botnet-c2-prevention blacklist [**ip***ip-address* [**port***port-number*] | **domain***domain-name* [**wildcard**] | **url***url*]

Description:

- entry: Indicates the IP address, domain name, or URL of the blacklist.
- type: Indicates the type of the blacklist. 1 indicates IP, 2 indicates the exact domain name, 3 indicates the wildcard domain name, 4 indicates IP+Port, and 5 indicates the URL.
- define_type: Indicates in which type the blacklist is defined. 1 indicates the predefined blacklist and 2 indicates the user-defined blacklist.
- tag: Indicates the Botnet tag related to the Botnet C&C IOC Blacklist. If there are multiple tags, only the first 5 tags are displayed.
- malware_family: Indicates the name of the APT group associated with the IOC blacklist.
- APT_group: Indicates the name of the APT group associated with the IOC blacklist.

Example

```
hostname# show botnet-c2-prevention bl ip 118.0.0.2
Botnet Prevention blacklist
Total num: 0
========================================
entry type define type tag malware family APT group
------------------------------------------------------------
--------------------------
========================================
```

To view the custom exclude list entry, in any mode, use the following command:

show botnet-c2-prevention whitelist [**ip***ip-address* [**port***port-number*] | **domain***domain-name* [**wildcard**] | **url***url*]

Configuring the Blacklist Library of Botnet Prevention

You can manually import/export the blacklist library or automatically update the blacklist library file from a specified server.

To manually import a blacklist library file, in the execution mode, use the following command:

import botnet-c2-prevention blacklist-lib {**add** | **cover**} **from** {{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} [**vrouter***vrouter-name*] *file-name*

- **add** | **cover** - Specifies the mode to update the blacklist library, in which **add** indicates incremental import and **cover** indicates overwrite import.
- {**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] - Specifies the IP address and username and password of the account of the FTP/FTPS/SFTP server.
- **tftp server***ip-address* - Specifies the IP address of the TFTP server.
- [**vrouter***vrouter-name*] - Specifies the VRouter to which the FTP, FTPS, SFTP, or TFTP server belongs.
- *file-name* – Specifies the path of the blacklist file in FTP, FTPS, SFTP, or TFTP.

To export all blacklist library files, in the execution mode, use the following command:

export botnet-c2-prevention blacklist-lib to {{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} [**vrouter***vrouter-name*] *file-name*

- {**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] - Specifies the IP address and username and password of the account of the FTP/FTPS/SFTP server.
- **tftp server** *ip-address* - Specifies the IP address of the TFTP server.
- [**vrouter** *vrouter-name*] - Specifies the VRouter to which the FTP, FTPS, SFTP, or TFTP server belongs.
- *file-name* – Specifies the name of the blacklist library file to be imported.

To configure the **import mode**, **ip+file name (or URL)**, **virtual router**, **username and password** of auto update of the blacklist library, use the following command:

botnet-c2-prevention black-lib auto-update {**add** | **cover**} **from** {{ **ftp server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} [**vrouter***vrouter-name*] *file-name* | {**http** | **https**} [**vrouter***vrouter-name*] **url***url*}

- **add** | **cover**- Specifies the mode to update the blacklist library, in which **add** indicates incremental import and **cover** indicates overwrite import.
- **ftp server***ip-address* [**user***user-name***password***password*] - Specifies the IP address and username and password of the account of the FTP server.
- **tftp server***ip-address* - Specifies the IP address of the TFTP server.
- [**vrouter***vrouter-name*] - Specifies the VRouter to which the FTP or TFTP server belongs.
- *file-name* – Specifies the path of the blacklist file in FTP or TFTP.
- **http** | **https** - Specifies to update the blacklist library via the HTTP or HTTPS server.
- [**vrouter***vrouter-name*] - Specifies the VRouter to which the HTTP or HTTPS server belongs.
- **url***url* - Specifies the URL of the HTTP or HTTPS server. Valid values: 1 to 255 characters. The URL of the HTTP server needs to start with "http://" and the URL of the HTTPS server needs to start with "https://". The URL for the HTTP/HTTPS server needs to end with a file name suffix such as .csv, .json, .stix2, .ioc, or .xml. Example: http://192.1.1.1:8080/chf-s/shared/SERVER/ftp/test/score.csv.

To configure the frequency and time of auto update of the blacklist library, in the global configuration mode, use one of the following methods:

- To set the frequency to **Daily Update**, use the following command:
- **botnet-c2-prevention black-lib auto-update schedule daily** [*HH:MM*]
    - *HH:MM* - Specifies the the point in time. Valid values: 00:00 to 23:59.

- To set the frequency to **Weekly Update**, use the following command:
- **botnet-c2-prevention black-lib auto-update schedule weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} [*HH:MM*]
  - **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** - Specifies the the day of the week.
  - *HH:MM* - Specifies the the point in time. Valid values: 00:00 to 23:59.
- To set the frequency to **Custom Period Update**, use the following command:
- **botnet-c2-prevention black-lib auto-update schedule interval***<30-10080>*
  - **interval***<30-10080>* - Specifies the interval at which the blacklist library is updated. Valid values: 30 to 10080. Unit: minute.
- **Note**: Before configuring the frequency and time of auto update, you need to configure the import mode. Otherwise, the commands above do not take effect.



Notes:

- The manually imported or automatically updated blacklist library files support the following formats: CSV/STIX/OpenIOC. The file name extension can be .csv/.json/.stix2/.ioc/.xml.
- The size of manually imported or automatically updated blacklist library files varies based on the model of devices.
- The blacklist library files to be imported or automatically updated will be checked for redundancy in the order of import. If the format and content of the blacklist library file are valid, the import will be successful. The corresponding logs will display the total number of blacklist entries in the imported file, the actual number of imported blacklist entries, and the number of duplicate blacklist entries.



- When manually importing or automatically updating the blacklist library file, if the imported blacklist entries exceed the blacklist and whitelist capacity of botnet prevention of the device, the manual import will fail; In this case, the maximum number of entries that fit within the total blacklist and whitelist capacity of botnet prevention of the device, and the remaining blacklist entries will not be imported.
- SG-6000-A2200, SG-6000-A1800, and SG-6000-A1600 do not support the blacklist library.

To clear the auto update configuration of the blacklist library, in the global configuration mode, use the following command:

no botnet-c2-prevention black-lib auto-update

To clear the blacklist library file, in any configuration mode, use the following command:

clear botnet-c2-prevention blacklist lib

To view the auto update configuration of the blacklist library, in any configuration mode, use the following command:

show botnet-c2-prevention blacklist lib update

For example, to view the configuration of the blacklist library that is automatically updated from the FTP server:

SG-6000# **show botnet-c2-prevention blacklist lib update**

Botnet blacklist lib update:

server ip: 10.182.201.11（displays the IP address of the FTP server）

Vrouter: trust-vr（displays the VRouter to which the FTP server belongs）

update type: add（displays the import mode of auto update）

user: admin（displays the username used to log in to the FTP server）

password: 01010363dLnWw8ijZ3zWr+5f+Ymt9iq/Bb8=（displays the encrypted password, which is the password corresponding to the username used to the log in to the FTP server）

file: /test/123.xml（displays the path of the automatically updated blacklist library file on the

FTP server)

download mode ftp（displays that the blacklist library is updated from the FTP server)

schedule: daily 12:34（displays that the frequency of auto update is 12:34 every day)

To view the number and total capacity of custom whitelist, custom blacklist, and imported blacklist entries, in any configuration mode, use the following command:

show botnet-c2-prevention capacity

Example:

SG-6000# **show botnet-c2-prevention capacity**

Botnet whitelist and blacklist capacity:

total num: 7047/160000（displays the total number of custom blacklist and whitelist entries and the total capacity of the blacklist and whitelist entries of botnet prevention as of the current query time)

custom whitelist num: 3518（displays the number of custom whitelist entries)

custom blacklist num: 3518（displays the number of custom blacklist entries)

blacklist lib num: 11（displays the number of imported blacklist entries)

Configuring the Sinkhole IP address

You can select the system's predefined Sinkhole IP address or specify a user-defined Sinkhole IP address to replace the IP address in the DNS response message

To configure the Sinkhole IP address, in the global configuration mode, use the following command:

botnet-c2-prevention sinkhole {**ipv4***IPv4-address* | **ipv6***IPv6-address* | **predefined-sinkhole**}

- **ipv4***IPv4-address* - Specifies a custom IPv4 address. If only the IPv4 address is configured, the system will automatically map the configured IPv4 address to the corresponding IPv6 address when the DNS server communicates by using the IPv6 protocol.

- **ipv6***IPv6-address* - Specifies a custom IPv6 address.
- **predefined-sinkhole** -Specifies to use a predefined sinkhole IP address.

Binding a Botnet Prevention Profile to a Security Zone

If the botnet prevention profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a botnet prevention Profile, and the destination zone of the policy rule is also bound with a botnet prevention profile, then the botnet prevention profile bound to the policy rule will be valid, while the botnet prevention profile bound to the security zone will be void.

To bind the botnet prevention profile to a security zone, in the security zone configuration mode, use the following command:

botnet-c2-prevention enable *profile-name*

- *profile-name* – Specifies the name of the botnet prevention profile that will be bound to the security zone. One security zone can only be bound with one botnet prevention profile.

To cancel the binding, in the security zone configuration mode, use the following command:

no botnet-c2-prevention enable

Binding a Botnet Prevention Profile to a Policy Rule

If the botnet prevention profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the botnet prevention profile to a policy rule, in the policy rule configuration mode, use the following command:

botnet-c2-prevention *profile-name*

- *profile-name* – Specifies the name of the botnet prevention profile that will be bound to the policy rule.

To cancel the binding, in the policy rule configuration mode, use the following command: **no botnet-c2-prevention**

Viewing Botnet Prevention Profile Information

To view the botnet prevention profile information, in any mode, use the following command:

show botnet-c2-prevention-profile *profile-name*

Viewing Botnet Prevention Status

To view the botnet prevention status, in any mode, use the following command:

show botnet-c2-prevention status

Viewing Botnet Prevention Log Aggregation Configuration

To view the botnet prevention log aggregation configuration, in any mode, use the following command:

show botnet-c2-prevention log aggregation

Updating Botnet Prevention Signature Database

By default system updates the botnet prevention signature database everyday automatically. You can change the update configuration as needed. The configurations of updating botnet prevention signature database include:

- Configuring the botnet prevention signature update mode
- Configuring an Update Protocol
- Configuring an update server
- Specifying a HTTP Proxy Server
- Specifying an update schedule
- Updating now
- Importing a botnet prevention signature file

- Viewing botnet prevention signature information
- Viewing botnet prevention signature load status
- Viewing botnet prevention signature update information

Configuring the Botnet Prevention Signature Update Mode

System supports both manual and automatic update modes. To configure a botnet prevention signature update mode, in the global configuration mode, use the following command:

botnet-c2-prevention signature update mode {**auto** | **manual**}

- **auto** – Specifies the automatic botnet prevention signature update mode. This is the default mode.
- **manual** – Specifies the manual botnet prevention signature update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no botnet-c2-prevention signature update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

botnet-c2-prevention signature update protocol HTTP

In the global configuration mode, use the command **no botnet-c2-prevention signature update protocol HTTP** to restore the default value.

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest

botnet prevention signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

botnet-c2-prevention signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update the server, in the global configuration mode, use the following command:

no botnet-c2-prevention signature update {**server1** | **server2** | **server3**}

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the botnet prevention signature database updating, use the following command in the global configuration mode:

botnet-c2-prevention signature update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the **backup**parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the command **no botnet-c2-prevention signature update proxy-server** {**main** | **backup**}.

Specifying an Update Schedule

By default, system automatically updates the botnet prevention signature database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

botnet-c2-prevention signature update schedule { {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*] | **hourly** *MM* }

- **daily** – Updates the database every day.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Updates the database every week. Parameter **mon | tue | wed | thu | fri | sat | sun**is used to specify the specific date in a week.
- **monthly** *date* - Updates the database every month. Parameter *date* is used to specify the specific date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically upgraded this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.
- **hourly** *MM* – Updates the database every three hours. Minute is used to specify the specific minute in one hour.

Updating Now

For both manual and automatic update modes, you can update the botnet prevention signature database immediately as needed. To update the botnet prevention signature database now, in any mode, use the following command:

exec botnet-c2-prevention signature update

- **exec botnet-c2-prevention signature update** – Only updates the incremental part between the current botnet prevention signature database and the latest botnet prevention signature database released by the update server.

Importing a Botnet Prevention Signature File

In some cases, your device may be unable to connect to the update server to update the botnet prevention signature database. To solve this problem, system provides the botnet prevention signature file import function, i.e., importing the botnet prevention signature files to the device from an FTP, TFTP server or USB disk, so that the device can update the botnet prevention signature database locally. To import the botnet prevention signature file, in the execution mode, use the following command:

import botnet-c2-prevention signature from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1** } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the botnet prevention signature file that be imported.

Viewing Botnet Prevention Signature Information

To view botnet prevention signature database information, in any mode, use the following command:

show botnet-c2-prevention signature info

Viewing Botnet Prevention Signature Load Status

To view botnet prevention signature load status, in any mode, use the following command:

show botnet-c2-prevention load-status

Viewing Botnet Prevention Signature Update Information

You can view the botnet prevention signature update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the botnet prevention signature database update. To view the botnet prevention signature update information, in any mode, use the following command:

show botnet-c2-prevention signature update

Encrypted Traffic Detection

Traffic processed by using encryption technology is called encrypted traffic. Malicious traffic is typically hidden by using SSL/TLS encryption protocols, which is difficult to detect and can pose great threats to network security. After you configure the Encrypted Traffic Detection function, the system extracts feature data from encrypted traffic and detects the data based on the detection model in the encrypted traffic detection database. If abnormal encrypted traffic is detected, the system records threat logs.

The system supports daily automatic update of the encrypted traffic detection database or you can manually update the database in real time.

Encrypted Traffic Detection Configurations

The encrypted traffic detection configurations of devices include the following parts:

- Enabling/Disabling the Encrypted Traffic Detection Function
- Configuring the IP Whitelist of Encrypted Traffic Detection



Notes:

- The Encrypted Traffic Detection function is supported for A-series (except A200/A6800/A7600) devices, CloudEdge, K2380, and K2680.



- If you are using the Encrypted Traffic Detection function for the first time, you need to update the encrypted traffic detection database. For more information, see Updating Encrypted Traffic Detection Database. To ensure that the connection to the default update server succeeds, configure a DNS server for the device before the update.

Enabling/Disabling the Encrypted Traffic Detection Function

To enable or disable the Encrypted Traffic Detection function, you need to enter the encrypted traffic detection configuration mode. To do this, use the following command in global mode:

encrypted-traffic-detection

To enable the Encrypted Traffic Detection function, use the following command in encrypted traffic detection configuration mode:

enable

To disable the Encrypted Traffic Detection function, use the **disable** command in encrypted traffic detection configuration mode.

Configuring the IP Whitelist of Encrypted Traffic Detection

After the Encrypted Traffic Detection function is enabled, all traffic are detected by the function. However, in practice, if you do not want traffic sent by specific hosts to be detected, you can add addresses or address ranges (source address or destination address) to the IP whitelist of the encrypted traffic detection. The IP whitelist supports IPv4 and IPv6 addresses. An IP address or CIDR block in the whitelist are not detected by the Encrypted Traffic Detection function.

To configure the IP whitelist, use the following command in encrypted traffic detection configuration mode:

whitelist [**id***id*] {**source-ip** | **destination-ip**} {*IPv4-address/M* | *IPv6-address/prefix* }

- **id** – Specifies the ID of the whitelist. Valid values: 1 to 64. If not specified, an ID is automatically assigned.
- **source-ip** | **destination-ip** – Specifies the type of addresses added to the whitelist, which can be **source-ip** or **destination-ip**.
- *IPv4-address/M* – Specifies the IPv4 address and subnet mask added to the whitelist rule.
- *IPv6-address/prefix* – Specifies the IPv6 address and prefix length added to the whitelist rule. Valid values of the prefix length: 120 to 128.

To delete a specified whitelist rule, use the **nowhitelist** [**id***id*] command.

Updating Encrypted Traffic Detection Database

By default, the system automatically updates the encrypted traffic detection database everyday. You can change the encrypted traffic detection database configuration as needed. The configurations of updating the encrypted traffic detection database include:

- Configuring an Encrypted Traffic Detection Database Update Mode
- Configuring an Update Protocol
- Configure an Update Server
- Specifying an HTTP Proxy Server
- Specifying an Update Schedule
- Updating Now
- Importing an Encrypted Traffic Signature File
- Viewing Encrypted Traffic Detection Database Information
- Viewing Encrypted Traffic Detection Database Update Information

Configuring an Encrypted Traffic Detection Database Update Mode

Both manual and automatic update modes are supported. To configure an encrypted traffic detection database update mode, use the following command in global configuration mode:

etd update mode {**auto** | **manual**}

- **auto** – Specifies to automatically update the encrypted traffic detection database. This is the default update mode.
- **manual** – Specifies to manually update the encrypted traffic detection database.

To restore to the default mode, use the following command in the global configuration mode:

no etd update mode

Configuring an Update Protocol

You can update the signature database over HTTP or HTTPS, and the default protocol is HTTPS. To set the update protocol to HTTP, use the following command in global configuration mode:

etd update protocol HTTP

To restore to the default update protocol, use the command in global configuration mode:

no etd update protocol HTTP

Configure an Update Server

The system provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers as needed. To configure an update server, use the following command in the global configuration mode:

etd update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is

update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.

To cancel a specified update server, use the following command in the global configuration mode:

no etd update {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device accesses the Internet by using an HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature databases can update automatically and normally.

To specify the HTTP proxy server for the encrypted traffic detection database update, use the following command in global configuration mode:

etd update proxy-server {**main** | **backup**} *ip-addressport-number*

- **main** | **backup** – Uses the main field to set the HTTP proxy server to the main proxy server and uses the backup field to set the HTTP proxy server to the backup proxy server.
- *ip-addressport-number* – Specifies the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no etd update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, the system automatically updates the encrypted traffic detection database every day. To reduce the workload of the update server, the time of daily update is random. To specify the schedule and time for the update, use the following command in global configuration mode:

etd update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. The field **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**is used to specify a date in a week.
- **monthly** *date* - Updates the database every month. The field *date* is used to specify a date in a month., the range is 1 to 31. If a month does not contain the specified date (eg, there is no 30th in February), the database will not be automatically updated in this month.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the encrypted traffic detection database immediately as needed. To update the encrypted traffic detection database now, use the following command in any mode:

exec etd signature update

Importing an Encrypted Traffic Signature File

In some cases, your device may be unable to connect to the update server to update the encrypted traffic signature database. To avoid this issue, the system provides the encrypted traffic signature file import function, i.e., importing the encrypted traffic signature files to the device from an FTP, FTPS, SFTP, or TFTP server, so that the device can update the encrypted traffic signature database locally. To import an encrypted traffic signature file, use the following command in execution mode:

import etd signature from {{**ftp server** | **ftps server** | **sftp server**} *ip-address* [**user** *user-name***password** *password*] | **tftp server** *ip-address* } [**vrouter***vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP, FTPS, SFTP, or TFTP server.
- **user***user-name***password** *password* – Specifies the username and password of the FTP, FTPS, or SFTP server.

- **vrouter***vr-name* – Specifies the VRouter to which the FTP, FTPS, SFTP, or TFTP server belongs.
- *file-name* – Specifies the name of the encrypted traffic signature file to be imported.

Viewing Encrypted Traffic Detection Database Information

You can view the encrypted traffic detection database information of the device as needed, including the encrypted traffic detection database version and release date. To view AV signature database information, use the following command in any mode:

show etd signature info

Viewing Encrypted Traffic Detection Database Update Information

You can view the encrypted traffic detection database update information of the device as needed, including the update server , update mode, and update frequency and time of the encrypted traffic detection database update. To view the encrypted traffic detection database update information, use the following command in any mode:

show etd signature update

Antispam

Overview

The system is designed with an Antispam function, which enables user to identify and filter mails transmitted by SMTP and POP3 protocol through the cloud server, timely discover the mail threats, such as spam, phishing and worm mail, and then process the found spam according to the configuration, so as to protect the user's mail client or mail server.

The Antispam function will not work unless an antispam license has been installed on a system that supports Antispam.



Notes:

- SG-6000-A200 and SG-6000-A200W do not support Antispam function.
- To assure a proper connection to the cloud server, you need to configure a DNS server for system before configuring the Antispam.

Configuring Antispam

The Antispam configurations are based on security zones or policies.

To configure antispam via CLI, take the following steps:

1. Create an Antispam profile, and specify the mail protocol, spam category, action and black-list /whitelist of sender in the profile.
2. Bind the Antispam profile to a security zone or policy rule.

Creating an Antispam Profile

You need to specify the mail protocol, spam category, action and exempt domain of sender of the Antispam profile. To create an Antispam profile, in the global configuration mode, use the following command:

antispam-profile *antispam-profile-name*

- *antispam-profile-name* - Specifies the name of the Antispam profile, and enter the configuration mode of the Antispam profile. If the specified name exists, the system will directly enter the Antispam profile configuration mode. Up to 32 new Antispam profile can be created.

To delete the specified Antispam profile, in the global configuration mode, use the command**no antispam-profile** *antispam-profile-name*.

Specifying a Mail Protocol Type

To specify a protocol type and enter the protocol configuration mode, in the Antispam profile configuration mode, use the following command:

protocol {pop3 | smtp}

- **pop3** – Scans the Emails transferred over POP3.
- **smtp** – Scans the Emails transferred over SMTP.

To cancel the specified protocol type, in the Antispam profile configuration mode, use the following command:

no protocol{ pop3 | smtp }

Specifying the Spam Category

To specify the spam category and action, in the protocol configuration mode, use the following command:

spam-class {bulk | confirmed | suspected | validbulk} action { log-only | reset }

- **bulk** – Specifies the action for the bulk spam.
- **confirmed** – Specifies the action for the confirmed spam.
- **suspected** – Specifies the action for the suspected spam.
- **validbulk** – Specifies the action for the valid bulk mails.

- **action** { **log-only** | **reset** } – Specifies the action for the spam.
- **log-only** – Generates logs. This is the default action. The spams transferred over POP3 only supports generate logs action.
- **reset** – Resets the connection if any spams has been detected.

To cancel the specified spam category, in the protocol configuration mode, use the following command:

no spam-class {**bulk** | **confirmed** | **suspected** | **validbulk**}

Specifying the Whitelist of Sender

The whitelist of sender is used to specify the mail domains or email that will not be filtered by antispam. Each antispam profile can specify up to 16 exempt domains of sender.

To specify the whitelist of sender, in the Antispam profile configuration mode, use the following command:

sender-whitelist {**domain** *domain-name* | **mailbox** *email-address* }

- *domain-name* – Specifies the domain name. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.
- *email-address* - Specifies the demail address. The length is 1 to 255 characters.

To delete the specified whitelist of sender, in the Antispam profile configuration mode, use the following command:

no sender-whitelist {**domain** *domain-name* | **mailbox** *email-address*}

User-defined Blacklist Spam

You can add the sender's domain name or email address to the User-defined Blacklist. When Anti-Spam User-defined Blacklist function is enabled, system will directly identify the email from the User-defined Blacklist as spam, and reset the link or record to the threat log.

Enabling/Disabling User-defined Blacklist

To enable or disable user-defined blacklist spam, in the Antispam profile configuration mode, use the following command:

- Enable: **user-defined-blacklist enable**
- Disable: **no user-defined-blacklist enable**

Adding/Deleting User-defined Blacklist

To add the user-defined blacklist spam, in the Antispam profile configuration mode, use the following command:

exec antispam user-defined-blacklist add {**domain** *domain-name* | **mailbox** *email-address*}

To delete the user-defined blacklist spam, in the Antispam profile configuration mode, use the following command:

exec antispam user-defined-blacklist delete {**domain** *domain-name* | **mailbox** *email-address*}

- *domain-name* – Specifies the domain name. The length is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters.
- *email-address* - Specifies the demail address. The length is 1 to 255 characters.

Binding an Antispam Profile to a Security Zone

If the Antispam profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with an antispam Profile, and the destination zone of the policy rule is also bound with an Antispam profile, then the Antispam profile bound to the policy rule will be valid, while the Antispam profile bound to the security zone will be void.

To bind the Antispam profile to a security zone, in the security zone configuration mode, use the following command:

antispam *antispam-profile-name*

- *antispam-profile-name* – Specifies the name of the Antispam profile that will be bound to the security zone. One security zone can only be bound with one Anti-Spam profile.

To cancel the binding, in the security zone configuration mode, use the following command:

no antispam

Binding an Antispam Profile to a Policy Rule

If the Antispam profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the Antispam profile to a policy rule, in the policy rule configuration mode, use the following command:

antispam *antispam-profile-name*

- *antispam-profile-name* – Specifies the name of the Antispam profile that will be bound to the policy rule.

To cancel the binding, in the policy rule configuration mode, use the following command:*no anti-spam*

Configuring the Mail Scan Maximum Limit

To configure the mail scan maximum limit, in the global configuration mode, use the following command:

antispam max-mail-size *max-mail-size-value*

- *max-mail-size-value* – Specifies the mail scan maximum limit. The range is 512 Kb to 2048 Kb, the default value is 1024 Kb.

To restore to the default value, in the global configuration mode, use the following command:**no antispam** *max-mail-size*

Viewing Antispam Profile Information

To view the Antispam profile information, in any mode, use the following command:

show antispam-profile [*antispam-profile-name*]

- *antispam-profile-name* – Shows the specified antispam profile information. If this parameter is not specified, the command will show the information of all the Anti-Spam profiles.

Viewing the Antispam Status Information

To view the Antispam status information, in any mode, use the following command:

show antispam status

Viewing the Global Configuration

To view the global configuration of Antispam, in any mode, use the following command:

show antispam configuration

End Point Protection

The endpoint security control center is used to monitor the security status of each access endpoint and the system information of the endpoint.

When the end point protection function is enabled, the device can obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.



Notes:

- At present, end point protection function only supports linkage with "JIANGMIN" endpoint security control center.
- End point protection is controlled by license. To use end point protection, apply and install the EPP license.

Configuring the End Point Protection

Preparation for Configuring End Point Protection

Before enabling end point protection, make the following preparations:

1. Make sure your system version supports end point protection.
2. Import an EPP license and reboot.

Configuring End Point Protection

To configure the end point protection function, take the following steps:

1. Enable the end point protection function.
2. Define an end point protection profile, and specify the protection action corresponding to the endpoint status in the profile.
3. Bind the end point protection profile to an appropriate policy rule or security zone.

Configuring Endpoint Security Control Center Parameters

The configurations of endpoint security control center include:

- Specifying the Name of the Endpoint Security Control Center Server
- Specifying the Address of the Endpoint Security Control Center Server
- Specifying the Port of the Endpoint Security Control Center Server
- Specifying the Synchronization Period

Specifying the Name of the Endpoint Security Control Center Server

To specify the name of endpoint security control center server and enters the endpoint security control center server configuration mode, in the global configuration mode, use the following

command:

epp server*server-name*

- *server -name* - Specifies the the name of endpoint security control center server and enters the endpoint security control center server configuration mode. If the specified name exists, then the system will directly enter the endpoint security control center server configuration mode. System only allows 1 endpoint security control center server to be configured.

To delete the specified endpoint security control center server, in the global configuration mode, use the command **no epp server**.

Specifying the Address of the Endpoint Security Control Center Server

To specify the address of the endpoint security control center server, in the endpoint security control center server configuration mode, use the following command:

host*hostname*

- *hostname* - Specifies the address or domain name of the endpoint security control center server. The range is 1 to 255 characters.

To delete the specified address, in the endpoint security control center server configuration mode, use the command **no host**.

Specifying the Port of the Endpoint Security Control Center Server

To specify the the port of the endpoint security control center server, in the endpoint security control center server configuration mode, use the following command:

port*port-number*

- *port-number* - Specifies the port number. The range is 1 to 65535.

To delete the specified port number, in the endpoint security control center server configuration mode, use the command **no port**.

Specifying the Synchronization Period

To specify the synchronization period of endpoint data information, in the endpoint security control center server configuration mode, use the following command:

sync*sync-cycle*

- *sync-cycle* - Specifies the synchronization period. The range is 1 to 60 minutes. The default value is 10 minutes.

To restore the default value, in the endpoint security control center server configuration mode, use the command **no sync**.

Enabling/Disabling the Timeout Entry

By default, when the endpoint security control center is disconnected, the endpoint data information that the system has synchronized will be invalid, and the synchronized endpoint data information will be cleared. To enable/disable the timeout entry, in the global configuration mode, use the following command:

- Enable: **epp timeout-used**
- Disable: **no epp timeout-used**

Creating an End Point Protection Profile

The end point protection profile specifies the the protection action corresponding to the endpoint status. To create an end point protection profile, in the global configuration mode, use the following command:

epp-profile*profile-name*

- *profile-name* - Specifies the end point protection profile name and enters the end point protection profile configuration mode. If the specified name exists, then the system will directly enter the end point protection profile configuration mode.

To delete the specified end point protection profile, in the global configuration mode, use the command **no epp-profile***profile-name*.

Specifying the Protection Action

To specify the protection action for the endpoint which doesn't install an anti-virus client. In the end point protection profile configuration mode, use the following command:

status uninstall { **log-only** | **redirect***url* | **block** [*block-interval*]}

- **log-only** – System will pass traffic and record logs only.
- **redirect***url* – Redirects the endpoint to the specified *url*.
- **block** [*block-interval*] – Block the endpoint connection, and specifies the block interval *block-interval*.

To cancel the protection action for the endpoint which doesn't install an anti-virus client, in the end point protection profile configuration configuration mode, use the following command:

no status uninstall

Specifies the protection action for the unhealthy endpoint, infected endpoint and abnormal end-point. In the end point protection profile configuration mode, use the following command:

status { **unhealthy** | **infected** | **abnormal** } { **log-only** | **block** [*block-interval*]}

- **unhealthy** – Specifies the protection action for the unhealthy endpoint.
- **infected** – Specifies the protection action for the infected endpoint.
- **abnormal** – Specifies the protection action for the abnormal endpoint.
- **log-only** – System will pass traffic and record logs only.
- **block** [*block-interval*] – Block the endpoint connection, and specifies the block interval *block-interval*. The value range is 60 to 65535 seconds. The default value is 60.

To cancel the protection action for the unhealthy endpoint, infected endpoint and abnormal end-point, in the end point protection profile configuration configuration mode, use the following command:

no status { **unhealthy** | **infected** | **abnormal** }

Specifying the Exception Address

The exception address is not controlled by the end point protection rule. To specify the exception address, in the end point protection profile configuration configuration mode, use the following command:

address*address-name*

- *address-name* - Specifies the address book name.

To cancel the specified exception address, in the end point protection profile configuration configuration mode, use the following command:

no address



Notes: Before selecting the exception address, you need to add the exception end-point address to the address book. For configuration, see **Configuring an Address Book**.

Binding an End Point Protection Profile to a Security Zone

If the end point protection profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration.

To bind the end point protection profile to a security zone, in the security zone configuration mode, use the following command:

epp enable*profile-name*

- *profile-name* – Specifies the name of the end point protection profile that will be bound to the security zone. One security zone can only be bound with one end point protection profile.

To cancel the binding, in the security zone configuration mode, use the following command:

no epp enable

Binding an End Point Protection Profile to a Policy Rule

If the end point protection profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration. To bind the end point protection profile to a policy rule, in the policy rule configuration mode, use the following command:

epp*profile-name*

- *profile-name* – Specifies the name of the end point protection profile that will be bound to the policy rule.

To cancel the binding, in the policy rule configuration mode, use the following command: **no epp**.

Manually Synchronizing the Endpoint Data Information

To synchronize the endpoint data information manually, in any mode, use the following command:

exec epp server-flush

Viewing End Point Protection Profile Information

To view the end point protection profile information, in any mode, use the following command:

show epp-profile [*profile-name*]

Viewing the End Point Status

To view the end point status, in any mode, use the following command:

show epp ep-status

Viewing the End Point Information Synchronization Status

To view the synchronization status of endpoint, in any mode, use the following command:

show epp sync-status

Viewing the Endpoint Security Control Center Information

To view the endpoint security control center information:

show epp server

IoT Monitor

The Internet of Things (IoT) refers to the billions of physical devices around the world that are now connected to the internet through information sensing devices, all collecting and sharing data for intelligent identification and management. The IoT technology is widely applied in large and medium-sized enterprises. Typically, in the IoT networks of these enterprises, there are various types of IoT devices, including video surveillance devices, access control systems, time attendance machines, facial recognition systems, office computers, televisions, IP phones, and more. However, with the increasing number of internal IoT devices within enterprises, it brings a series of security concerns such as devices being attacked by threats, controlled by botnets, and data leakage.

The system provides the overall IoT monitor function, which can implement the identification, security control, and threat management of IoT devices within the enterprise, and can protect devices from attacks and safeguard data privacy.

The IoT monitor function consists of the following four parts:

- **IoT Asset Identification**: The system supports two methods for identifying various types of IoT devices within the network: deploying the asset identification system in the Docker environment of the device, deploying the asset identification system in the virtual machine.
- **IoT Asset Management**: Monitor identified IoT devices in real time, combined with statistical analysis of the IoT devices. In addition, the system can manage assets in a unified manner.
- **IoT Policy Control**: Support to configure policy rules based on IoT devices. By analyzing the traffic flowing through the device, the system automatically maps the IP address to the IoT device object based on the attributes of the IoT device. This allows security policies automatically and dynamically manage and control the network permissions of the IoT device.
- **IoT Threat Management**: Combined with the threat protection function, endpoint protection function, and data security function in the system, IoT devices detected with security threats can be correspondingly governed.



Notes:

- The IoT montior function can identify IoT devices from the following manufacturers: Hikvision, Dahua, Uniview, Greenwill, Vivotek, Lenovo, Tiandy, Honeywell, Viewpointec, JSCT, Johnson Controls, Canon, HP, Epson, Samsung, Xiaomi, Huawei, JVC Kenwood, Netgear, Apple, Walkera, Foxconn, Schneider Electric, and Hillstone Networks.
- The IoT monitor function is controlled by license. In other words, this function is available only after the IoT license is installed for devices that support the IoT monitor function.
- The IoT monitor function cannot be used to identify IoT devices in a NAT scenario.
- In deployment environments that use the IoT monitor function, DHCP traffic from IoT devices needs to pass through the firewall or mirror the traffic to the firewall.

Typical Deployment Scenario

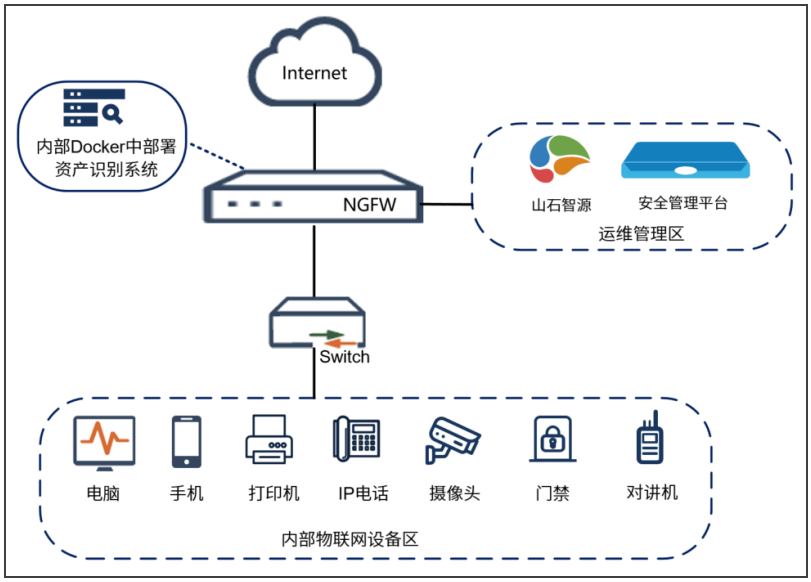
The typical deployment method of IoT monitor includes:

- **Local Asset Identification**: Identify information about IoT device assets based on the local asset identification module., which is divided into the following two types:
  - Built-in: Use the Docker management function of the system to deploy the asset identification system within the firewall.
  - External: Install the asset identification program on the virtual machine and use the asset identification system deployed on the virtual machine.

Notes: The built-in type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

Built-in Asset Identification

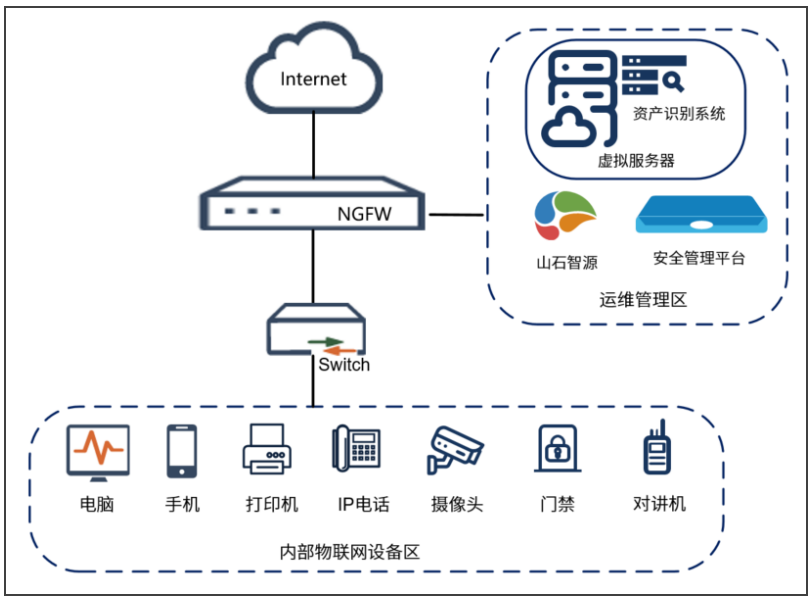
As shown in the figure below, the internal IoT of the enterprise contains various types of IoT devices, such as video surveillance devices, access control systems, office computers, IP phones, mobile phones, and walkie-talkies. A firewall (NGFW) is deployed in the enterprise, and the asset identification system is deployed into the system by using the Docker management function of the firewall to identify IoT device asset information, which is used in conjunction with the IoT monitor function of the firewall to implement security control. Meanwhile, HSM and iSource are deployed to upload IoT asset data for further security control and threat governance.



External Asset Identification

As shown in the figure below, the internal IoT of the enterprise contains various types of IoT devices, such as video surveillance devices, access control systems, office computers, IP phones, mobile phones, and walkie-talkies. A firewall (NGFW) is deployed in the enterprise, and the asset identification system is installed and deployed on the virtual server to identify IoT device asset

information, which is used in conjunction with the IoT monitor function of the firewall to implement security control. Meanwhile, HSM and iSource are deployed to upload IoT asset data for further security control and threat governance.



Configuration Procedure of IoT Monitor Function

To use the IoT monitor function, you need to configure the following:

1. Select an IoT asset identification type:

    a. **Local asset identification:**

    Note: The built-in type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

        1. Configure Docker——Deploy the asset identification system into the device system
        2. Enable the local asset identification function
        3. Configure the local asset identification function

b. **Local asset identification——External Docker:**

- Deploy the asset identification system on the virtual machine

2. **IoT Asset Identification**

a. Configuring the identification list——Specify the address list of IoT asset devices that you want to identify.

b. Configuring the zone——Enable the IoT Monitor function within a zone and bind the identification list.

3. **IoT Monitor Management**

a. Configuring the region——Add the regionof the corresponding region for IoT devices.

b. Viewing IoT monitor——View the manufacturer, type, online devices, and various detailed statistics of all identified IoT devices.

c. Viewing IoT logs.

4. **IoT Policy Control**

a. Configuring the device object——Specify classification dimensions for IoT devices, such as manufacturer, type, device model, operating system, etc. The system will then map the identified IoT device information to corresponding device objects.

b. Configuring the policy rule——Configure the policy rule based on device objects.

5. **IoT Threat Governance**

a. Combined with the threat protection function, endpoint protection function, and data security function, IoT devices detected with security threats can be correspondingly governed.

b. Uploading IoT data to iSource——You can implement further threat event response and handling such as asset management and policy/blocking deployment by using iSoutce.

c. Uploading IoT data to the Hillstone cloud platform——Upload IoT report data and asset data to the cloud platform for unified analysis, statistics, and management.

Notes: The IoT monitor function is controlled by license. Make sure that the current device supports the IoT monitor function and is installed with the IoT license.

Deploying the Asset Identification System on the Virtual Machine

When you use the external local asset identification type, you can deploy the asset identification system on the virtual machine.

This topic describes how to deploy the asset identification system in different environments, including VMware and OpenStack. Before the deployment, you need to be familar with VMware and OpenStack.

- Deploying the asset identification system on VMware ESXi
- Deploying the asset identification system on OpenStack

Deploying the Asset Identification System on VMware ESXi

You can deploy the asset identification system on an X86 device that supports the VMware ESXi virtual machine by importing the OVF+VMDK file. After the deployment is completed, you can automatically update the identification engine version by using Update Server.

Before You Start

Before you deploy the asset identification system on the VMware ESXi server, make sure:

- You are familiar with the vSphere Hypervisor structure, ESXi host settings, and virtual machine deployment of VMware.

- Prepare the virtual machine environment based on the system requirements and limits and set up the ESXi Server host.
- Contact the customer service personnel of Hillstone to obtain the installation file (in the ZIP format) that contains ovf, vmdk, iso and mf files, unzip it, and save the ovf and vmdk files to your PC.

System Requirements and Limits

To deploy the asset identification system on VMware ESXi, the VMware ESXi server needs to be:

- VMware ESXi 7.0 or later.
- Requires at least 4 vCPU, 4GB memory, 20 GB disk space, and NIC is installed.

Procedure

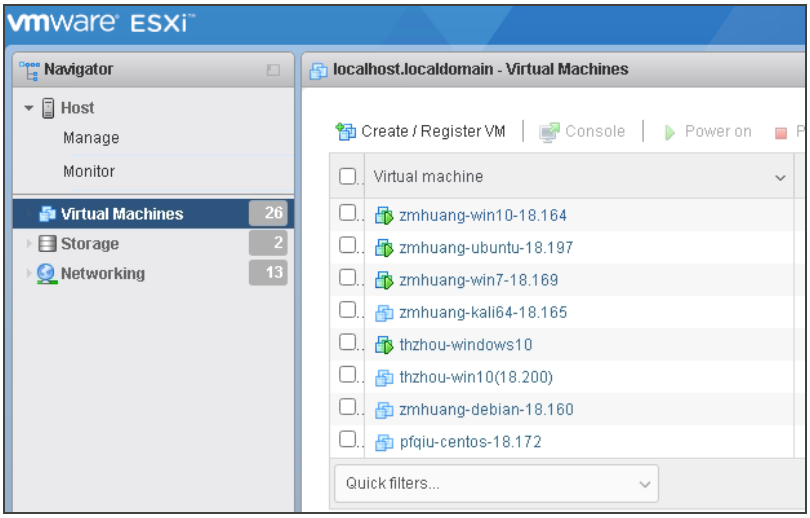
In the following example, VMware ESXi 7.0 is used.

Step 1: Log in to VMware ESXi

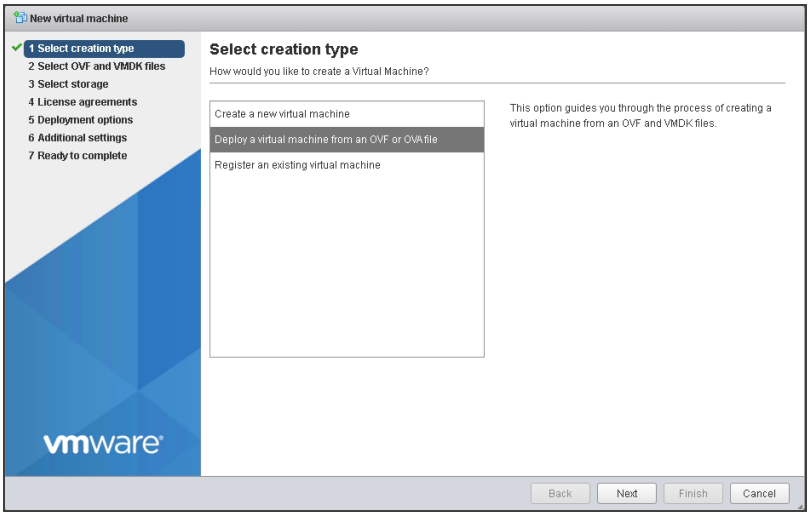
To access VMware ESXi 7.0, enter the username and password and click Login.

Step 2: Create a VM

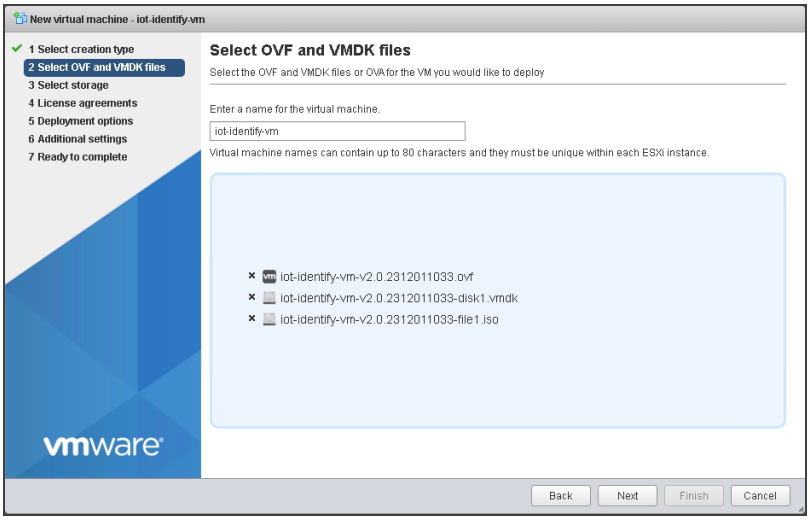
1. After you log in to VMware ESXi 7.0, click **Virtual Machines** in the left-side navigation pane. On the page that appears, click **Create/Register VM**.



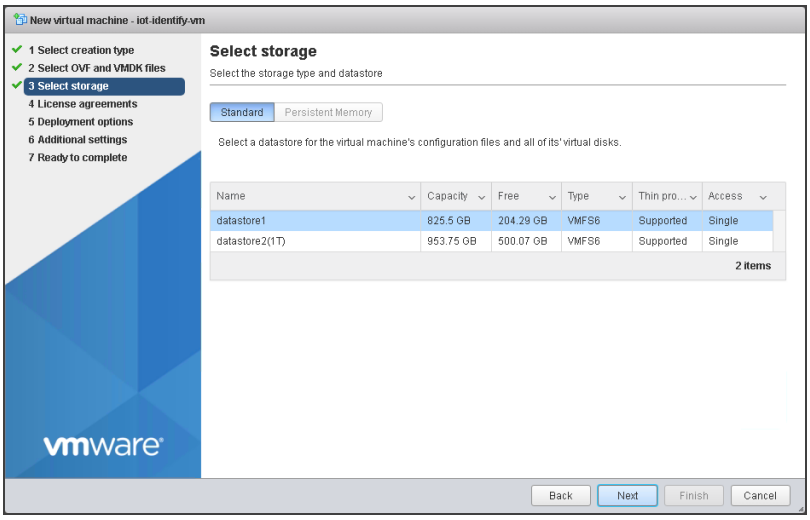
2. In the **New virtual machine** dialog box, select **1 Select creation type** > **Deploy a virtual machine from an OVF file**, and click **Next**.



3. Enter a name for the VM, and click the upload section to select the OVF and VMDK files or drag the file to the upload section. Then, click **Next**.

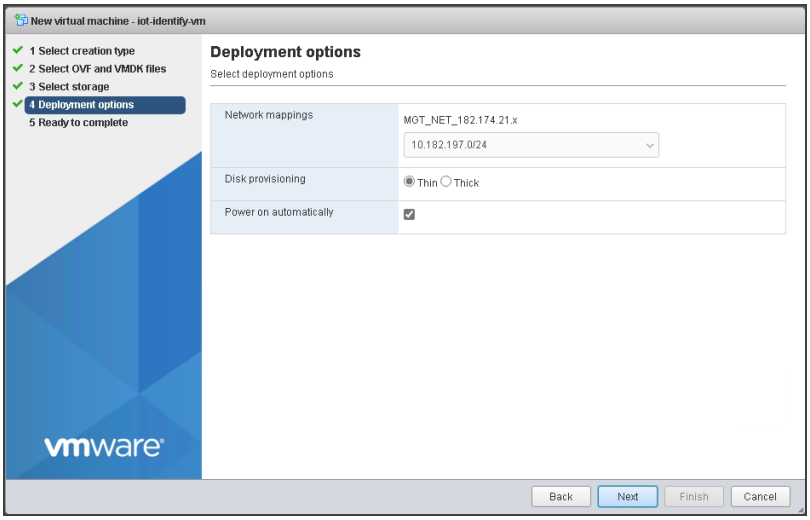


4. Select a storage type and datastore and click **Next**.



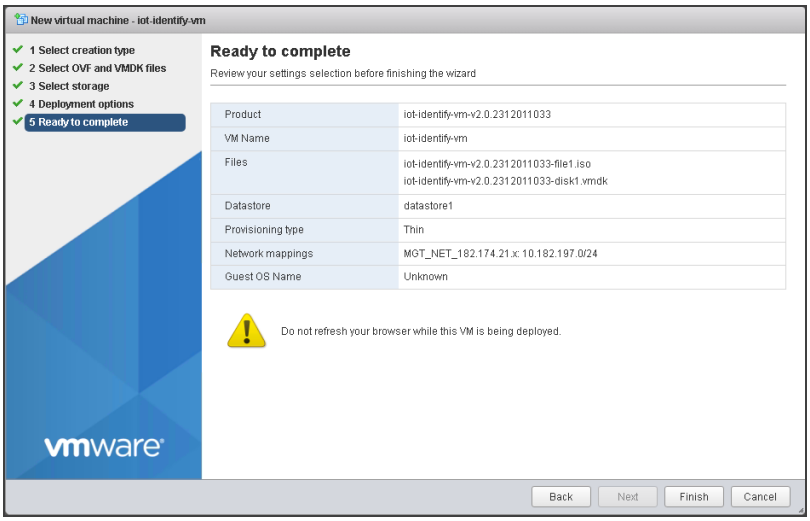
Note: The hard disk needs to be at least 20 GB in size.

5. Select deployment options. Set the **Network mappings** parameter based on your network environment and set the **Disk provisioning** parameter to **Thin**. Then, click **Next**.



Note: "Thick device" consumes more disk space.

6. After you check that the configurations are correct, click **Finish**. You can ignore error messages.



7. After the system files are uploaded to the disk, the VM is created.

Notes: The procedure may take a long time. Please do not refresh the page and wait until the deployment is completed.

Step 3: Log in to the virtual machine

1. After the virtual machine is created, it is automatically powered on and started.
2. In the left-side Navigator, click Virtual Machine and then select the virtual machine created in Step 2.
3. Select **Console** > **Open browser console** or click the console thumbnail to open the console.
4. Enter the default username and password (hillstone/hillstone) to lo in to the virtual machine.

Step 4: Configure NIC

After the virtual machine is deployed, you need to configure the configuration file within /etc/netplan to modify the NIC configuration based on the current environment.

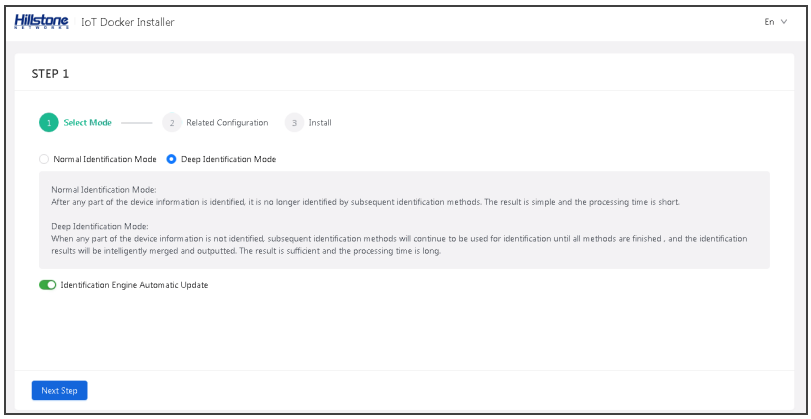
1. In the console, run the **cat /etc/netplan/00-installer-config.yaml** command to view the current configuration file.
2. Run the **vi /etc/netplan/00-installer-config.yaml** to open the configuration file.
3. Move the cursor to the position where you want to modify and press **i** to enter the editing mode. You can modify the IP address, gateway address, or configure DHCP.
   Note: The IP address needs to be accessible by the firewall and the browser of the PC on which the asset identification system is installed. This IP address is used as that of the IoT local asset identification virtual machine. (In this example, 10.182.197.172 is used)
4. Press "ESC" and then **:wq** to exit the configuration file and save the configuration.
5. Restart the virtual machine to ensure the modified NIC information.

Step 5: Install the asset identification program

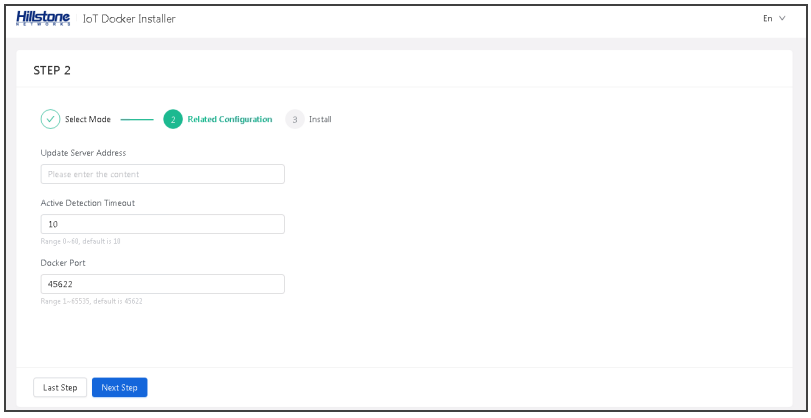
1. Open the browser and access the IP address configured in Step 4. Example: https://10.182.197.172:22654

2. Due to the use of a self-signed certificate, the browser displays a warning: 'Your connection is not private'. Click **Advanced** > **Proceed** to continue accessing the site.

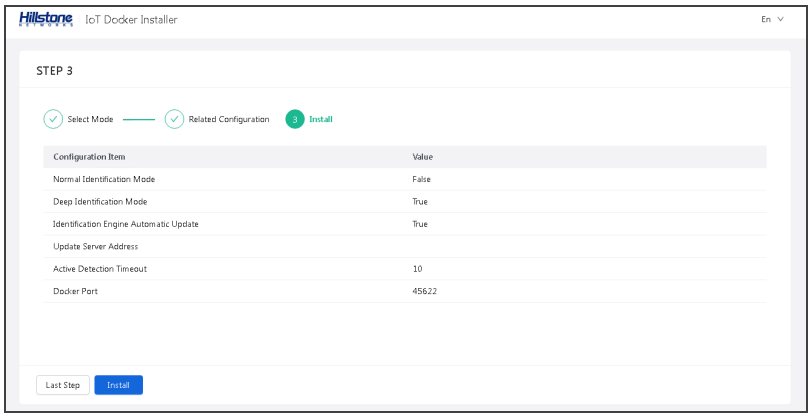
3. Enter the asset identification program installation guide. Select an identification mode and click **Next**. By default, **Deep Identification Mode** is selected and **Identification Engine Automatic Update** is enabled.



4. In the **Related Configuration** step, configure the Update Server address, active detection timeout, and Docker port number. If you use the default configuration, Update Server provided by Hillstone Networks is used.



5. Confirm the configuration and click **Install**.



6. After the installation is completed, the asset identification program is automatically started.

At this point, the asset identification system is deployed on VMware ESXi.

Deploying the Asset Identification System on Openstack

Before You Start

Before you deploy the asset identification system on Openstack, make sure:

- Prepare the host environment based on the system requirements.
- Contact the customer service personnel of Hillstone to obtain the image file of the asset identification system in qcow2 format and store the file to your PC.

System Requirements

To deploy the asset identification system on an OpenStack platform, the following requirements need to be met:

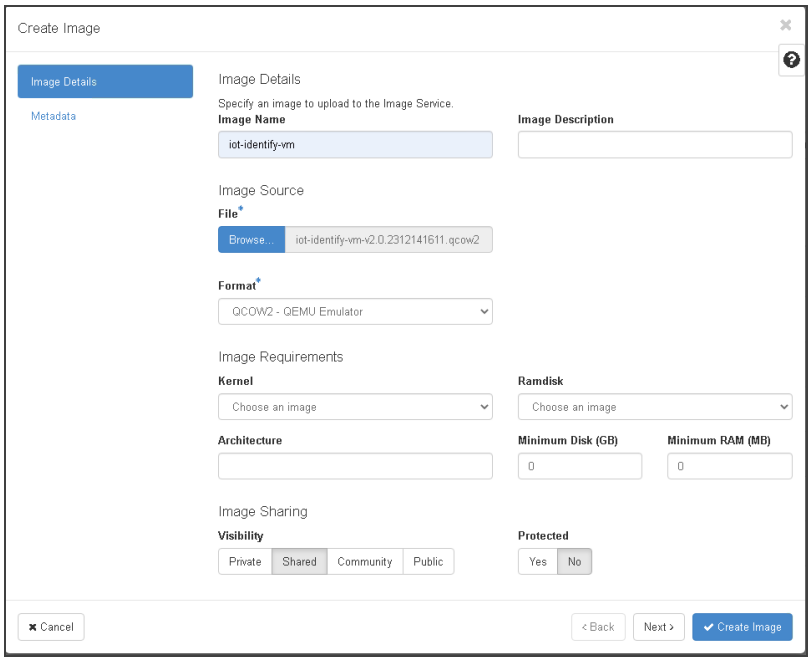
- Requires at least 4 CPU and 4 GB memory.
- Openstack and its components Horizon, Nova, Neutron, Glance, and Cinder are installed. (For more information about how to install Openstack, see http://-docs.Openstack.org/icehouse/install-guide/install/apt/content/)

Procedure

Step 1: Import the Image File

1. Log in to the OpenStack WebUI with a normal account, and select **Project** > **Compute**> **Images**.

2. Click **Create Image** on the top right corner.



3. In the <Create Image> dialog, configure following options.

Option	Description
Image Name	Enter the name of the image, such as "iot-identity-vm".
File	Click **Browse**, and select the image file in the qcow2 format from the local PC.
Format	Select **QCOW2-QEMUEmulator** from the **Format** drop-down list.

4. Keep other information as default.

5. Click **Create Image**.

6. Wait a few moments, it takes about 10 minutes. The image file will be imported successfully and displayed in the list.

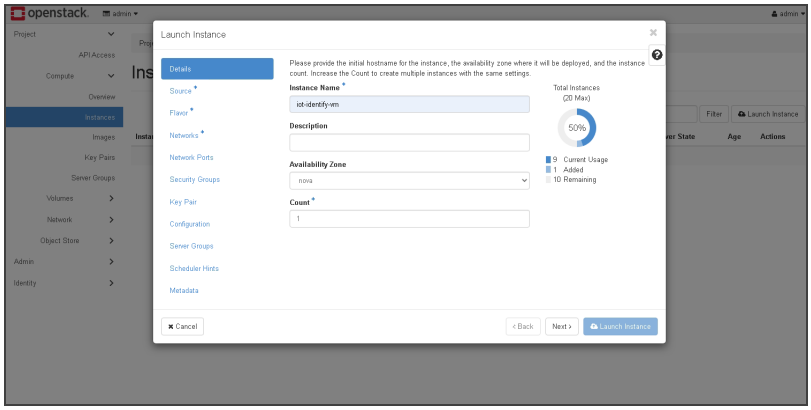
Step 2: Create a Flavor

Normally, a non-admin user cannot change the properties of an instance, including core, and memory. If you want to change an instance, you can change the flavor it belongs to, since the instance inherits what its flavor has.

To create a flavor, take the following steps:

1. Log in to OpenStack WebUI with the admin account.

2. Select **Admin**> **System**> **Flavors**, and click **Create Flavor** on the top right corner.



3. In the <Create Flavor> dialog, configure the flavor.

Option	Description
Name	Enter the flavor name, such as "iot.normal".
ID	Skip this step since ID is automatically generated by OpenStack.
VCPUs	Specify the number of CPU cores. "4" is recommended and "2" is the lowest configuration.
RAM (MB)	Specify the RAM size of the virtual machine. "4096MB" is recommended and "2048MB" is the lowest configuration.
Root Disk (GB)	Specify the size of root disk .The minimum is 8 GB. We recommend that you set the size to 20 GB.

4. Click **Create Flavor** in the lower-right corner.

Step 3: Create a Network

The network services of OpenStack provide scalable network connectivity for OpenStack cloud deployments. On the OpenStack WebUI, you can create and modify networks.

This document does not describe how to create a network because different users have different networking needs and creating a network is a basic operation of Openstack. For more information, see http://docs.Openstack.org/user-guide/content/dashboard_create_networks.html

In most cases, there is usually an external network, such as 'ext-net,' available in the OpenStack environment, which you can use directly.

Step 4: Start the Instance

Log in to OpenStack WebUI with admin account. To create an instance, take the following steps:

1. Select **Project** > **Compute** > **Instance** , and click **Launch** after the image list created in Step 1.



2. In the < Launch Instance> dialog box, configure the followings.
3. In the <Details> tab, enter the **Instance Name**, such as "iot-identify-vm".
4. In the <Source> tab, you can select **No** for **Create New Volume**.
5. In the <Flavor>tab, select the flavor "iot.normal" configured in step 2.
6. In <Networks> tab, select the network "ext-net" and click  so that the instance can be accessible externally.
7. Keep the other information as default.
8. Click **Create Instance** in the lower-right corner. In most cases, the instance will be automatically started after created.
9. After the instance is created, an IP address is assigned to the instance. You can use this IP address as that of the virtual machine of IoT local asset identification.

Step 5: Log in to Virtual Machine

1. Log in to OpenStack WebUI.
2. Select **Project** > **Compute**> **Instance**.
3. In the list, click the instance name "iot-identify-vm" to go to the instance details page. You can click the Console tab to open the console page in the embedded CLI.
4. Enter the default username and password (hillstone/hillstone) to log in to the virtual machine.

Setp 6: Configure NIC

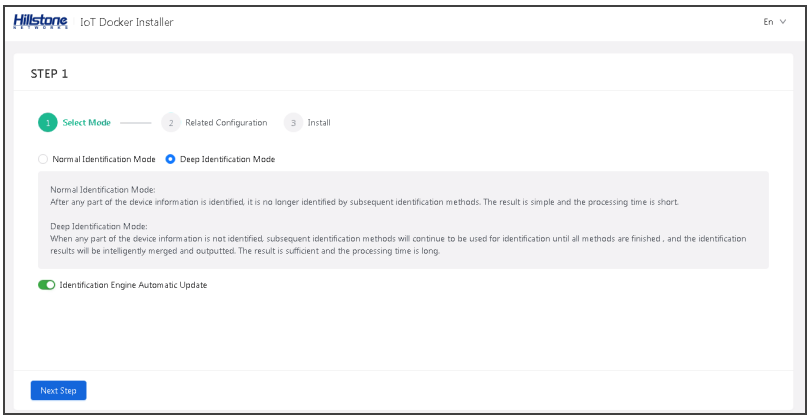
After the virtual machine is deployed, you need to configure the configuration file within /etc/netplan to modify the NIC configuration based on the current environment.

1. Confirm the NIC name. Run the **ip addr** command to view the current NIC name. The default NIC name is "ens160". The default NIC name that is automatically assigned may vary based on deployment environments.
2. Run the **cat /etc/netplan/00-installer-config.yaml** command to view the current configuration file.
3. Run the **vi /etc/netplan/00-installer-config.yaml** command to open the configuration file.
4. Move the cursor to the position where you want to modify and enter **i** to enter the editing mode. You can modify the NIC name and NIC number.
   Note: The NIC name needs to be consistent with the confirmed NIC name.
5. Press "ESC" and then enter **:wq** to exit the configuration file and save the configuration.
6. Restart the virtual machine to ensure the modified NIC information.

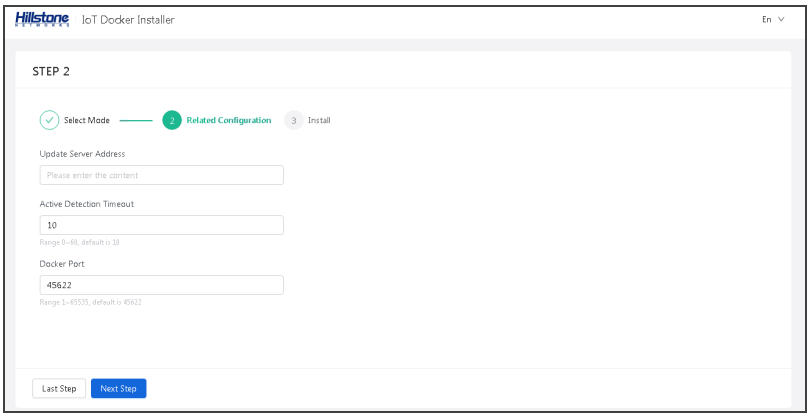
Step 7: Install the asset identification program

1. Open the browser and access the IP address configured in NIC information. Example: https://10.182.237.89:22654
2. Due to the use of a self-signed certificate, the browser displays a warning: 'Your connection is not private'. Click **Advanced** > **Proceed** to continue accessing the site.
3. Enter the asset identification program installation guide. Select an identification mode and click **Next**. By default, **Deep Identification Mode** is selected and **Identification Engine**

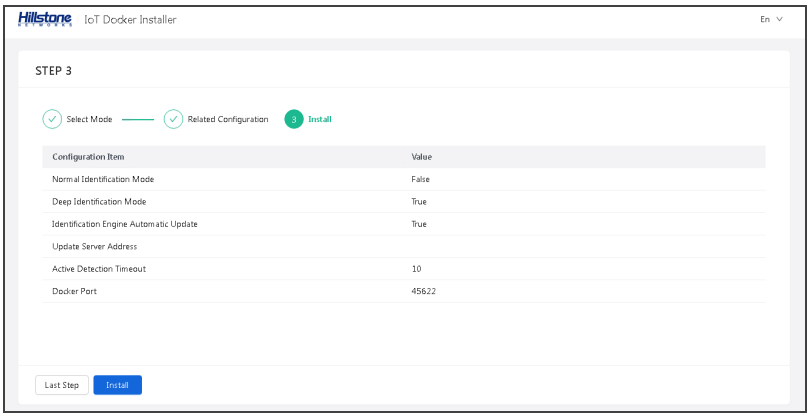
Automatic Update is enabled.



4. In the **Related Configuration** step, configure the Update Server address, active detection timeout, and Docker port number. If you use the default configuration, Update Server provided by Hillstone Networks is used.



5. Confirm the configuration and click **Install**.



6. After the installation is completed, the asset identification program is automatically started.

At this point, the asset identification system is deployed on OpenStack.

Configuring Identification List

Creating Identification List

To create an identification list and enter the configuration mode of the IoT identification list, in the global configuration mode, use the following command:

iot-monitor identify-list *list-name*

- *list-name* - Specifies the name of the identification list and enter the configuration mode of identification list. If the specified name already exists, enter the configuration mode directly.

In the global configuration mode, use the command **no iot-monitor identify-list** *list-name* to delete the specified identification list.



Notes: For the identification list bound to the security zone, it cannot be deleted unless it's unbound.

Configuring the IP/MAC Identification List

To add the IPv4 address, MAC address, username and password of IoT devices into the identification list, in the IoT identification list configuration mode, use the following command:

ip-mac *ipv4-address mac-address* [**username** *username* **password** *password*]

- *ipv4-address* - Specifies the IPv4 address of the IoT device.
- *mac-address* - Specifies the corresponded MAC address of the configured IPv4 address.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the corresponded password of the user.

In the IoT identification list configuration mode, use the command **no ip-mac** *ipv4-address mac-address* to remove the IPv4 address and MAC address of the specified IoT device from the identification list.

To add the IPv6 address, MAC address, username and password of IoT devices into the identification list, in the IoT identification list configuration mode, use the following command:

ipv6-mac *ipv6-address mac-address* [**username** *username* **password** *password*]

- *ipv6-address* - Specifies the IPv6 address of the IoT device.
- *mac-address* - Specifies the corresponded MAC address of the configured IPv6 address.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the corresponded password of the user.

In the IoT identification list configuration mode, use the command **no ipv6-mac** *ipv6-address mac-address* to remove the IPv6 address and MAC address of the specified IoT device from the identification list.

Configuring the IP Identification List

Specifying IP

To add the IPv4 address, user name and password of the IoT device to the identification list, in the IoT identification list configuration mode, use the following command:

ip network {*ip-prefix/mask* | *ip-address mask*} [**username** *username***password** *password*]

- *ip-prefix/mask* - Specifies the IP address and mask, such as 1.1.1.1/24.
- *ip-address* - Specifies the IP address, such as 1.1.1.1.
- *mask* - Specifies the mask, such as 255.255.255.0.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the password of the user.

In the IoT identification list configuration mode, use the command **no ip network** {*ip-prefix/mask* | *ip-address mask*} to delete the IP address of the IoT device from the identification list.

To add the IPv6 address, user name and password of the IoT device to the admittance list, in the IoT identification list configuration mode, use the following command:

ipv6 prefix {*ipv6-prefix / prefix-length*} [**username** *username* **password** *password*]

- *ipv6-prefix / prefix-length* – Specifies the IPv6 prefix and prefix length, the range is 1 to 128.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the password of the user.

In the IoT identification list configuration mode, use the command **no ipv6 prefix** *ipv6-prefix / prefix-length* to delete the IPv6 address of the IoT device from the identification list.



Notes: When the specified IP already exists, system will pop up an error.

Specifying IP Range

To add the IPv4 address range, user name and password of the IoT device to the identification list, in the IoT identification list configuration mode, use the following command:

ip range *start-ip end-ip* [**username** *username* **password** *password*]

- *start-ip* - Specifies the start IP.
- *end-ip* - Specifies the end IP.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the password of the user.

In the IoT identification list configuration mode, use the command **no ip range** *start-ip end-ip* to delete the IP range of IoT device from the identification list.

To add the IPv6 address range, user name and password of the IoT device to the identification list, in the IoT identification list configuration mode, use the following command:

ipv6 range *min-ipv6-address max-ipv6-address* [**username** *username* **password** *password*]

- *min-ipv6-address* – Specifies the start IPv6 address.
- *max-ipv6-address* – Specifies the end IPv6 address.
- *username* - Specifies the user name of the IoT device.
- *password* - Specifies the password of the user.

In the IoT identification list configuration mode, use the command **no ipv6 range** *min-ipv6-address max-ipv6-address* to delete the IPv6 address range of IoT device from the identification list.

Notes: When the specified IP range already exists, system will pop up an error.

Configuring the MAC Identification List

To add the MAC address of the IoT device to the identification list, in the IoT identification list configuration mode, use the following command:

mac *mac-address*

- *mac-address*- Specifies the MAC address.

In the IoT identification list configuration mode, use the command **no mac** *mac-address* to delete the MAC address of the IoT device from the identification list.

Notes: The system allows you to add at most 600 MAC addresses to the identification list.

Importing Identification List

You can import the identification list via the FTP or TFTP server. To import the identification list, in the execution mode, use the following commands:

import iot-monitor identify-list*list-name* **from** {**ftp server** *ip-address***user** *user-name* **password** *password* [**vrouter** *vrouter-name*] | **tftp server** *ip-address* [**vrouter***vrouter-name*] | {**usb0** | **usb1**} *file-name*

- *list-name*- Specifies the name of the target identification list.
- *ip-address*- Specifies the IP address of FTP or TFTP server.
- **user***user-name***password***password* - Specifies the user name and password of the FTP server.
- *vrouter-name* - Specifies the VRouter that the identification list will be import to. If the parameter is not specified, VRouter will be specified as trust-vr.
- *file-name* - Specifies the name of the identification list on the FTP or the TFTP server.

Viewing Information about the Identification List

To show the identification list, in any mode, use the following command:

show iot-monitor identify-list*list-name* [**ip-entry** | **ip-mac-entrty** | **mac-entry**]

- *list-name* - Displays the admittance list information of the specified name.
- **ip-entry** - Displays identification list of the IP type.
- **ip-mac-entrty** - Displays identification list of the IP/MAC type.
- **mac-entrty** - Displays identification list of the MAC type.

Configuring Local Asset Identification

The local asset identification function is to identify IoT devices by using the asset identification module deployed in the device.

Enabling/Disabling the Local Asset Identification Function

By default, the local asset identification function is disabled. To enable or disable the function, in global configuration mode, use the following command:

- Enable: **iot-monitor docker-detect enable**
- Disable: **no iot-monitor docker-detect**

Configuring the Local Asset Identification Function

Local asset identification is divided into built-in and external types.

- Built-in: Use the built-in asset identification module. Before you select this type, configure the Docker management functon of the system to deploy the asset identification system within the firewall.
- External: Use the asset identification system deployed on the virtual machine. Before you select this type, deploy the asset identification system in the virtual machine.



Notes: The built-in type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

To configure the local asset identification function, in global configuration mode, use the following command:

iot-monitor docker-detect {**local-docker** | **external-docker ip** *ip-address*} **port** *port-number* **vrouter** *vr-name*

- **local-docker** - Specifies to use the built-in asset identification module. The default IP address is 127.0.0.1, which requires no configuration or modification.

- **external-docker ip** *ip-address* - Specifies to use the asset identification system deployed on the virtual machine, and specifies the IP address of the virtual machine.
- **port** *port-number* - Specifies the port number of the asset identification module. When you use **local-docker**, this port number is the host port number of Docker. Please make sure this port number is consistent with the host port number specified in Docker. Valid values: 1-65535.
- **vrouter** *vr-name* - Specifies the name of the VRouter to which the virtual machine belongs from the drop-down list.

To cancel the configuration of the local asset identification function, in global configuration mode, use the following command:

no iot-monitor docker-detect local-docker

Viewing the Configuration about the Local Asset Identification Function

To view the configuration about the local asset identification function, in any mode, use the following command:

show iot-monitor docker-detect

Example:

```
-------------------------------------------------------------------------------------------
-------
IoT-monitor docker-detect module environment: A-Firewall local iot
docker
IoT-monitor docker-detect module ip: 127.0.0.1
IoT-monitor docker-detect module port: 36000
IoT-monitor docker-detect module vrouter: trust-vr
IoT-monitor docker-detect action status: disable
-------------------------------------------------------------------------------------------
-------
```

Configuring the Interval of Re-identifying IoT Devices

By default, the device system re-identifies IoT devices at an interval of 20 minutes (1,200 seconds). You can adjust this interval based on your requirements. To do this, in global configuration mode, use the following command:

iot-monitor identify-renew interval *interval-value*

- *interval-value* - Specifies the interval of re-identification. Valid values: 10 to 1200 seconds. Default value: 1200 seconds.

To restore the interval to the default value, in global configuration mode, use the following command:

no iot-monitor identify-renew interval

Configuring Region and Synchronizing Endpoint to Repository

Configuring Region and Sub-region

To create a region and enter the IoT region configuration mode, in global configuration mode, use the following command:

iot-monitor districtid *id***name** *name*

- **id** *id* - Specifies the ID of the region, which can be 1 to 5000.
- **name** *name* - Specifies the name of the region, which can be 1 to 31 characters.

After you run the command, the system creates a region with the specified name and enters the IoT region configuration mode. If the specified name exists, the system enters the IoT region configuration mode directly. In global configuration mode, use the command **no iot-monitor districtid** *id* to delete a specified region.

You can create a sub-region within a specified region. To create a sub-region within a specified region, in IoT region configuration mode, use the following command:

member id *id*

- **id** *id* - Specifies the ID of the region. which can be 1 to 5000. Note: It cannot be the same as the ID of the region.

In IoT region configuration mode, use the command **no member id***id* to delete a specified sub-region.

Configuring an IP Segment for a Region

To configure an IPv4 segment for a region, IoT devices in the region IP network segment will automatically join the region. In IoT region configuration mode, use the following command:

ip network *ip-address/netmask*

- *ip-address/netmask* - Specifies the IP address and the subnet mask corresponding to the region.

In IoT region configuration mode, use the command **no ip network***ip-address/netmask* to delete the IPv4 segment where the specified region resides.

After you configure an IPv6 segment for a region, IoT devices in the regional IP network segment will automatically join the region. The command is valid only when the system version is IPv6. In IoT region configuration mode, use the following command:

ipv6 prefix*ipv6-prefix / prefix-length*

- *ipv6-prefix/prefix-length* - Specify the IPv6 prefix and its length. The range is 1 to 128.

In IoT region configuration mode, use the command **no ipv6 prefix***ipv6-prefix / prefix-length* to delete the IPv6 segment where the specified region resides.

Configuring an IP Range for a Region

To configure an IPv4 range for a region, IoT devices in the region IP network segment will automatically join the region. In IoT region configuration mode, use the following command:

ip range*ip-min ip-max*

- *ip-min* - Specifies the minimum value of the IP range corresponding to the region.
- *ip-max* - Specifies the maximum value of the IP range corresponding to the region.

In IoT region configuration mode, use the command **no ip range***ip-min ip-max* to delte the IPv4 range where the specified region resides.

After you configure an IPv6 range for a region, IoT devices in the region IP network segment will automatically join the region.The command is valid only when the system version is IPv6. In IoT region configuration mode, use the following command:

ipv6 range*ipv6-min ipv6-max*

- *ipv6-min* - Specifies the minimum value of the IPv6 range corresponding to the region.
- *ipv6-max* - Specifies the maximum value of the IPv6 range corresponding to the region.

In IoT region configuration mode, use the command **no ipv6 range***ipv6-min ipv6-max* to delte the IPv6 range where the specified region resides.

Viewing IoT Region Information

To view IoT region information, in any mode, use the following command:

show iot-monitor district [*id*]

- *id* - Specifies the ID of the IoT region whose information you want to view. If not, all region configuration information will be displayed.

Example:

hostname#**show iot-monitor district**

IoT-monitor-district total num: 3

==========

ID name & IP

---

1 test1

139.0.0.0/8

```
2 test2
140.0.0.0/9
3 test3
141.0.0.0/8
=======================================
```

Enabling/Disabling Automatic Synchronization of Endpoint to Repository

To enable/disable automatic synchronization of endpoint to repository, in global configuration mode, use the following command:

iot-monitor sync-respository type *type-name*

- *type-name* - Specifies the endpoint type name. You can use the Tab key after the **type** parameter to view the endpoint type name list and enter the selected endpoint type name.

  Note: If the endpoint type name contains space, you need to use the double quote to quote the entire endpoint type name.

In global configuration mode, use the **no iot-monitor sync-respository type** *type-name* command to disable automatic synchronization of endpoint to repository.

Viewing the Enabling Status of IoT Endpoint Synchronization to Repository

To view all the enabling status of IoT endpoint synchronization to repository, in any mode, use the following command:

show iot-monitor sync-respository type

```
Example:
hostname#show iot-monitor sync-respository type
=======================================================
type sync-repository
-------------------------------------------------------
UNKNOWN disable
```

IPC disable

NVR disable

CVR disable

DVR disable

Video Server disable

Network Server disable

Server disable

Cloud Storage disable

PC disable

Door Control enable

Intercoms disable

Alarm Mainframe disable

Printer disable

Ipad disable

Firewall disable

Other disable

Router disable

Gaming Console disable

Switch disable

Phone disable

Tablet disable

Monitoring Device disable

Video Conferencing disable

Projector disable

Thin Client disable

Scanner disable

```
Video Equipment disable
Voip Phone disable
Attendance Machine disable
Storage disable
==========================================================
```

Configuring the IoT Monitor Function of Security Zone

To perform IoT device identification on security zone traffic based on identification list, take the following steps:

1. Configure an Identification List.
2. Enable the IoT monitor function of security zone and bind the created identification list.
3. Enable the MAC address function in referenced traffic (Optional).

To bind the identification list to the security zone and enable the MAC address function in referenced traffic, you need to enter the zone configuration mode. To do this, in global configuration mode, use the following command:

zone *zone-name*

Binding the Identification List to Security Zone

After you bind the created identification list to security zone, the system performs IoT device identification on security zone traffic based on identification list.

In zone configuration mode, use the following command to bind the identification list to the security zone:

iot-monitor enable *identify-list-name*

- *identify-list-name* - Specifies the identification list name that you want to bind to the security zone. A security zone can be bound to only one identification list.

To unbind the identification list to the security zone, in zone configuration mode, use the following command:

no iot-monitor enable

Enabling/Disabling the MAC Address Function in Referenced Traffic

To use the MAC address obtained in security zone traffic, you can enable the MAC address function in referenced traffic. In other words, no MAC address is used in IoT device identification. By default, this function is disabled.

To enable or disable the MAC address function in referenced traffic, in zone configuration mode, use the following command:

- Enable: **iot-monitor mac-import**
- Disable: **no iot-monitor mac-import**

IoT Monitor

IoT Monitor consists of the following parts:

- Viewing the IoT Monitor List Information
- Modifying IoT Monitor List Entry
- Deleting IoT Monitor List Entry

Viewing the IoT Monitor List Information

To view the whole or the specified IoT monitor list information, in any mode, use the following command:

show iot-monitor-list [**ip** *ip-address*| **ipv6** *ipv6-address*] [**vrouter** *vr-name* | **vswitch** *vs-name*] [**manufacturer** *manufacturer-name*] [**type** *type-name*] [**status** {**online** | **offline**}]

- *ip-address* - Displays the IoT monitor list information of the specified IP address.
- **ipv6***ipv6-address* - Displays the IoT monitor list information of the specified IPv6 address.
- *vr-name* - Displays the IoT monitor list information of the specified VRouter.
- *vs-name* - Displays the IoT monitor list information of the specified VSwitch.
- **manufacturer** *manufacturer-name* - Displays the IoT monitor list information of the specified manufacturers.
- **type** *type-name*- Displays the IoT monitor list information of the specified device type.
- **status** {**online** | **offline**} - Displays the IoT monitor list information of the specified status, including **online** and **offline**.

Modifying IoT Monitor List Entry

To modify the IoT Monitor list entries, in any mode, use the following command:

exec iot-monitor modify iot-monitor-list{ **ip** *ip-address*| **ipv6** *ipv6-address*} {**vrouter** *vr-name* | **vswitch** *vs-name*} [**manufacturer***manufacturer-name*] [**type** *type-name*] [**model** *model-name*]

- *ip-address* - Modify the IoT monitor list entries of the specified IP address.
- **ipv6***ipv6-address* - Modify the IoT monitor list entries of the specified IPv6 address.
- *vr-name* - Specifies the VRouter name of the IP.
- *vs-name* - Specifies the VSwitch name of the IP.
- **manufacturer** *manufacturer-name*- Modify the manufacturers of the IoT monitor list entry of the specified IP address.
- **type** *type-name*- Modify the device type of the IoT monitor list entry of the specified IP address.

- *model-name* - Modify the device model of the IoT monitor list entry of the specified IP address.

Deleting IoT Monitor List Entry

To delete the whole or the specified IoT monitor list entries, in any mode, use the following command:

exec iot-monitordeleteiot-monitor-list [**ip***ip-address*| **ipv6** *ipv6-address*] [**vrouter** *vr-name* | **vswitch** *vs-name*] [**manufacturer** *manufacturer-name*] [**type** *type-name*] [**status** {**online** | **offline**}]

- *ip-address* - Delete the IoT monitor list entries of the specified IP address.
- **ipv6***ipv6-address* - Delete the IoT monitor list entries of the specified IPv6 address.
- *vr-name* - Delete the IoT monitor list entries of the specified VRouter.
- *vs-name* - Delete the IoT monitor list entries of the specified VSwitch.
- **manufacturer** *manufacturer-name* - Delete the IoT monitor list entries of the specified manufacturers.
- **type***type-name*- Delete the IoT monitor list entries of the specified device type.
- **status** {**online** | **offline**} - Delete the IoT monitor list entries of the specified status, including **online** and **offline**.

Device Object

You can categorize one or more IoT devices into a device collection based on multiple dimensions of the device (including the manufacturer, type, model, and operating system of the device) and assign a device object name to the device collection. The system maps the identified IoT device information with the device object attributes, and then the security policy can directly reference the device object name to control the IoT device collection.



Notes: The device object can be configured only after you install an IoT control license.

Configuring Device Object

You can perform the following operations on device object:

- Creating/Deleting a device object
- Configuring the device type of the device object
- Configuring the manufacturer of the device object
- Configuring the model of the device object
- Configuring the OS family of the device object
- Configuring the OS version of the device object
- Viewing the configuration about the device object
- Viewing the mapping IP address of device
- Viewing the device object to which the specified IP address belongs

Creating/Deleting a Device Object

To create a device object, in global configuration mode, use the following command:

device *device-name*

- *device-name* – Specifies the name of the device object, which needs to be 1 to 31 characters in length.

After you run the command, the system creates a device object with the specified name and enters the device object configuration mode. If the specified name exists, the system enters the device object configuration mode directly.

To delete the device object, in global configuration mode, use the following command:

no device *device-name*

Configuring the Device Type of the Device Object

To configure the device type of the device object by selecting a predefined device type or custom device type, in device object configuration mode, use the following command:

type *type-name*

- *type-name* – the device type of the device object:
    - Predefined: Specifies the predefined OS family name. You can use the Tab key after the **type** parameter to view the complete predefined device type list.
    - User-defined: Enter the device type name, which needs to be 1 to 63 characters in length.

To delete the specified device type, in device object configuration mode, use the following command:

no type

Configuring the Manufacturer of the Device Object

To configure the manufacture of the device object by selecting a predefined manufacturer name or custom manufacturer name, in device object configuration mode, use the following command:

manufacturer *manufacturer-name*

- *manufacturer-name* – the manufacturer name of the device object:
    - Predefined: Specifies the predefined manufacturer name. You can use the Tab key after the **manufacturer** parameter to view the complete predefined manufacturer name list.
    - User-defined: Enter the manufacturer name, which needs to be 1 to 63 characters in length.

To delete the specified manufacturer name, in device object configuration mode, use the following command:

no manufacturer

Configuring the Model of the Device

To configure the device model of the device object, in device object configuration mode, use the following command:

model *model-name*

- *model-name* – Specifies the device model of the device object, which needs to be 1 to 31 characters in length.

To delete the specified device model, in device object configuration mode, use the following command:

no model

Configuring the OS Family of the Device Object

To configure the OS family of the device object by selecting a predefined OS family name or custom OS family name, in device object configuration mode, use the following command:

os-family *os-family-name*

- *os-family-name* – the OS family name:
    - Predefined: Specifies the predefined OS family name. You can use the Tab key after the **os-family** parameter to view the complete predefined OS family name list.
    - User-defined: Enter the OS family name, which needs to be 1 to 63 characters in length.

To delete the specified OS family, in device object configuration mode, use the following command:

no os-family

Configuring the OS Version of the Device Object

To configure the OS version of the device object by selecting a predefined OS version or custom OS version name, in device object configuration mode, use the following command:

os-version *os-version-name*

- *os-version-name* – the OS version name:
  - Predefined: Specifies the predefined OS version name. You can use the Tab key after the **os-version** parameter to view the complete predefined OS version list.
  - User-defined: Enter the OS version name, which needs to be 1 to 127 characters in length.

To delete the specified OS version, in device object configuration mode, use the following command:

no os-version

Viewing the Configuration about the Device Object

You can use the following command to view the configuration about the device object in any mode:

show device *device-name*

- **show device** – Displays the detailed configuration of all device objects.
- *device-name* – Displays the configuration of the device object with the specified name.

Viewing the Mapping IP Address of Device

You can use the following command to view the mapping IP address list of the device object with the specified name in any mode:

show device *device-name***ip-list**

- *device-name* – Specifies the device object name whose mapping IP address you want to view.

Viewing the Device Object to Which the Specified IP Address Belongs

You can use the following command to view the device object to which the specified IP address belongs in any mode:

show device mapping ip *ipv4-address / ipv6-address*

- *ipv4-address / ipv6-address* – Specifies to query the IPv4 address or IPv6 address that belongs to the device object.

Honeypot

Introduction

Hillstone Deception Decoy System employs deception and trap techniques to induce and redirect malicious traffic, leading attackers into a honeypot environment. This disrupts their tactics, consumes their time, actively combats their actions, and provides you with proactive defense capabilities, including attack capture, attack display, attacker profiling, attack replay, data analysis, and traceback and countermeasures. The deception decoy system acts as the last line of defense.

The system supports the honeypot function and enables collaboration between the firewall device and Hillstone Deception Decoy System (Honeypot or Honeypot system). By connecting the honeypot system to the firewall device and configuring trap rules, attacker IP addresses that match the trap rules are diverted to the honeypot system for containment. This prevents attacks on your real business environment. Meanwhile, the honeypot system analyzes trapped attacker information, synchronizes it to the firewall device, and then allows you to add attacker IP addresses to the blacklist based on your requirements.

Configuring the Honeypot Function

To configure the Honeypot function, take the following steps:

1. Connecting to Honeypot
2. Configuring a Trap Rule
3. Viewing the Configuration about the Honeypot Function

Connecting to Honeypot

Before you use the Honeypot function, the firewall needs to connect to the honeypot system (including cloud honeypot or local honeypot). Before the connection, you need to obtain the following information about the honeypot system: IP address or domain name of the server, port number, tenant ID, and authentication key. After the connection is established and the authentication is successful, the firewall sends heartbeat messages to the honeypot system at regular intervals to check the connection.

The configurations required for connecting to Honeypot are as follows.

- Enabling/Disabling the Honeypot Function
- Configuring the Address of the Honeypot System
- Configuring the Port Number of the Honeypot System
- Configuring the Heartbeat Detection Cycle
- Configuring the Virtual Router to Which the Honeypot System Belongs
- Configuring the Tenant ID of the Honeypot System
- Configuring the Authentication Key of the Honeypot System
- Configuring the Source Address of the Trap Rule
- Configuring the Disguised Address of the Trap Rule

Entering the Honeypot Configuration Mode

Before you connect to Honeypot and configure a honeypot trap rule, you need to enter the honeypot configuration mode. To do this, in global configuration mode, use the following command:

honeypot

Enabling/Disabling the Honeypot Function

By default, the Honeypot Function is disabled. To enable/disable the Honeypot function, in honeypot configuration mode, use the following command:

- Enable: **enable**
- Disable: **disable**

Configuring the Address of the Honeypot System

To configure the address of the honeypot system, in honeypot configuration mode, use the following command:

server {*ip_address* | *ipv6_address* | *domain_name*}

- *ip_address* – Specifies the IPv4 address of the honeypot system.
- *ipv6_address* – Specifies the IPv6 address of the honeypot system.
- *domain_name* – Specifies the domain name of the honeypot system, which needs to be 1 to 255 characters in length.

To delete the configured address of the honeypot system, in honeypot configuration mode, use the following command:

no rule

Configuring the Port Number of the Honeypot System

To configure the port number of the honeypot system, in honeypot configuration mode, use the following command:

auth-port*port_number*

- *port_number* – Specifies the port number of the honeypot system. Valid values: 0 to 65535. Default value: 443.

To restore the port number to the default value, in honeypot configuration mode, use the following command:

no auth-port

Configuring the Heartbeat Detection Cycle

The heartbeat detection cycle is used to check the connection between the firewall and honeypot system. If the firewall does not receive a heartbeat message from the honeypot system within the specified heartbeat detection cycle, the firewall and honeypot are not connected.

To configure the heartbeat detection cycle, in honeypot configuration mode, use the following command:

track-interval *time_value*

- *port_number* – Specifies the heartbeat detection cycle. Valid values: 3 to 60 seconds. Default value: 15 seconds.

To restore the heartbeat detection cycle to the default value, in honeypot configuration mode, use the following command:

no track-interval

Configuring the Virtual Router to Which the Honeypot System Belongs

To configure the virtual router to which the honeypot system belongs, in honeypot configuration mode, use the following command:

vrouter *vrouter_name*

- *vrouter_name* – Specifies the name of the virtual router to which the honeypot system belongs.

To delete the configured virtual router, in honeypot configuration mode, use the following command:

no vrouter

Configuring the Tenant ID of the Honeypot System

To configure the tenant ID of the honeypot system, in honeypot configuration mode, use the following command:

hf-id *id_number*

- *id_number* – Specifies the tenant ID of the honeypot system, which needs to be 1 to 63 characters in length. This ID is provided by the honeypot system. To obtain this ID, contact Hillstone technical support.

To delete the configured tenant ID, in honeypot configuration mode, use the following command:

no hf-id

Configuring the Authentication Key of the Honeypot System

To configure the authentication key of the honeypot system, in honeypot configuration mode, use the following command:

auth-key *key_word*

- *key_word* – Specifies the authentication key of the honeypot system, which needs to be 1 to 255 characters in length. This authentication key is provided by the honeypot system. To obtain this authentication key, contact Hillstone technical support.

To delete the configured authentication key, in honeypot configuration mode, use the following command:

no auth-key

Configuring a Trap Rule

The system can divert the attack traffic to the decoy business of the honeypot based on the conditions configured in the trap rule. This ensures the security of real business.

The configurations of the trap rule are as follows.

- Creating a Trap Rule and Entering the Trap Rule Configuration Mode
- Enabling/Disabling the Trap Rule
- Configuring the Trap Rule Name
- Configuring the Honeypot Template
- Configuring the Virtual Router to Which the Trap Rule Belongs

Creating a Trap Rule and Entering the Trap Rule Configuration Mode

Before you configure the trap rule, you need to create one and enter the trap rule configuration mode. If the specified ID or name already exists, you will directly enter the trap rule configuration mode.

To create a trap rule and enter the trap rule configuration mode, in honeypot configuration mode, use the following command:

rule {**id** *id*| **name** *name*}

- *id* – Specifies the ID of the trap rule. Valid values: 1 to 255. If the specified ID already exists, you will directly enter the trap rule configuration mode.
- *name* – Specifies the name of the trap rule, which needs to be 1 to 127 characters in length. If the specified name already exists, you will directly enter the trap rule configuration mode.

To delete the trap rule of the specified ID/name, in honeypot configuration mode, use the following command:

no rule {**id** *id*| **name** *name*}

Enabling/Disabling the Trap Rule

To enable/disable the trap rule, in trap rule configuration mode, use the following command:

- Enable: **enable**
- Disable: **disable**



Notes: By default, a created trap rule is enabled.

Configuring the Trap Rule Name

To configure the trap rule name, in trap rule configuration mode, use the following command:

name *name*

- *name* – Specifies the name of the trap rule, which needs to be 1 to 127 characters in length.

To delete the configured trap rule name, in trap rule configuration mode, use the following command:

no name

Configuring the Source Address of the Trap Rule

To configure the source address of the trap rule, that is, the attacker address, in trap rule configuration mode, use the following command:

src-ip {*A.B.C.D/M* | *X:X:X:X::X/M*}

- *A.B.C.D/M* – Specifies the attacker address of the IPv4 type.
- *X:X:X:X::X/M* – Specifies the attacker address of the IPv6 type.

Configuring the Disguised Address of the Trap Rule

When the attacker accesses the disguised address, the trap rule is hit. In this case, the attacker will be diverted to the disguised business of the honeypot template. This protects your real business from attacks.

To configure the disguised address of the trap rule, in trap rule configuration mode, use the following command:

disguised-ip {*A.B.C.D/M* | *X:X:X:X::X/M*}

- *A.B.C.D/M* – Specifies the disguised address of the IPv4 type.
- *X:X:X:X::X/M* – Specifies the disguised address of the IPv6 type.

Configuring the Honeypot Template

After the firewall establishes a connection with the honeypot system, honeypot templates in the honeypot system will be automatically synchronized to the firewall. The attacker who hits the trap rule will be diverted to the disguised business of the honeypot template. This protects your real business from attacks.

To configure the honeypot template, in trap rule configuration mode, use the following command:

profile id *id*

- *id* – Specifies the ID of the honeypot template.

To delete the specified honeypot template, in trap rule configuration mode, use the following command:

no profile id

Configuring the Virtual Router to Which the Trap Rule Belongs

To configure the virtual router, in trap rule configuration mode, use the following command:

vrouter *vrouter_name*

- *vrouter_name* – Specified the name of the virtual router to which the effective scope of the trap rule belongs. If not specified, the trap rule takes effect globally.

To delete the configured virtual router, in trap rule configuration mode, use the following command:

no vrouter

Viewing the Configuration about the Honeypot Function

To view the configuration about the Honeypot function, in any mode, use the following command:

show honeypot {**config** | **service-profiles** | **memory** | **rules**}

- **config** – Shows the configuration of connecting to Honeypot, including the enable status, connection status, server address and port number of the honeypot system, tenant ID, and authentication key.
- **service-profiles** – Shows the configuration of the honeypot template, including the template ID, template name, IP address, and port number.
- **memory** – Shows the memory usage of the Honeypot function, including the current memory usage and the historical maximum memory usage.
- **rules** – Shows the configuration of the created trap rule, including the enable status, rule ID, rule name, attacker address, disguised address, and honeypot template.

Cloud-Network Collaborative DNS Protection

The Domain Name System (DNS) is a critical component of network communication, and its security is vital for maintaining the overall safety of the network environment. Attackers often exploit DNS's widespread presence and high traffic to mask malicious activities. Research shows that up to 80% of malware uses DNS to initiate command-and-control programs. Consequently, implementing effective DNS security detection not only uncovers potential network threats but is also crucial in preventing malware propagation and data breaches.

Hillstone Networks offers several cloud-network collaborative DNS security solutions:

- Unknown Domain Cloud Collaborative Query: Collaborating with CloudVista, the system continuously enhances threat detection capabilities by leveraging vast cloud-based threat intelligence. It performs real-time cloud queries to assess the risk status of unknown domains. Coupled with the botnet prevention function, this solution effectively intercepts risky DNS traffic at the internet egress.
- Cloud-Based DNS Security Detection: Integrating with secure DNS SaaS services, this solution proxies and forwards DNS traffic from the internal network to the cloud for domain resolution via DoH (DNS over HTTPS). This ensures the integrity and confidentiality of the resolution process. In addition, the cloud can identify and block malicious domains using extensive threat intelligence, effectively safeguarding internal network hosts.

Unknown Domain Cloud Collaborative Query

Introduction

For domains that are not included in the botnet address library, exception list, or block list (referred to as "unknown domains" in this context), there may be challenges in controlling and defending against them by using the botnet prevention function.

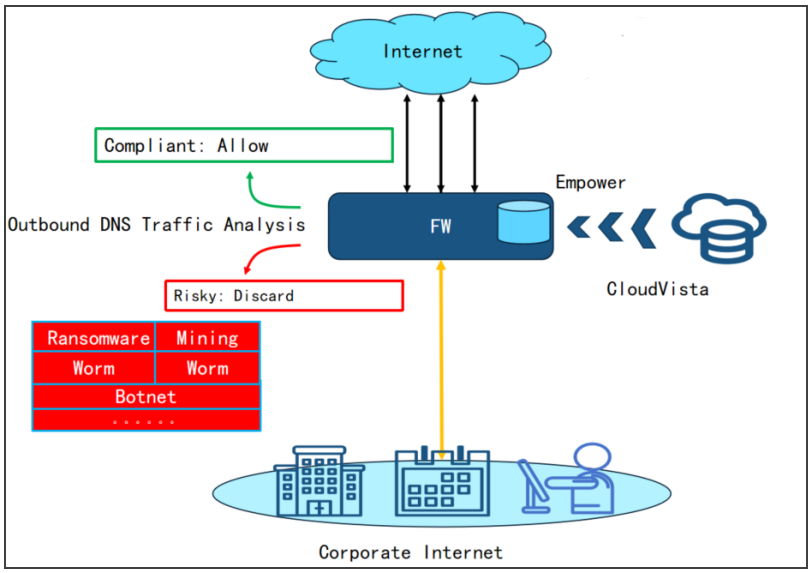
The system provides the Unknown Domain Cloud Collaborative Query function (referred to as "Cloud Query"), which retains the original network deployment while using real-time cloud queries to assess the risk status of these unknown domains. This expands the botnet prevention's signature database by integrating with CloudVista, enhancing DNS traffic analysis and malicious

domain control capabilities. This solution can effectively intercept risky DNS traffic at the internet egress, thereby protecting internal network hosts from potential threats.

Typical Application Scenario

The firewall is deployed as a gateway at the internet border egress, combined with CloudVista, to send unknown domain data to the cloud for risk status verification. The function collaborates with the botnet prevention function's domain signature database to analyze the outbound DNS traffic:

- For compliant domain request traffic, it allows;
- For risky domain request traffic, it discards and blocks.



Configuring Unknown Domain Cloud Collaborative Query (Cloud Query)

Notes: This function is controlled by the Botnet Prevention license and no longer takes effect after the Botnet Prevention license expires.

Before you begin:

- Read Unknown Domain Cloud Collaborative Query
- Install the Botnet Prevention license
- Connecting to Hillstone Cloud Service Platform

This section consists of the following content:

- Enabling/Disabling Unknown Domain Cloud Collaborative Query
- Specifying the Unknown Domain Cloud Collaborative Query Token
- Configuring Cloud Query Timeout Time
- Viewing Cloud Query Timeout Time
- Viewing Cloud Query Cache Data
- (Optional) Clearing Cloud Query Cache Data
- Viewing Cloud Query Configuration

Enabling/Disabling Unknown Domain Cloud Collaborative Query

By default, this function is disabled. To enable/disable Unknown Domain Cloud Collaborative Query, in CloudVista configuration mode, use the following command:

- Enable: **connect-vista enable**
- Disable: **no connect-vista enable**

Specifying the Unknown Domain Cloud Collaborative Query Token

When you use the Unknown Domain Cloud Collaborative Query function, you need to specify the token for validation. The cloud provides available query services based on the token, which corresponds to the Hillstone cloud service account that connects to the cloud platform.

Before you start

- Take the following steps to obtain the token.

    1. Visit https://ti.hillstonenet.com.cn/.
    2. Click **Login** to go to the Hillstone Cloud Service login page. Then, use the Hillstone Cloud Service account to log in to the cloud platform.
    3. Return to CloudVista. Click the username in the upper-right corner and select **Authorization Management** from the drop-down list.
    4. On the page that appears, copy the token displayed in the **API Key** field.

To specify the Unknown Domain Cloud Collaborative Query token, in CloudVista configuration mode, use the following command:

auth-token*auth-token*

- *auth-token* - Specifies the obtained token, which needs to be 64 characters in length.

In CloudVista configuration mode, use the **no auth-token** command to delete the specified token.

Configuring Cloud Query Timeout Time

After enabling the Unknown Domain Cloud Collaborative Query function, the system will upload unknown domains of the Botnet Prevention function to the cloud for further query, and then handle traffic based on the verification results. The cloud-based verification results can be cached on the device (Cloud Cache), and is used for subsequent domain detection. During the upload of domain query, the system temporarily suspends forwarding packets containing unknown domains. The maximum duration for suspension is the cloud query timeout time.
If the cloud returns the risk status within the cloud query timeout time, the system performs the corresponding action (continue forwarding or drop) based on the severity of the risk; If no cloud-based query results are returned within the cloud query timeout time, packets containing unknown domains will be forwarded.

Before you start

- Enable Unknown Domain Cloud Collaborative Query.

To configure Cloud Query timeout time, in global configuration mode, use the following command:

botnet-c2-prevention delay-time*delay-time*

- *delay-time* - Specifies the maximum value of the cloud query timeout time. Default value: 500 ms. Valid values: 0 to 1000 ms.

Querying Cloud Query Cache Data

After the device connects to the Hillstone cloud platform, the cloud will periodically push domain/IP/URL addresses to the device. This data, along with the cloud query results for unknown domains, is stored in the "Cloud Cache" of the device for subsequent botnet prevention threat detection.

To specify the IP/domain/URL to query detailed results in cloud cache information and take corresponding measures, in any mode, use the following command:

show botnet-c2-prevention cache*cache-information*

- *cache-information* - Specifies the IP address, domain name, or URL that you want to query.

Based on the cloud query results for unknown domains, different actions can be taken:

- **Blacklist**: When the "result" is "black," traffic associated with the domain is handled based on the configured botnet prevention rules. If manual analysis determines that the domain is a false positive or the traffic is safe to allow, you can add the entry to a custom exclude list. When traffic matches this IP address, domain, or URL, the system will not apply botnet prevention controls to it.
- **Whitelist/Unknown**: When the "cloud query result" is "white" or "grey," the traffic will be allowed by default.

Take the domain name "hr.woqukaoqin.com" as an example:

```
hostname#show botnet-c2-prevention cache hr.woqukaoqin.com
Botnet Prevention Cloud Cache Data
```

```
=============================================================-
=========
name                type            result          time            tags
-------------------------------------------------------------------------------
hr.woqukaoqin.com       specific domain         grey        0d 0h 1m 20s
=============================================================-
=========
```

Clearing Cloud Query Cache Data

To quickly clear cloud query cache results stored in the device, in any mode, use the following command:

clear botnet-c2-prevention cache-data

Viewing Cloud Query Configuration

To view cloud query configuration, in any mode, use the following command:

show botnet-c2-prevention cloud-search-config

Cloud-Based DNS Security Detection

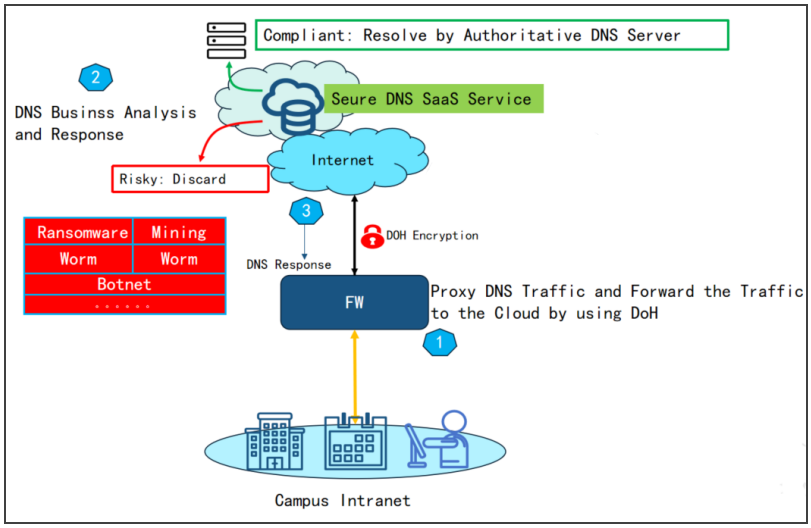
Introduction

In traditional DNS resolution, packets are transmitted by using unencrypted DNS protocols (such as UDP). Attackers can exploit this by using man-in-the-middle techniques to tamper with DNS traffic, posing significant security threats to organizations.

The system provides the Cloud-Based DNS Security Detection function that maintains the existing network deployment while integrating with a secure DNS SaaS service. This function forwards DNS traffic from the internal network by using DoH (DNS over HTTPS) to the cloud for domain name resolution, ensuring the integrity and confidentiality of the resolution process. In addition, the cloud leverages its extensive threat intelligence to identify and block risky domains or IP addresses, effectively safeguarding internal network hosts.

Typical Application Scenario

The firewall is deployed as a gateway at the internet border egress. After integrating with the secure DNS SaaS service, it proxies internal network's DNS traffic and forwards the traffic to the cloud by using DoH. While performing domain name resolution, the cloud leverages extensive threat intelligence to identify and block risky domains or IP addresses. Compliant DNS response packets are returned to the firewall, while malicious domains are discarded.



Secure DNS

The Secure DNS function is a cloud-network collaborative security solution that allows real-time security detection of DNS traffic and blocks malicious domain access when DNS proxy requests are initiated by intranet devices. In this solution, the firewall forwards DNS traffic proxies passing through the firewall to the cloud-based Secure DNS SaaS service by using the DNS proxy function and DoH encrypted transmission protocol, where the threat is sensed, identified, and blocked. In addition, basic DNS resolution is implemented.

When configuring the Secure DNS function, you do not need to modify the DNS configuration of intranet devices, so it is completely transparent to the intranet devices. In addition, compared with traditional DNS service, Secure DNS SaaS service provides DNS service as well as the ability of security protection.



Notes: The device supports integration with 360 Secure DNS SaaS service. Before you enable this function, go to sdns.360.cn to apply for 360 Secure DNS SaaS service.

The configuration of the Secure DNS function includes:

- Enabling/Disabling the Secure DNS Function
- Entering the Secure-DNS Profile Configuration Mode of a Specified Provider
- Configuring the DoH Server
- Enabling/Disabling the Function of Sending the Client Address
- Configuring the Health Check Interval
- Enabling/Disabling the Function of Generating Logs
- Viewing Information about Secure DNS Configuration

Enabling/Disabling the Secure DNS Function

By default, the Secure DNS function is disabled. To enable this function and specify the DoH server provider, in global configuration mode, use the following command:

secure-dns enable service-provider *provider-name*

- *provider-name* – Specifies the provider name of the DoH server. Only 360 is supported.

To disable the Secure DNS function, in global configuration mode, use the following command:

secure-dns disable

Entering the Secure-DNS Profile Configuration Mode of a Specified Provider

To configure the Secure DNS function, you need to enter the Secure-DNS Profile configuration mode of a specified provider. To do this, in global configuration mode, use the following command:

secure-dns profile service-provider *provider-name*

- *provider-name* – Specifies the provider name of the DoH server. Only 360 is supported.

Configuring the DoH Server

To configure the domain name or IP address of the DoH server and the corresponding virtual router, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

doh-server {*domain* | *ip-address*} [**vrouter** *vr-name*]

- *domain* | *ip-address* – Specifies the domain name or IP address of the DoH server. By default, doh.360.cn is used.
- *vr-name* – Specifies the virtual router to which the DoH server belongs. By default, trust-vr is used.

In Secure-DNS Profile configuration mode, use the **no doh-server** command to restore to the default configuration.

Enabling/Disabling the Function of Sending the Client Address

After enabling this function, when you request domain resolution by using DNS proxy, the system uploads the IP address of the client to 360 cloud for O&M.

To enable/disable the function of sending the client address, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

- Enable: **send-client-ip enable**
- Disable: **send-client-ip disable**

Configuring the Health Check Interval

To avoid the failure of domain name resolution by using the DoH protocol due to an abnormal DoH server, the system can periodically send DNS health check messages to the DoH server. When two consecutive health checks fail, the system switches the Secure DNS function to Inactive. While in the Inactive status, the system cannot use the DoH protocol through the Secure DNS function to resolve domain names , but it continues to send health check messages. Once a

successful check is detected, the Secure DNS function will be immediately switched to Active.

To configure a health check interval, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

track-interval *time-value*

- *time-value* – Specifies the interval at which a DNS health check message is sent to the DoH server. Valid values: 3 to 60 seconds. Default value: 10 seconds.

In Secure-DNS Profile configuration mode, use the **no track-interval** command to restore to the default configuration.

Enabling/Disabling the Function of Generating Logs

After enabling this function, when you request the resolution of malicious domain names by using DNS proxy, corresponding threat logs are generated. By default, this function is disabled.

To enable/disable the function of generating logs, in Secure-DNS Profile configuration mode of the specified provider, use the following command:

- Enable: **threat-log enable**
- Disable: **threat-log disable**

Viewing Information about Secure DNS Configuration

To view information about Secure DNS configuration, in any mode, use the following command:

show secure-dns

The following result is returned:

```
hostname(config)# show secure-dns
==========================================================-
=============
Secure DNS: Enable (The status of the Secure DNS function)
Service provider: 360 (The provider that provides the Secure DNS function)
Service status: Active (The availability status of the Secure DNS function)
```

```
------------------------------------------------------------------------------------------------------------
----------------------

Profile 360:

Bootstrap server: 101.198.198.198 101.198.199.200 (The built-in 360 public DoH server,
which is used to resolve the DoH server domain name)

DoH server domain: hxr5.n.360.net (The specified DoH server domain name)

DoH server IP: 36.110.234.252, TTL 241 s (The IP address of the DoH server that is
resolved by Bootstrap)

DoH server vrouter: trust-vr (The VRouter to which the DoH server belongs)

Send-client-addr: Enable (The status of the function of sending the client address)

Threat-log: Enable (The status of the function of generating logs)

Track interval: 10 s (The health check interval)

==============================================================
=============
```

Chapter 13 Data Security & URL Filtering

The chapter introduces the following topics:

- "Data Security" on Page 2416 describes the data security functions included in the system, including content filtering, file filtering, online behavior auditing, and log management.
- "Object Configuration" on Page 2465 describes the public Data Security configurations that are used for configuring Data Security rules.
- "URL Filtering" on Page 2484 explains how to configure the URL filtering function to control the access to some websites.
- "SSL Proxy" on Page 2494 describes how to configure the SSL proxy function in two typical scenarios to decrypt HTTPS traffic.

Data Security

Overview

The booming and popularization of Internet bring significant convenience to people’ s work and life. However, problems caused by access to Internet, like bandwidth misuse, low efficiency, information leakage, legal risks, security potentials, etc., are also becoming increasingly prominent. For example, in some enterprises, online chatting and Internet forum browsing during the office hours, or disclose some confidential information to the public in emails; in some public places like net bar, netizens randomly visit illegal websites, post irresponsible topics, or even get involved in illegal network movement.

To solve the above problems, system provides the Data Securityfunction to control and audit network behaviors, and check the transmitted files,effectively optimizing the utilization of Internet resources.

Introduction to Data Security

The Data Security function of StoneOS allows you to flexibly configure control rules for different users, network behaviors and schedules, check the transmitted files, in order to perform comprehensive control and audit (by behavior logs) on users’ network behavior.

StoneOS Data Security includes the following features. The main functions and description is listed in the table below.

- Content filter
    - File content filter
    - Web Content
    - Web posting
    - Email filter
    - APP behavior control

- Network Behavior Record
    - IM
    - Web Surfing Record
- File filter
- Log management

Function		Description
Content Filter	File Content Filter	Detect sensitive keywords carried in the file content of the specified protocol type and file type, and can log or block them.
	URL keyword	Controls the network behavior of visiting the webpages (including the webpages encrypted by HTTPS) that contain certain keywords, and log the actions.
	Web posting	Controls the network behavior of posting on websites (including the webpages encrypted by HTTPS) and posting specific keywords, and logs the posting.
	Email filter	Controls and audit SMTP/POP3/IMAP mails: • Control and audit all the behaviors of sending emails; • Control and audit the behaviors of sending emails that contain specific sender, recipient, keyword or attachment.
	APP behavior control	Controls and audits the actions of HTTP, FTP and TELNET applications:

Function		Description
		• FTP content and methods, including Login, Get, and Put; • HTTP methods, including Connect, Get, Put, Head, Options, Post, and Trace; • Request content initiated by the TELNET client.
Network Behavior Record	IM	Audits the QQ, wechat and sinaweibo user behaviors.
	Web Surfing Record	Log the access behaviors.
File filter		Checks the files transported through HTTP, FTP, SMTP, IMAP, POP3, SMBprotocols and control them according to the file filter rules.
Log		Rich Data Security log export and storage solution; combined with HSM, allows in-depth log statistics and audit analysis.

Content Filter

Security includes the following features.

- File Content Filter
- Web Content
- Web posting
- Email filter
- APP behavior control

If IPv6 is enabled, Content Filter function supports content detection and behavior control based on IPv6. For more information about how to enable IPv6, see IPv6.

File Content Filter

The file content filtering function can detect sensitive keywords carried in the file content of the specified protocol type and file type, and can log or block them. For example, the content of doc-type files downloaded through the HTTP protocol is detected, and the log information is recorded for the files containing the keyword content of the mobile phone number.

Configuring File Content Filter via CLI

The file content filter function is mainly implemented by binding a profile to a policy rule. Once the Web content profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. The system also supports binding the file content filter profile to a ZTNA policy to perform file content detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To configure Web content via CLI, take the following steps:

1. Create a file content filter profile, and specify the file type, protocol type, direction, keyword category and action in the profile.

2. Bind the file content filter profile to an appropriate policy rule or a zone.

Creating a File Content Filter Profile

You need to specify the file type, protocol type, direction, keyword category and action in the Web content profile. To create a file content filter profile, in the global configuration mode, use the following command:

file-contentfilter-profile *profile-name*

- *profile-name* - Specifies the name of the file content filter profile, and enter the configuration mode of the file content filter profile. If the specified name exists, the system will directly enter the file content filter profile configuration mode. To delete the specified file content filter profile, in the global configuration mode, use the command **no file-contentfilter-profile** *profile-name*.

Specifying the File Type

To specify the file type that will be filtered, in the file content filter profile configuration mode, use the following command:

file-type {**txt** | **doc** | **docx** | **ppt** | **pptx** | **xls** | **xlsx**}

- **txt** | **doc** | **docx** | **ppt** | **pptx** | **xls** | **xlsx** - Specifies the file type that will be filtered. Currently supported file types are: txt, doc, docx, ppt, pptx, xls, xlsx.

Repeat the command to add more file types.

To cancel the specified the file type, in the file content filter profile configuration mode, use the command **no file-type** {**txt** | **doc** | **docx** | **ppt** | **pptx** | **xls** | **xlsx**}.

Specifying the Keyword Category and Action

To specify the keyword category that will be filtered and the corresponding action, in the file content filter profile configuration mode, use the following command:

keyword-category*keyword-category-name* **action** {**block** | **log-only**}

- *keyword-category-name* - Specifies the keyword category that will be filtered. It can be a custom keyword category or a predefined keyword category. For more information about keyword category, see Keyword Category.
- **block** – Blocks the transmission of files containing the content of the corresponding keywords and log records.
- **log** – Logs the behavior of transferring files containing corresponding keyword content.

Repeat the command to add more keyword categories and actions.

To cancel the specified the keyword category and action, in the file content filter profile configuration mode, use the command **no keyword-category** *keyword-category-name* .

Specifying the Protocol Type and Direction

To specify the protocol type and direction, in the file content filter profile configuration mode, use the following command:

protocol-type {**ftp** | **http** | **imap4** | **pop3** | **smb** | **smtp** } **direction** {**both** | **download** | **upload**}

- **ftp** | **http** | **imap4** | **pop3** | **smb** | **smtp** - Specifies the protocol type.
- **direction** {**both** | **download** | **upload**}- Specifies the direction, include bidirectional **both**, download **download**and upload**upload**. HTTP, FTP, and SMB protocols support Download, Upload, and Bidirectional; SMTP protocol only supports select Upload; POP3 and IMAP protocols only support Download.

To cancel the specified the protocol type and direction, in the file content filter profile configuration mode, use the command**no protocol-type**.

Binding the File Content Filter Profile to a Policy Rule

After binding the file content filter profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the file content filter profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the file content filter profile to a policy rule, in the policy rule configuration mode, use the following command:

file-contentfilter *profile-name*

- *profile-name* - Specifies the name of file content filter profile that will be bound.

Binding the File Content Filter Profile to a Security Zone

If the file content filter profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a file content filter profile, and the destination zone of the policy rule is also bound with a file content filter profile, then the file content filter profile bound to the policy rule will be valid.

To bind the file content filter profile to a security zone, in the security zone configuration mode, use the following command:

file-contentfilter enable *profile-name*

- *profile-name* – Specifies the name of the file content filter profile that will be bound to the security zone. One security zone can only be bound with one file content filter profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no file-contentfilter enable

Viewing File Content Filter Profile Information

To view the file content filter profile information, in any mode, use the following command:

show file-contentfilter-profile [*profile-name*]

- *profile-name* – Shows the specified file content filter profile information. If this parameter is not specified, the command will show the information of all the file content filter profiles.

Web Content

The web content function is designed to control the network behavior of visiting the webpages that contain certain keywords, and log the actions. For example, you can configure to block the access to webpage that contains the keyword "gamble", and record the access action and content in the log.

Configuring Web Content via CLI

The Web content function is mainly implemented by binding a profile to a policy rule. Once the Web content profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure Web content via CLI, take the following steps:

1. Create a Web content profile, and specify the keyword category, action and control range in the profile. You can also configure to exclude HTML tags from the Web content.
2. Bind the Web content profile to an appropriate policy rule or a zone.

Creating a Web Content Profile

You need to specify the keyword category, action and control range in the Web content profile. To create a Web content profile, in the global configuration mode, use the following command:

contentfilter-profile *profile-name*

- *profile-name* - Specifies the name of the Web content profile, and enter the configuration mode of the Web content profile. If the specified name exists, the system will directly enter

the Web content profile configuration mode. To delete the specified Web content profile, in the global configuration mode, use the command **no contentfilter-profile** *profile-name*.

Specifying the Keyword Category and Action

To specify the keyword category that will be filtered and the corresponding action, in the Web content profile configuration mode, use the following command:

keyword-category*keyword-category-name* { [**block**] [**log**] }

- *keyword-category-name* - Specifies the keyword category that will be filtered. It can be a custom keyword category or a predefined keyword category. For more information about keyword category, see Keyword Category.
- **block** – Blocks access to the website that contains the specified keyword.
- **log** – Logs access to the website that contains the specified keyword.

Repeat the command to add more keyword categories and actions.

To cancel the specified the keyword category and action, in the Web content profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Range

The system will only control the keyword within the specified websites. To specify the control range, in the Web content profile configuration mode, use the following command:

url-category {**all** | *url-category-name*}

- **all** | *url-category-name* – Specifies the URL category that will be controlled. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*). For more information about how to create a URL category, see Specifying a HTTP Proxy Server.

Repeat the command to add more URL categories.

To cancel the specified URL category, in the Web content configuration mode, use the command **no url-category** {**all** | **url-category-name**}.

Excluding HTML Tags

By default the system with Web content enabled will not only filter the content displayed in the webpage, but also filter the codes in the HTML tag. To exclude the HTML tags from the filtering, in the Web content profile configuration mode, use the following command:

exclude-html-tag

To restore to the default value, in the Web content profile configuration mode, use the following command:

no exclude-html-tag



Notes: This function only takes effect when the HTML content type is set to text/html, i.e., content="text/html".

Binding the Web Content Profile to a Policy Rule

After binding the Web content profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the Web content profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the Web content profile to a policy rule, in the policy rule configuration mode, use the following command:

contentfilter *profile-name*

- *profile-name* - Specifies the name of Web content profile that will be bound.

Binding the Web Content Profile to a Security Zone

If the Web content profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a Web content profile, and the destination zone of the policy rule is also bound with a Web content profile, then the Web content profile bound to the policy rule will be valid.

To bind the Web content profile to a security zone, in the security zone configuration mode, use the following command:

contentfilter enable *profile-name*

- *profile-name* – Specifies the name of the Web content profile that will be bound to the security zone. One security zone can only be bound with one Web content profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no contentfilter enable

Viewing Web Content Profile Information

To view the Web content profile information, in any mode, use the following command:

show contentfilter-profile [*profile-name*]

- *profile-name* – Shows the specified Web content profile information. If this parameter is not specified, the command will show the information of all the Web content profiles.

Web Posting

The web posting function is designed to control the network behavior of posting on websites and posting specific keywords, and can log the posting action and posted content. For example, forbid the users to post information containing the keyword X, and record the action log.

Configuring Web Posting via CLI

The Web posting can be configured via CLI by binding a profile to a policy rule. Once the Web posting profile is bound to a policy rule, the system will process the matching traffic according to

the profile configuration.

To configure Web posting via CLI, take the following steps:

1. Create a Web posting profile, and specify the control type, action and control range in the profile.
2. Bind the Web posting profile to an appropriate policy rule or a zone.

Creating a Web Posting Profile

You need to specify control type, action and control range in the Web posting profile. To create a Web posting profile, in the global configuration mode, use the following command:

webpost-profile *profile-name*

- *profile-name* - Specifies the name of the Web posting profile, and enter the configuration mode of the Web posting profile. If the specified name exists, the system will directly enter the Web posting profile configuration mode.

Specifying the Control Type and Action of Web Posting

You can control all the posting information, or only control the posting information with specific keyword.

To control all the posting information and specify the action, in the Web posting profile configuration mode, use the following command:

webpost all [**block**] [**log**]

- **block** – Blocks all the posting actions.
- **log** – Logs all the posting actions.

To cancel the specified control type, in the Web posting profile configuration mode, use the command **no webpost all**.

To control the posting information with specific keyword and specify the action, in the Web posting profile configuration mode, use the following command:

keyword-category*keyword-category-name* { [**block**] [**log**] }

- *keyword-category-name* - Specifies the keyword category that will be filtered. It can be a custom keyword category or a predefined keyword category. For more information about keyword category, see Keyword Category.
- **block** – Blocks postings that contain the specified keywords.
- **log** – Logs postings that contain the specified keywords.

Repeat the command to specify more keyword categories and actions.

To cancel the specified keyword category and action, in the Web posting profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Range

The system will only control the postings within the specified websites. To specify the control range, in the Web posting profile configuration mode, use the following command:

url-category {**all** | *url-category-name*}

- **all** | *url-category-name* – Specifies the URL category that will be controlled. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*. For more information about how to create a URL category, see Specifying a HTTP Proxy Server.

Repeat the command to add more URL categories.

To cancel the specified URL category, in the Web posting profile configuration mode, use the command **no url-category** {**all** | *url-category-name*}.

Binding the Web Posting Profile to a Policy Rule

After binding the Web posting profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the Web posting profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the Web posting profile to a policy rule, in the policy rule configuration mode, use the following command:

webpost *profile-name*

- *profile-name* - Specifies the name of Web posting profile that will be bound.

Binding the Web Posting Profile to a Security Zone

If the Web posting profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a Web posting profile, and the destination zone of the policy rule is also bound with a Web posting profile, then the Web posting profile bound to the policy rule will be valid.

To bind the Web posting profile to a security zone, in the security zone configuration mode, use the following command:

webpost enable *profile-name*

- *profile-name* – Specifies the name of the Web posting profile that will be bound to the security zone. One security zone can only be bound with one Web posting profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no webpost enable

Viewing Web Posting Profile Information

To view the Web posting profile information, in any mode, use the following command:

show webpost-profile [*profile-name*]

- *profile-name* – Shows the specified Web posting profile information. If this parameter is not specified, the command will show the information of all the Web posting profiles.

Email Filter

The email filter function is designed to control the emails and record logs according to the sender, receiver, email content and attachment when sending emails via SMTP, and control the receiving actions according to the email content when receiving emails via POP3 and IMAP.

Configuring Email Filter via CLI

The email filter can be configured via CLI by binding a profile to a policy rule. Once the email filter profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure email filter via CLI, take the following steps:

1. Create an email filter profile, and specify the control type, action, controlled mailbox and mailbox exception in the profile.
2. Bind the email filter profile to an appropriate policy rule or a zone.

Creating a Mail Filter Profile

You need to specify control type, action, controlled mailbox and mailbox exception in the email filter profile. To create an email filter profile, in the global configuration mode, use the following command:

mail-profile *profile-name*

- *profile-name* - Specifies the name of the email filter profile, and enter the configuration mode of the email filter profile. If the specified name exists, the system will directly enter the email filter profile configuration mode.

To delete the specified email filter profile, in the global configuration mode, use the command **no mail-profile** *profile-name*.

Specifying the Control Type

By default the email filter rule is applied to all the supported mailboxes. To specify the control type, in the email filter profile configuration mode, use the following command:

mail control {smtp | pop3 | imap}

- **smtp** - Specifies the email type that will be controlled as SMTP mails.
- **pop3**- Specifies the email type that will be controlled as POP3 mails.
- **imap**- Specifies the eamil type that will be controlled as IMAP mails.

To cancel the specified control type, in the email filter profile configuration mode, use the command **no mail control {smtp | pop3 | imap}**.

Controlling All the Emails and Specifying the Action

To control all the emails and specify the action, in the email filter profile configuration mode, use the following command:

mail any [log]

- **log** – Logs all the behaviors of sending emails.

To cancel the specified action, in the email filter profile configuration mode, use the command **no mail any**.

Specifying the Sender/Recipient and Action

To specify the sender/recipient that will be controlled and the corresponding action, in the email filter profile configuration mode, use the following command:

mail {**sender** | **recipient**} *email-address* [**block**] [**log**]

- **sender | recipient** – Specifies to control the sender or recipient.
- *email-address* – Specifies the email address of the sender or recipient.

- **block** – Blocks the emails that contain the specified sender or recipient.
- **log** – Logs the behaviors of sending emails that contain the specified sender or recipient.

Repeat the command to specify more senders/recipients and the corresponding actions.

To cancel the specified sender/recipient and action, in the email filter profile configuration mode, use the command **no {sender | recipient} email-address**.

Specifying the Keyword Category and Action

To control the email that contains the specified keyword category and the corresponding action, in the email filter profile configuration mode, use the following command:

keyword-category*keyword-category-name* { [**block**] [**log**] }

- *keyword-category-name* - Specifies the keyword category that will be filtered. It can be a custom keyword category or a predefined keyword category. For more information about keyword category, see Keyword Category.
- **block** – Blocks the emails that contain the specified keyword(s).
- **log** – Logs the behaviors of sending emails that contain the specified keyword(s).

Repeat the command to specify more keyword categories and actions.

To cancel the specified keyword category and the corresponding action, in the email filter profile configuration mode, use the command **no keyword-category** *keyword-category-name*.

Specifying the Control Type

To specify the control type, in the email filter profile configuration mode, use the following command:

mail enable {**sender** | **recipient** | **attach** | **keyword-category**}

- **sender | recipient | attach | keyword-category** – Specifies to control the **sender**, **recipient**, **attach**, **keyword-category**.

To disable the specified control type, in the email filter profile configuration mode, use the command **no mail enable** {**sender** | **recipient** | **attach** | **keyword-category**}.

Specifying the Action for other emails

Other emails refer to the emails that do not match any of the specified conditions (including sender, recipient, keyword category and attachment). To specify the action for other emails, in the email filter profile configuration mode, use the following command:

mail others [**block**] [**log**]

- **block** – Blocks other emails.
- **log** – Logs the behaviors of sending other emails.

To cancel the specified action for other emails, in the email filter profile configuration mode, use the command **no mail others**.

Specifying the Account Exception

The account exception, either a sender or a recipient account, is not controlled by the email filter rule. To specify an account exception, in the email filter profile configuration mode, use the following command:

mail whitelist *mail-address*

- *mail-address* – Specifies the email address of the exception account.

Repeat the command to specify more account exceptions.

To remove the specified account from the whitelist, in the email filter profile configuration mode, use the command **no mail whitelist** *mail-address*.

Binding the Email Filter Profile to a Policy Rule

After binding the email filter profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the email filter profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the email filter profile to a policy rule, in the policy rule configuration mode, use the following command:

mail *profile-name*

- *profile-name* - Specifies the name of email filter profile that will be bound.

Binding the Email Filter Profile to a Security Zone

If the email filter profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a email filter profile, and the destination zone of the policy rule is also bound with a email filter profile, then the email filter profile bound to the policy rule will be valid.

To bind the email filter profile to a security zone, in the security zone configuration mode, use the following command:

mail enable *profile-name*

- *profile-name* – Specifies the name of the email filter profile that will be bound to the security zone. One security zone can only be bound with one email filter profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no mail enable

Viewing Email Filter Profile Information

To view the email filter profile information, in any mode, use the following command:

show mail-profile [*profile-name*]

- *profile-name* – Shows the specified email filter profile information. If this parameter is not specified, the command will show the information of all the email filter profiles.

To view the control type information, in any mode, use the following command:

show mail-object [**mail-profile** *profile-name*]

- **mail-profile** *profile-name* – Shows the control type information of the specified email filter profile. If this parameter is not specified, the command will show all the control type information.

APP Behavior Control

The app behavior control function is designed to control and audit (record log messages) the actions of HTTP, TELNET and FTP applications, including:

- Control and audit the FTP contents and methods, including Login, Get, and Put;
- Control and audit the HTTP methods, including Connect, Get, Put, Head, Options, Post, and Trace;
- Control and audit the request content initiated by the TELNET client.

Configuring APP Behavior Control via CLI

The application behavior control function is mainly implemented by binding a profile to a policy rule. Once the application behavior control profile is bound to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration.

To configure the application behavior control via CLI, take the following steps:

1. Create an application behavior control profile, and specify the FTP, HTTP and TELNET applications that will be controlled and action in the profile.
2. Bind the application behavior control profile to an appropriate policy rule or a zone.

Creating an APP Behavior Control Profile

You need to specify the FTP, HTTP and TELNET applications that will be controlled and action in the application behavior profile. To create an application behavior control profile, in the global

configuration mode, use the following command:

behavior-profile *profile-name*

- *profile-name* - Specifies the name of the application behavior control profile, and enter the configuration mode of the profile. If the specified name exists, the system will directly enter the application behavior control profile configuration mode.

To delete the specified application behavior control profile, in the global configuration mode, use the command **no behavior-profile** *profile-name*.

Controlling FTP Application

To configure the action for the FTP method, in the application behavior control profile configuration mode, use the following command:

ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]} {**block** | **permit**} [**log**]

- **login** [*user-name*] – Controls FTP login method. To control the login method of the specified user, use parameter *user-name*.
- **get** [*file-name*] – Controls FTP Get method. To control the Get method to the specified file, use parameter *file-name*.
- **put** [*file-name*] – Controls FTP Put method. To control the Put method to the specified file, use parameter *file-name*.
- **block | permit** – Specifies the action. It can be **block**or **permit**.
- **log** – Logs the FTP method.

To cancel the specified action for the FTP method, in the application behavior control profile configuration mode, use the following command:

no ftp {**login** [*user-name*] | **get** [*file-name*] | **put** [*file-name*]}

Controlling HTTP Application

To configure the action for the HTTP method, in the application behavior control profile configuration mode, use the following command:

http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]} {**block** | **permit**} [**log**]

- **connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*] – Controls the specified HTTP method. To control the HTTP method to the specified host, use parameter host.
- **block | permit** – Specifies the action. It can be block or permit.
- **log** – Logs the HTTP method.

To cancel the specified action for the HTTP method, in the application behavior control profile configuration mode, use the following command:

no http {**connect** | **delete** [*host*] | **get** [*host*] | **head** [*host*] | **options** [*host*] | **post** [*host*] | **put** [*host*] | **trace** [*host*]}

Controlling TELNET Application

To control the request initiated by the TELNET client, in the application behavior control profile configuration mode, use the following command:

telnet keyword-category*keyword-category-name*{ [**block**] [**log**] }

- *keyword-category-name* - Specifies the keyword category that will be filtered. It can be a custom keyword category or a predefined keyword category. For more information about keyword category, see Keyword Category.
- **block** – System will block the content which matches the specifies keyword category.
- **log** – System will record logs when the content matches the specifies keyword category.

In the application behavior control profile configuration mode, use the command **no telnetkeyword-category***category-name* to cancel the controlling of TELENT content.

Binding the APP Behavior Control Profile to a Policy Rule

After binding the application behavior control profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the application behavior control profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the application behavior control profile to a policy rule, in the policy rule configuration mode, use the following command:

behavior *profile-name*

- *profile-name* - Specifies the name of application behavior control profile that will be bound.

Binding the APP Behavior Control Profile to a Security Zone

If the application behavior control profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a application behavior control profile and the destination zone of the policy rule is also bound with a application behavior control profile, then the application behavior control profile bound to the policy rule will be valid.

To bind the application behavior control profile to a security zone, in the security zone configuration mode, use the following command:

behavior enable *profile-name*

- *profile-name* – Specifies the name of the application behavior control profile that will be bound to the security zone. One security zone can only be bound with one application behavior control profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no behavior enable

Viewing APP Behavior Control Profile Information

To view the application behavior control profile information, in any mode, use the following command:

show behavior-profile [*profile-name*]

- *profile-name* – Shows the specified application behavior control profile information. If this parameter is not specified, the command will show the information of all the application behavior control profiles.

To view the object information in the application behavior control profile, in any mode, use the following command:

show behavior-object [**behavior-profile** *profile-name*]

- **behavior-profile** *profile-name* – Shows the object information of the specified application behavior control profile. If this parameter is not specified, the command will show the object information of all the application behavior control profiles.

File Filter

The file filter function checks the files transported through HTTP, FTP, SMTP, IMAP, POP3 , SMBprotocols and control them according to the file filter rules.

- Be able to check and control the files transported through GET and POST methods of HTTP, FTP, SMTP, IMAP, POP3 and SMB. If SMB protocol type is used, the system supports the detection and controlling of files in break-point resumption scenarios.
- Support file size, file type, and file name filter conditions.
- Support block, log, and permit actions.

If IPv6 is enabled, File Filter function supports file detection and behavior control based on IPv6. For more information about how to enable IPv6, see IPv6.

The filter conditions supported by each protocol area shown below:

	HTTP		FTP	SMTP	POP3
	GET	POST			
File size	√	√	√	√	√
File type	√	√	√	√	√
File name	√	√	√	√	√

Configuring File Filtering

After bind the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile. The system also supports binding the file filter profile to a ZTNA policy to perform file detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To configure file filter via CLI, take the following steps:

- Create a file filter profile, and configure the file filter rule.
- Specify the protocol to be checked, the filter condition, and the actions in the file filter rule.
- Bind the file filter profile to an appropriate policy rule.

Creating a File Filter Profile

To create a file filter profile, in the global configuration mode, use the following command:

dlp-profile *profile-name*

- *profile-name* - Specifies the name of the file filter profile, and enter the configuration mode of the file filter profile. If the specified name exists, the system will directly enter the file filter profile configuration mode.

To delete the file filter profile, use the **no dlp-profile** *profile-name* command.

Creating a File Filter Rule

Use the file filter rule to specify the protocol that you want to check, the filter conditions, and the actions. To create a filter rule, in the file filter profile configuration mode, use the following command:

filter id *id-number*

- **id** *id-number* – Specifies the ID of the created file filter rule, and enter the configuration mode of the file filter rule. If the specified ID exists, the system will directly enter the file filter rule configuration mode. The ID value ranges from 1 to 8, you can specify up to 8 file filter rules.

The file must match all filter conditions in a file filter rule, and the system will perform corresponding control actions.

Use the **no filter id** *id-number* to delete the specified filter id.

Specifying the File Size

When the size of the transported file reaches the specied file size, the system will trigger the actions. To specify the file size, in the file filter rule configuration mode, use the following command:

file-size-threshold *size-value*

- *size-value* – Specify the file size. The value ranges from 1 to 512,000. The unit KB.

To cancel the file size settings, use the **no file-size-threshold** command.

Specifying the File Name

When the name of the transported file matches the specified file name, the system will trigger the actions. To specify the file name, in the file filter rule configuration mode, use the following command:

file-name*name*

- *name* – Specify the file name. The value ranges from 1 to 255 characters. You can specify up to 32 file names. If there is no wildcard in this specified name, then the transported file whose name is the same as the specfied name will trigger the actions. If the asterisk (*) appears in this specified name, then the transported file whose name contains the part that followes the asterisk will trigger the actions.

Use the **no file-name** *name* command to cancel the settings.

Configuring the Description

To add the description to a file filter profile, in the file filter profile configuration mode, use the following command:

description *description*

- *description* – Enters the description.

Use **no description** to delete the description.

Specifying the Protocol

The file filter function will check the files transpored through the protocols you specified. To specify the protocol, in the file filter rule, use the following command:

protocol-type { **all** | **http-get** | **http-post** | **ftp** | **smtp** | **imap** | **pop3**| **smb-upload** | **smb-download**}

- **all | http-get | http-post | ftp | smtp | pop3| smb-upload | smb-download** – Specifies the protocols. **all**represents to check the files transported through the GET and POST methods of HTTP, FTP, SMTP， POP3 and SMB. **http-get**represents to check the files transported through the GET method of HTTP. **http-post**represents to check the files transported through the POST method of HTTP. **ftp**represents to check the files transported through FTP. **smtp**represents to check the files transported through SMTP. **imap**represents to check the files transported through IMAP. **pop3**represents to check the files transported through POP3.**smb-upload**represents to check the files transported through the upload request of SMB. **smb-download** represents to check the files transported through the download request of SMB.

To cancel the settings, use the **no protocol-type**command.

Specifying the File Type

When the transmitted file is a particular type, the system will trigger the actions. The file filter function can identify the following file types:

7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV, MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, BZIP2, UNKNOWN

To specify the file type, in the file filter rule configuration mode, use the following command:

file-type *type*

- *type* - Specify the file type. The type names are described above. You can specify one type once and repeat this command to specify multiple types. To control the file type that not supported, you can use the UNKNOWN type.

Use the **no file-type** *type*command to cancel the settings.

Specifying the Action

Specify the action to control the files that matches the filter conditions. To specify the action, in the file filter rule configuration mode, use the following command:

action { **log** | **block** }

- **block** – block represents to block the uploading or downloading of the file that matches the filter conditions.
- **log** – Permit the transporting of the file that matches the filter conditions with logs.

Use the **no action**command to cancel the settings.

Binding the File Filter Profile to a Policy Rule

After binding the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile. To bind the file filter profile to a policy rule, enter the policy rule configuration mode in two steps.

In the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the file filter profile to a policy rule, in the policy rule configuration mode, use the following command:

dlp-profile *profile-name*

- *profile-name* - Specifies the name of file filter profile that will be bound.

To cancel the binding, use the **no dlp-profile**command.s

Viewing File Filter Profile

To view the file filter profile, in any mode, use the following command:

show dlp-profile *profile-name*

- *profile-name* – Shows the specified file filter profile.

Configuring Decompression Control Function

After configuring the decompression control function, StoneOS can decompress the transmitted compressed files, and can handle the files that exceed the max decompression layer as well as the encrypted compressed files in accordance with the specified actions. This function supports to decompress the files in type of RAR, ZIP, TAR, GZIP, and BZIP2.



Tips: The decompression control function are effective for both the file filter function and the Anti-Virus function. For the Anti-Virus function, refer to "Anti-Virus" on Page 2114.

Enabling / Disabling Decompression Function

StoneOS can decompress the transmitted compressed files. The decompression function is enabled by default. To enable or disable the decompression function, in the global configuration mode, use the following command:

decompression {**enable** | **disable**}

- **enable** | **disable** - Enable(**enable**) or (**disable**) the decompression function.

Specifying the Maximum Decompression Layer

By default, StoneOS can check the files of up to 5 decompression layers. To configure the maximum decompression layers and the actions for the compressed files that exceed the max decompression layer, in the global configuration mode, use the following command:

decompression max-recursion *number* **exceed-action** {**log-only** | **reset-conn**}

- *number* - Specifies the decompression layer. The value range is 1 to 5. The default value is 1.
- **log-only** | **reset-conn** - Specifies the action for the compressed files that exceed the maximum decompression layer. The available options include (**log-only**) and (**reset-conn**). The default action is **log-only**.

To restore to the default value, in the global configuration mode, use the following command:

no decompression max-recursion



Notes: For compressed files containing docx, pptx, xlsx, jar, and apk formats, when action is specified as **reset-conn**, the maximum compression layers should be added one more layer to prevent download failure.

Specifying an Action for Encrypted Compressed Files

By default, system not take any actions against the files. To specify an action for encrypted compressed files, in the global configuration mode, use the following command:

decompression encryption-file action {**log-only** | **reset-conn**}

- **log-only** | **reset-conn** – Specifies the action for the encrypted compressed files. The available options include (**log-only**) and (**reset-conn**).

Use the **no decompression encryption-file action** command to restore to the default value.

Viewing Decompression Control Configuration Information

To view the decompression control configuration information, in any mode, use the following command:

show decompression configuration

Network Behavior Record

Network behavior record function audits the IM applications behaviors and record log messages for the access actions, includes:

- Audits the QQ, wechat and sinaweibo user behaviors.
- Log the access behaviors.

If IPv6 is enabled, Network behavior record function supports IM application behavior auditing and behavior control based on IPv6. For more information about how to enable IPv6, see IPv6.

Configuring Network Behavior Recording via CLI

The Network behavior record can be configured via CLI by binding a profile to a policy rule. Once the Network behavior record profile is bound to a policy rule, the system will process the matching traffic according to the profile configuration.

To configure Network behavior record via CLI, take the following steps:

1. Create a Network behavior record profile, and specify the IM application type, timeout and record log messages for the access actions in the profile.
2. Bind the Network behavior record profile to an appropriate policy rule or a zone.

Creating a Network Behavior Record Profile

You need to specify the the IM application type, timeout and record log messages for the access actions in the network behavior record profile. To create a NBR profile, in the global configuration mode, use the following command:

nbr-profile *profile-name*

- *profile-name* - Specifies the name of the NBR profile, and enter the configuration mode of the NBR profile. If the specified name exists, the system will directly enter the NBR profile configuration mode.

To delete the specified NBR profile, in the global configuration mode, use the command **no nbr-profile** *profile-name*.

IM Audit

The system can identify the UID (unique identification) from the IM applications traffic, as well as the related IP address, MAC address, and occurred time. Then it records the corresponding logs in IM logs.

To enable this function, in the NBR configuration mode, use the following command:

im {**qq** | **wechat** | **sinaweibo**} **log enable**

- **qq** - Specifies the audits of QQ.
- **wechat** - Specifies the audits of WeChat.
- **sinaweibo** - Specifies the audits of sina Weibo.

To disable this function, in the NBR configuration mode, user the **no im** {**qq** | **wechat** | **sina-weibo**} **log enable**command.



Notes: To configuring the IM auditing function, you need to use the **application-identify**command to enable the application identification function of the zone bound by the rule.

Configuring Timeout Value

During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs. To configure the timeout value, in the NBR configuration mode, use the command below:

im {**qq** | **wechat** | **sinaweibo**} **timeout** *value*

- **qq** | **wechat** | **sinaweibo** – Specifies the IM user type.
- **value** – Specifies the timeout value. The unit is minute. The default value is 20.

In the NBR configuration mode, use **no im** {**qq** | **wechat** | **sinaweibo**} **timeout**command to restore to the default value.

Recording Web Surfing Log

In the NBR profile configuration mode, you can use the following command to enable the system to record the web surfing log:

web-surfing-record method [**get** | **get-post** [**post-content**] | **post** [**post-content**]]

- **get** - Records the web surfing log using the GET method.
- **get-post** - Records the web surfing log using the GET and POST methods.
- **post** - Records the web surfing log using the POST method.
- **post-content** – Records the POST content.

In the NBR profile configuration mode, use the following command:

no web-surfing-record

Binding the NBR Profile to a Policy Rule

After binding the NBR profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the NBR profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the NBR profile to a policy rule, in the policy rule configuration mode, use the following command:

nbr *profile-name*

- *profile-name* - Specifies the name of NBR profile that will be bound.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. After then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule. For more information, see the "Policy".

Binding the NBR Profile to a Security Zone

If the NBR profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with a NBR profile, and the destination zone of the policy rule is also bound with a NBR profile, then the NBR profile bound to the policy rule will be valid.

To bind the NBR profile to a security zone, in the security zone configuration mode, use the following command:

nbr enable *profile-name*

- *profile-name* – Specifies the name of the NBR profile that will be bound to the security zone. One security zone can only be bound with one NBR profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no nbr enable

Viewing NBR Profile Information

To view the NBR profile information, in any mode, use the following command:

show nbr-profile [*profile-name*]

- *profile-name* – Shows the specified NBR profile information. If this parameter is not specified, the command will show the information of all the NBR control profiles.

Log Management

The Data Security logs (File Filter logs, Content Filter logs, Network Behavior Record logs) of system provide comprehensive records of users' network behaviours, including visiting URLs, sending emails, content of the emails and the attachments, Web postings, IM and chatting content, and FTP/HTTP methods, etc. These records are the data source for HSM (Hillstone Security ManagementTM) to provide log query, statistics, audit, analysis and other services. For more information, see Hillstone Security Management help document.

Log Severity and Format

The Data Security logs belong to the severity of Information.

To facilitate the access and analysis of the Data Security logs, StoneOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**. See the example below.

2017-06-17 11:34:27, WEBPOST: IP 100.100.10.55 (-) vrouter trust-vr, url, content_type content_type, action action, reason reason, rule rule, character set character-set, content

Output Destinations

Log files can be sent to the following destinations. You can specify one of them at your own choice:

- Console - Console port of the device.
- Buffer - Memory buffer.
- Syslog Server - Sends logs to a UNIX or Windows Syslog Server.

Configuring Log

The configurations of Data Security logs include enabling/disabling Data Security log, specifying the output destination, exporting and clearing logs. For more information about the configurations, see the table below.

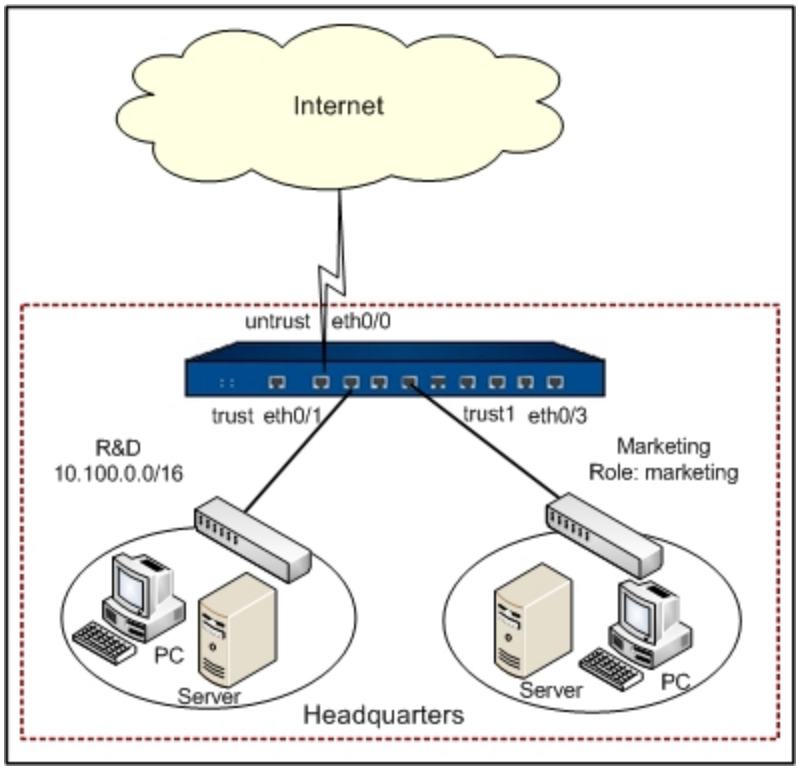
Configuration	CLI
To enable/disable the log function	In the global configuration mode, use the following command: • Enable: **logging data-security [dlp | cf | nbr] on** • Disable:**no logging data-security[dlp | cf | nbr] on**
To record the login/-logout log messages of IM	In the NBR profile configuration mode, use the following command: • To record the login/logout log messages of QQ, WeChat, and sinaWeibo:**im {qq | wechat | sinaweibo} log enable** • To disable the recording of the login/logout log messages of QQ, WeChat, and sinaWeibo:**no im {qq | wechat | sinaweibo} log enable**
To specify the output destination	In the global configuration mode, use the following command: • To Console or syslog server:**logging data-security [dlp | cf | nbr] to {console | syslog[binary-format [distributed [src-ip-hash | round-robin]] | custom-format] }** • To buffer:**logging data-security [dlp | cf | nbr] to buffer** [**size** *buffer-size*]
To view the data security logs	**show logging data-security [dlp | cf | nbr]**
To clear data security logs	**clear logging data-security [dlp | cf | nbr]**

Data Security Configuration Examples

This section describes five Data Security configuration examples, including:

- Example 1: URL filter
- Example 2: Web content
- Example 3: Web posting
- Example 4: Mail filter
- Example 5: Network behavior record

The network topology is shown in the figure below. Hillstone device works as the gateway of an enterprise. Ethernet0/0 connects to Internet and belongs to the untrust zone; ethernet0/1 connects to the Intranet of R&D Department and belongs to the trust zone; ethernet0/3 connects to the Intranet of Marketing Department and belongs to the trust1 zone.





Tip:

- Do not use CLI and WebUI to configure Data security at the same time. Choose only one method.
- For more information about how to configure the interface, security zone and log, see other related chapters. This section only describes Data security configuration.

Example1: URL Filter Configuration

The goal is to configure a URL filter rule that forbids the members in the R&D department (the network segment is 10.100.0.0/16) to access the news websites (except for www.abc.com) and an entertainment websites www.bcd.com during office hours (09:00 to 18:00, Monday to Friday), also forbids searching the keyword ef, and logs the access and search attempts.

Preparations

Before configuring the URL filter function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure a schedule:

```
hostname(config)# schedule workday
hostname(config-schedule)# periodic weekdays 09:00 to 18:00
hostname(config-schedule)# exit
hostname(config)#
```

Step 2: Configure the user-defined URL category named bcd that contains www.bcd.com:

```
hostname(config)# url-category bcd
hostname(config)# url www.bcd.com url-category bcd
```

Step 3: Configure the keyword category named url-keyword:

```
hostname(config)# category url-keyword
hostname(config)# keyword ef simple category url-keyword
```

Step 4: Configure the URL filter profile named urlcontrol:

```
hostname(config)# url-profile urlcontrol
hostname(config-url-profile)# url-category News block log
hostname(config-url-profile)# keyword-category url-keyword block log
hostname(config-url-profile)# exit
hostname(config)#
```

Step 5: Bind the URL filter profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# url urlcontrol
hostname(config-policy-rule)# src-ip 10.100.0.0/16
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# schedule workday
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 6: Configure a bypass domain that excludes www.abc.com from control:

```
hostname(config)# address abc
hostname(config-addr)# host www.abc.com
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to abc service any permit
```

```
hostname(config-policy)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, during the office hours, the member in the R&D department cannot access the news websites (except for www.abc.com) and www.b-cd.com, and cannot search the keyword ef. The system will log the access and search attempts.

Example 2: Web Content Configuration

The goal of Exmaple 2 is to configure a Web content rule that forbids the members in the R&D department to access the web pages containing the keywords X and Y (except for the member a. The network segment of the R&D department is 10.100.0.0/16), and logs the access attempts.

Preparations

Before configuring the Web content function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure the keyword category named web-keyword:

```
hostname(config)# contentfilter
hostname(config-contentfilter)# category web-keyword
hostname(config-contentfilter)# keyword X simple category stock-keyword
hostname(config-contentfilter)# keyword Y simple category stock-keyword
hostname(config-contentfilter)# exit
hostname(config)#
```

Step 2: Configure the Web content profile named webkeyword-control:

```
hostname(config)# contentfilter-profile webkeyword-control
hostname(config-contentfilter-profile)# keyword-category web-keyword block log
```

```
hostname(config-contentfilter-profile)# exit
hostname(config)#
```

Step 3: Bind the Web content profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# contentfilter webkeyword-control
hostname(config-policy-rule)# src-ip 10.100.0.0/16
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 4: Set the user exception that excludes member a from control:

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user a
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to any from-zone trust to-zone untrust service any permit
Rule id 3 is created
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# user local a
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the members in the R&D department cannot access web pages containing the keyword X or Y. And also, the system will log the access attempts.

Example 3: Web Posting Configuration

The goal is to configure a Web posting rule that logs the actions of posting information with keyword X on the website www.abc.com.

Preparations

Before configuring the Web posting function, finish the following preparations first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

Configuration Steps on CLI

Step 1: Configure the keyword category named reactionary-keyword:

```
hostname(config)# contentfilter
hostname(config-contentfilter)# category reactionary-keyword
hostname(config-contentfilter)# keyword X simple categoryreactionary-keyword
hostname(config-contentfilter)# exit
hostname(config)#
```

Step 2: Configure the use-defined URL category named abc that contains www.abc.com:

```
hostname(config)# url-category abc
hostname(config)# url www.abc.com url-category abc
```

Step 3: Configure the Web posting profile named webpost-control:

```
hostname(config)# webpost-profile webpost-control
hostname(config-webpost-profile)# keyword-category reactionary-keyword log
hostname(config-webpost-profile)# url-category abc
hostname(config-webpost-profile)# exit
hostname(config)#
```

Step 4: Bind the Web posting profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# webpost webpost-control
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the system will record log messages when someone is posting information with keyword X in the website www.abc.com.

Example 4: Email Filter Configuration

The goal is to forbid the employees to send emails through QQ mailbox, and record log messages when any is sending emails through other mailboxes.

Configuration Steps on CLI

Step 1: Configure the Email filter profile named mailfilter:

```
hostname(config)# mail-profile mailfilter
hostname(config-mail-profile)# mail sender *@qq.com block
hostname(config-mail-profile)# mail others log
hostname(config-mail-profile)# mail control all
hostname(config-mail-profile)# exit
hostname(config)#
```

Step 2: Bind the Email filter profile to a policy rule:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# mail mailfilter
hostname(config-policy-rule)# dst-zone untrust
```

```
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the employees cannot send emails through QQ mailbox, and all the sending actions through other mailboxes will be logged.

Example 5: Network Behavior Record Configuration

The goal is to configure a network behavior record rule that records the WeChat login/logout log messages of the Marketing department members (the role is marketing).

Configuration Steps on CLI

Step 1: Configure the user, role, and role mapping rule (take user1 as the example):

```
hostname(config)# aaa-server local
hostname(config-aaa-server)# user-group usergroup1
hostname(config-user-group)# exit
hostname(config-aaa-server)# user user1
hostname(config-user)# password 123456
hostname(config-user)# group usergroup1
hostname(config-user)# exit
hostname(config-aaa-server)# exit
hostname(config)# role marketing
hostname(config)# role-mapping-rule role-mapping1
hostname(config-role-mapping)# match user-group usergroup1 role marketing
hostname(config-role-mapping)# exit
hostname(config)#
```

Step 2: Configure the role mapping rule for the local AAA server:

```
hostname(config)# aaa-server local
```

```
hostname(config-aaa-server)# role-mapping-rule role-mapping1
hostname(config-aaa-server)# exit
hostname(config)#
```

Step 3: Configure interfaces and zones:

```
hostname(config)# internet ethernet0/3
hostname(config-if-eth0/3)# zone trust1
hostname(config-if-eth0/3)# ip address 192.168.1.1/16
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 66.1.200.1/16
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 4: Configure WebAuth and DNS policy:

```
hostname(config)# webauth
hostname(config-webauth)# enable
hostname(config-webauth)# protocal http
hostname(config-webauth)# exit
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service any webauth local
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-ip 192.168.1.1/16
hostname(config-policy-rule)# src-zone trust1
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# role unknown
```

```
hostname(config-policy-rule)# exit
hostname(config-policy)# rule from any to any service dns permit
Rule id 2 is created
hostname(config-policy)# rule id 2
hostname(config-policy-rule)# src-zone trust1
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 5: Configure the policy rule:

```
hostname(config-policy)# rule from any to any service any permit
Rule id 3 is created
hostname(config-policy)# rule id 3
hostname(config-policy-rule)# src-zone trust1
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# role marketing
hostname(config-policy-rule)# exit
hostname(config)#
```

Step 6: Configure the NBR profile named marketim:

```
hostname(config)# nbr-profile marketim
hostname(config-nbr-profile)# im wechat log enable
hostname(config-nbr-profile)# exit
hostname(config)#
```

Step 7: Control the NBR rule named imcontrol:

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
hostname(config-policy-rule)# im marketim
```

```
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# role marketing
hostname(config-policy-rule)# exit
hostname(config)#
```

After the configuration, modify the priority of the policy rule to assure the traffic matching to the configured rule is prioritized. When the rule takes effect, the system will log the WeChat login/-logout actions of the Marketing department members.

Object Configuration

Objects mean the items referenced during Content Filter profiles and URL Filtering profiles configurations, including:

- Predefined URL database
- User-defined URL database
- URL lookup
- Keyword category
- Warning page
- Bypass domain
- User exception
- First Access of Uncategorized URL

Predefined URL Database

System ships with a license controlled predefined URL database. The predefined URL database will not take effect on the supported platforms until a URL license is installed.

Predefined URL database provides URL categories for the configurations of URL filter, web content, and web posting. The predefined URL database is divided into 39 categories, with a total number of URLs up to 20 million.

Updating the Predefined URL Database

By default, the system updates the predefined URL database every day. You can change the update parameters according to your own requirements. Hillstone provides two default URL database update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can update your URL database online or manually. For more information about how to configure the predefined URL database, see the following table:

Configuration	CLI
Specifying the update mode	In the global configuration mode, use the following command: **url-db update mode** {**auto** | **manual**}
To configure an update protocol (HTTPS by default)	In the global configuration mode, use the following command: • Specifying the update protocol: **url-ub update protocol HTTP** • Restoring to the default: **no url-ub update protocol HTTP**
Configuring the update server	In the global configuration mode, use the following command: **url-db update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*]
Specifying the update schedule	In the global configuration mode, use the following command: **url-db update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]
Updating now	In the execution mode, use the following command: **exec url-db update**
Updating manually	In the execution mode, use the following command: **import url-db from** {**ftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] | **tftp server** *ip-address* | **usb0** | **usb1**} *file-name* **Note**: Non-root VSYS does not support this command.
Viewing URL DB info	**show url-db info**
Viewing URL DB update configuration	**show url-db update**

Configuration	CLI
Viewing URL statistics	**show statistics-set** *name* [{**current** | **history** | **history-max**} [**sort-by** {**up** | **down** | **item**}]]
Refreshing URL information in the local cache manually	**exec url-db refresh** {**all** | **url** *url-string*} • **all**- Refresh all URL information in the local cache. • **url** *url-string*- Refresh the specified URL in the local cache.
Viewing the count of URL statistics	**show url-db statistics**
Clearing the count of URL statistics	**clear url-db statistics**

Specifying a HTTP Proxy Server

When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the URL category signature database updating, use the following command in the global configuration mode:

url-db update proxy-server {**main** | **backup**} *ip-address port-number*

- **main** | **backup** – Use the **main**parameter to specify the main proxy server and use the **backup**parameter to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the**no url-db update proxy-server** {**main** | **backup**}command.

User-defined URL Database

Besides categories in predefined URL database, you can also customize user-defined URL categories. User-defined URL database provides URL categories for the configurations of URL filter, web content, and web posting.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL category.

For more information about user-defined URL database, see the table below:

Configuration	CLI
To create a URL category	In the global configuration mode, use the following command: **url-category** *category-name*
To add a URL entry	In the global configuration mode, use the following command: **url** *url* **url-category** *category-name*
Enable/Disable the function that the user-defined URL database supports the domain name of the HTTPS protocol	To enable this function, use the following command in the global configuration mode: **url-db-https-enable** To disable this function, use the following command in the global configuration mode: **no url-db-https-enable**
To view the status of this function, use the command in any mode:	**show url-db-https**
Import User-defined URL	**import url-file** {**custom1** | **custom2** | **custom3**} **from ftp server** *IP* [**vrouter** *vrouter-name*][**user** *username* **password** *password*] *file-name* **import url-file** {**custom1** | custom2 | custom3} from tftp

Configuration	CLI
	server IP [vrouter vrouter-name] file-name **Note**: The URL file directory is /flash/urldb/url_file. The file should be less than 1 M, and has at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address. Non-root VSYS does not support this function.
Clear User-defined URL	**exec url-file** {**custom1** | **custom2** | **custom3**} **clear**
To view URL category info	**show url-category**
To view all the user-defined URLs	**show url**

URL Lookup

You can inquire a URL to view the details by URL lookup, including the URL category and the category type. For more information about how to inquire a URL, see the table below:

Configuration	CLI
To inquire a URL	**show url** *url-string*

Configuring a URL Inquiry Server

URL inquiry server can classify an uncategorized URL (an uncatergorized URL is an address that is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Hillstone provides two default URL inquiry servers: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL inquiry servers are enabled. For more information about how to configure the URL inquiry server, see the table below:

Configuration	CLI
To enable/disable a URL	Enable: in the global configuration mode, use the following

Configuration	CLI
inquiry server	command: **url-db-query** {**server1** | **server2**} **enable** Disable: in the global configuration mode, use the following command: **no url-db-query** {**server1** | **server2**} **enable**
To configure a URL inquiry server	In the global configuration mode, use the following command: **url-db-query** {**server1** | **server2**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*] [**port** *port*] [**encrypt-type** *BCAP*]
To view the URL inquiry server info	**show url-db-query** [**server1** | **server2**]

Keyword Category

Keyword categories include predefined keyword categories and custom keyword categories, which are used in the URL filtering/File Content Filter/Web Content/Web Posting/Email filter/HTTP/FTP Control function. You can use predefined keyword categories or customize the keyword category as needed. System provides four predefined keyword categories, which are **predef_bank_card** (keyword for bank card number), **predef_email_address** (keyword for email address), **predef_cellphone_number** (keyword for mobile phone number), and **predef_mainland_id_card** (keyword for ID number), which cannot be edited or deleted.

For more information about how to customize a keyword category, see the table below:

Configuration	CLI
To create a keyword category	In the global configuration mode, use the following command: **category** *category-name*
To add a keyword entry	In the global configuration mode, use the following command:

Configuration	CLI
	keyword *keyword* {**regexp** | **simple**} **category** *category-name* [**confidence** *value*]
To commit the changes to keywords (number increase/decrease, content changes)	In the execution mode, use the following command: **exec contentfilter apply**
Show the keyword category	In any mode,use the following command: **show category** *category-name*
Show the keyword entry	In any mode,use the following command: **keyword keyword** {**regexp** | **simple**} **category** *category-name* [**confidence** *value*]

Keyword Matching Rules

System will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of times * trust value of each keyword that belongs to the category. The system will perform the following actions according to the added up value:

- If the sum is larger than or equal to the category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is a block action configured, the final action is to block;
- If more than one category action can be triggered and all the configured actions are permit, the final action is to permit.

For example, a web content rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

If the system detects one occurrence of K1 and K2 each on a web page, then C1 trust value is 20*1+40*1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the web page access is permitted.

If the system detects three occurrences of K1 and 1 occurrence of K2 on a web page, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.



Tip:

- The keyword category threshold is 100.
- To implement network behavior control accurately and effectively, you are recommended to configure multiple keywords. E.g., if only web game is configured to block accesses to web game websites, lots of other websites will be blocked together. However, if you configure web game, experience value, and equipment as the keywords, and give proper trust values to these keywords, the control accuracy will be improved. And if you can collect all the game related terms and assign a proper trust value to each term, the control will be implemented completely and precisely.

Warning Page

The warning page shows the user block information and user audit information.

Configuring Block Warning

If the network behavior is blocked by the Data Security function (URL filter, web content, web post, email filter, HTTP/FTP control), the access to the Internet will be denied. The information of Access Denied will be displayed in your browser, and some web surfing rules will be shown to you on the warning page at the same time. You can also define the displayed information by your-

self. According to the different network behaviors, the default block warning page includes the following three situations:

- Visiting a certain type of URL:



- Visiting the URL that contains a certain type of keyword category:



- Posting information to a certain type of website or posting a certain type of keywords; HTTP actions of Connect, Get, Put, Head, Options, Post, and Trace; downloading HTTP binary files, such as .bat, .com; downloading ActiveX and Java Applets.



By default the block warning function is enabled. For more information about the configuration of the function, see the table below:

Configuration	CLI
To enable/disable block warning of **URL filtering**	Enable: In the global configuration mode, use the following command: **url-block-notification** Disable: In global configuration mode, use the fol-

Configuration	CLI
	lowing command: **no url-block-notification** **Note**: If a custom warning page is configured and enabled, the custom warning page is displayed. If no custom warning page is enabled, the default predefined warning page is displayed.
To enable/disable blocking warning of **content filtering**	Enable: In the global configuration mode, use the following command: **contentfilter-block-notification** Disable: In the global configuration mode, use the following command: **no contentfilter-block-notification** **Note**: If a custom warning page is configured and enabled, the custom warning page is displayed. If no custom warning page is enabled, the default predefined warning page is displayed.
To view the status of block warning	**show block-notification** **Note**: • When the status is enabled, **block-notification enable** is displayed; • When the status is disabled, **block-notification disable** is displayed.

Configuring Audit Warning

Audit warning is disabled by default. For more information about the configurations of the function, see the table below:

Configuration	CLI
To enable/disable audit warning of **URL filtering**	Enable: In the global configuration mode, use the following command: **url-user-notification** Disable: In the global configuration mode, use the following command: **no url-user-notification** **Note**: If a custom warning page is configured and enabled, the custom warning page is displayed. If no custom warning page is enabled, the default predefined warning page is displayed.
To enable/disable audit warning of **content filtering**	Enable: In the global configuration mode, use the following command: **contentfilter-user-notification** Disable: In the global configuration mode, use the following command: **no contentfilter-user-notification** **Note**: If a custom warning page is configured and enabled, the custom warning page is displayed. If no custom warning page is enabled, the default predefined warning page is displayed.

After enabling audit warning, if your network behavior originating from one single source IP is matched to any configured network behavior control rule, you will be prompted with the audit warning page every 24 hours when visiting the web page.

Configuring the Custom Warning Page

You can customize the warning page that meets your requirements by customizing warning information and image. The custom warning page contains the following configuration:

- Entering the warning page configuration mode
- Enabling the custom warning page function
- Creating an image object
- Uploading a custom image
- Uploading a custom warning page
- Viewing information about the custom warning page
- Viewing information about the custom image
- Clearing content on the custom warning page

Entering the Warning Page Configuration Mode

To enter the warning page configuration mode, in the global configuration mode, use the following command:

warning-page

Enabling the Custom Warning Page Function

The system supports the following 6 types of custom warning pages.

- Notification about URL filtering auditing users: The page which notifies you that the URL Filtering function will scan user traffic.
- Notification about URL filtering blocking users: The page which notifies that user traffic is blocked by URL filtering.

- Malware is detected by anti-virus: The warning page that appears when malware is detected after anti-virus scans network traffic.
- Malicious website is detected by anti-virus: The warning page that appears when malicious website is detected after anti-virus scans network traffic.
- Notification about content filtering auditing users: The page which notifies you that the Content Filtering function will scan user traffic.
- Notification about content filtering blocking users: The page which notifies you that user traffic is blocked by content filtering.

To enable the function of customizing the warning page and specify the type of the custom warning page, in warning page configuration mode, use the following command:

{av-malicious-website | av-malware | contentfilter-audit-notification | contentfilter block | url-audit-notification | url-block} customized

- **av-malicious-website** - Enable the warning page of malicious website being detected by anti-virus.
- **av-malware**- Enable the warning page of malware being detected by anti-virus.
- **contentfilter-audit-notification** - Enable the warning page which notifies you that content filtering audits users.
- **contentfilter block**- Enable the warning page which notifies you that content filtering blocks users.
- **url-audit-notification** - Enable the warning page which notifies you that URL filtering audits users.
- **url-block** - Enable the warning page which notifies you that URL filtering blocks users.
- **customized** - Enable the function of customizing the warning page.

In warning page configuration mode, use the no form of the command above to disable the function of customizing the warning page of the specified types:

no {**av-malicious-website** | **av-malware** | **contentfilter-audit-notification** | **contentfilter block** | **url-audit-notification** | **url-block**} **customized**

Creating an Image Object

To create an image object, in warning page configuration mode, use the following command:

image*image-name*

- *image-name*- Specifies the name of the image object, which can be 1 to 31 characters in length.

In warning page configuration mode, use the no form of the command above to delete the image object:

no image*image-name*

Uploading a Custom Image

To upload a custom image and bind the image to a created image object, in execution mode, use the following command:

import warning-page image*image-name* **from {ftp server***ip-address* [**vrouter***vrouter-name*] [**user***user-name***password***password*] | **tftpserver***ip-address* [**vrouter***vrouter-name*]} *file-name*

- *image-name* - Specifies the name of the image object to be bound.
- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user***user-name***password***password* – Specifies the username and password of the FTP server.
- **vrouter***vrouter-name* - Specifies the VRouter to which the FTP or TFTP server belongs.
- *file-name* – Specifies the name of the custom image file to be uploaded.

After the custom image is uploaded, you can select **System** > **Warning Page Management** > **Picture Management** on the WebUI to view the uploaded image.

Uploading a Custom Warning Page

After you edit the custom warning page on your PC, you need to upload the page to the specified FTP or TFTP server to make the page take effect.

To upload the edited custom warning page from your PC, in execution mode, use the following command:

import warning-page html {**av-malicious-website** | **av-malware** | **contentfilter-audit-notification** | **contentfilter block** | **url-audit-notification** | **url-block**} **from** {**ftp server***ip-address* [**vrouter***vrouter-name*][**user***user-name***password***password*] | **tftpserver***ip-address* [**vrouter***vrouter-name*]} *file-name*

- **av-malicious-website | av-malware | contentfilter-audit-notification | contentfilter block | url-audit-notification | url-block** - Specifies the type of the custom warning page to be uploaded.
- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user***user-name***password***password* – Specifies the username and password of the FTP server.
- **vrouter***vrouter-name* - Specifies the VRouter to which the FTP or TFTP server belongs.
- *file-name* – Specifies the name of the custom warning page file to be uploaded.

After the custom warning page is uploaded, you can select **System** > **Warning Page Management** > **Page Management** on the WebUI to view the preview page of the specified type.

Viewing Information about Custom Warning Page

You can use the following command in any mode to view the status and size of the custom warning page:

show warning-page html [**av-malicious-website** | **av-malware** | **contentfilter-audit-notification** | **contentfilter block** | **url-audit-notification** | **url-block**]

Viewing Information about Custom Image

You can use the following command in any mode to view the information about the custom image, including the image type and size:

show warning-page image [*image-name*]

Clearing Content on the Custom Warning Page

Each type of custom warning pages contains the warning information that is displayed by default. To clear the custom content on the page and restore to the default content, in execution mode, use the following command:

exec warning-page {**image***image-name* | **html** {**av-malicious-website** | **av-malware** | **contentfilter-audit-notification** | **contentfilter block** | **url-audit-notification** | **url-block**}} **clear**

- **image***image-name* - Specifies the name of the image object to be cleared.
- **html** { **av-malicious-website | av-malware | contentfilter-audit-notification | contentfilter block | url-audit-notification | url-block**} - Specifies the type of the warning page whose custom content you want to clear.

After you clear the content, the warning page will be restored to the default content of the custom warning page. You can view the default content of the custom warning page by using the WebUI. To view the preview page of the specified type, select **System** > **Warning Page Management** > **Page Management**.

Configuration	CLI
To enable/disable audit warning	
Customize the audit warning information or restore	

Configuration	CLI
the audit warning information to default	
To view the user-defined audit warning information	

Bypass Domain

Regardless of the Data Security configurations (URL filter, keyword filter, web posting control, email filter, and HTTP/FTP control), requests to the specified bypass domains will be allowed unconditionally. To add a bypass domain via WebUI, take the following steps:

1. Select **Object > Data Security >Content Filter > Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Bypass Domain**. The Bypass Domain dialog appears.
3. Click **Add**. The domain name will be added to the system and displayed in the bypass domain list. Repeat Step 3 to add more bypass domains.
4. Click **OK** to save your settings.



Notes:

- Bypass domains must be precisely matched
- Bypass domains are effective to the entire system.

User Exception

The user exception function is used to specify the users who will not be controlled by Data Security, including URL filter, Web content, Web posting control, email filter, IM control, and

HTTP/FTP control. The system supports the following types of user exception: IP, IP range, role, user, user group, and address entry.

To configure user exception via WebUI, take the following steps:

1. Select **Object > Data Security > Content Filter > Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > User Exception**. The User Exception dialog appears.
3. Select the type of the user from the Type drop-down list.
4. Configure the corresponding options.
5. Click **Add**. The user will be added to the system and displayed in the user exception list.
6. Click **OK** to save the settings.



Notes: User exceptions are effective to the entire system.

First Access of Uncategorized URL

For the uncategorized URL that you visit for the first time, that is, the URL which is neither in the system's predefined URL database nor in the user-defined URL database, system will continue to query the category of the URL in the cloud. Because the query may takes a litter while, system cannot process the uncategorized URL immediately until the query result is returned.

To solve the above problem, you can specify the waiting time of query and enable the block action when waiting times out. After the waiting time of query is exceeded, system will block the access to the uncategorized URL.

Specifying the Waiting Time of Query

To specify the waiting time of query, in the global configuration mode, use the following command:

url-match-pending hold-time *time*

- *time* - Specifies the waiting time of query. The range is 0 to 5000 ms, and the default value is 0 ms.

Use the command no **url-match-pending hold-time***time* to restore the default value, which means there is no wait time limit.

Enabling/Disabling the Block Action after Waiting Timeout

To enable the block action when waiting times out, in global configuration mode, use the following command:

url-match-pending timeout-action block

Use the command **no url-match-pending timeout-action block** to disable the block action when waiting times out. After the waiting time of query is exceeded, system will continue to perform URL filtering according to the configuration of URL filtering profile.

Viewing Configurations of First Access of Uncategorized URL

To view configurations of first access of uncategorized URL and the number of blocked times, in any mode, use the following command:

show url-match-pending

URL Filtering

URL filtering is designed to control the access to some websites. This function helps you control the network behaviors in the following aspects:

- Access control to certain category of websites, such as gambling and pornographic websites;
- Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours;
- Access control to the website whose URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.

Configuring URL Filter via CLI

The URL filtering configurations are based on security zones or policies. If IPv6 is enabled, you can configure URL and keyword for both IPv4 and IPv6 address.

To configure URL filtering via CLI, take the following steps:

1. Create a URL filtering profile, and specify the URL category, URL keyword category and action in the profile.
2. Bind the URL filtering profile to a security zone or policy rule.

Creating a URL Filter Profile

You need to specify the control type of the URL filtering profile. The control types are URL category, URL keyword category, and Web surfing record. URL category controls the access to some certain category of website; URL keyword category controls the access to the website who's URL contains the specific keywords; Web surfing record logs the GET and POST methods of HTTP, and the posted content. You can select only one control type for each URL filtering profile. There is a default URL filtering profile named no-url. It can not be edited and deleted. After you bind it to a policy, URL filtering is disabled. To create a URL filtering profile, in the global configuration mode, use the following command:

url-profile *profile-name*

- *profile-name* - Specifies the name of the URL filtering profile, and enter the configuration mode of the URL filtering profile. If the specified name exists, the system will directly enter the URL filtering profile configuration mode. You can configure same URL profile name in different VSYSs.

To delete the specified URL filtering profile, in the global configuration mode, use the command **no url-profile** *profile-name*.

Specifying the URL Category and Action

To specify the URL category that will be filtered and the corresponding action, in the URL filtering profile configuration mode, use the following command:

url-category {**all** | *url-category-name*} [**block**] [**log**]

- **all** | *url-category-name* – Specifies the URL category that will be filtered. It can be all the URL categories (**all**) or a specific URL category (*url-category-name*)). You can not specify URL category of other VSYSs. For more information about how to create a URL category, see Specifying a HTTP Proxy Server.
- **block** – Blocks access to the corresponding URL category.
- **log** – Logs access to the corresponding URL category.

Repeat the command to specify more URL categories and the corresponding actions.

To cancel the specified URL category and action, in the URL filtering profile configuration mode, use the command **no url-category** {**all** | *url-category-name*}.

Inspecting SSL Negotiation Packets

For HTTPS traffic, the system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this feature is configured. Then, the system will perform URL filtering in accordance with the domain name. This feature is only applicable to the URL filtering profile whose control type is URL category. If SSL proxy is configured at the same time, SSL negotiation packets inspection method will be preferred for URL filtering. To configure the

SSL negotiation packets inspection, in the URL filtering profile configuration mode, use the following command:

ssl-inspection

In the URL filtering profile configuration mode, use**no ssl-inspection**to cancel the SSL negotiation packets inspection.

Specifying the URL Keyword and Action

To specify the URL keyword that will be filtered and the corresponding action, in the URL filtering profile configuration mode, use the following command:

keyword-category {*keyword-category-name* | **other**} [**block**] [**log**]

- *keyword-category-name* | **other** – Specifies the URL keyword that will be filtered. The URL keyword can be a specific keyword category (*keyword-category-name*) or all the other URL keyword categories that are not listed (**other**). For more information about how to create a keyword category, see Keyword Category.
- **block** – Blocks the access to the website whose URL contains the specified keyword.
- **log** – Logs the access to the website whose URL contains the specified keyword.

Repeat the command to specify more URL keywords and the corresponding actions.

To cancel the specified URL keyword and action, in the URL filtering profile configuration mode, use the command **no keyword-category** {*keyword-category-name* | **other**}.

Enabling Safe Search

Many search engines, such as Google, Bing, Yahoo!, Yandex, and YouTube, all have a "SafeSearch" setting, which can filter adult content, and then return search results at different levels based on the setting. The system supports the safe search function in the URL filtering Profile to detect the "SafeSearch" setting of search engine and perform corresponding control actions.

To enable the safe search function and specify the control action, in the URL filter profile configuration mode, use the following command:

safe-search {**block** | **enforce**}

- **block** – Specifies the action as block, When the " SafeSearch" setting of search engine is not set, users will be prevented from accessing the search page and a warning page will pop up which provides users with the link for "SafeSearch" setting.
- **enforce** – Specifies the action as execute. When the "SafeSearch" setting of search engine is not set, system will force to set it at the "strict" level.

To disable the safe search function, in the URL filter profile configuration mode, use the **no safe-search** command.



Notes:

- The safe search function only can be used in the following search engines currently: Google, Bing, Yahoo!, Yandex, and YouTube.
- The safe search function only can be used in combination with the SSL proxy function because the search engine uses the HTTPS protocol. Therefore, when the "SafeSearch" is enabled, enable the SSL proxy function for the policy rule which is bound with URL filter profile.
- To ensure the valid "SafeSearch" function of Google, you need to configure policy rules to block the UDP 80 and UD

Binding the URL Filtering Profile to a Security Zone

If the URL filtering profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the policy rule is bound with an URL filtering Profile, and the destination zone of the policy rule is also bound with an URL filtering profile, then the URL filtering profile bound to the policy rule will be valid.

To bind the URL filtering profile to a security zone, in the security zone configuration mode, use the following command:

url enable *url-profile-name*

- *url-profile-name* – Specifies the name of the URL filtering profile that will be bound to the security zone. One security zone can only be bound with one URL filtering profile.

To cancel the binding settings, in the security zone configuration mode, use the following command:

no url enable

Binding the URL Filtering Profile to a Policy Rule

After binding the URL filtering profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the URL filtering profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the URL filtering profile to a policy rule, in the policy rule configuration mode, use the following command:

url *profile-name*

- *profile-name* - Specifies the name of URL filtering profile that will be bound.



Notes: Only after cancelling the binding can you delete the URL filtering profile.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. Then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule.

To perform the URL filtering function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. The system will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the URL filtering function on the decrypted

traffic. According to the various configurations of the security policy rule, the system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled URL filtering disabled	The system decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the URL filtering function on the decrypted traffic.
SSL proxy enabled URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic.
SSL proxy disabled URL filtering enabled	The system performs the URL filtering function on the HTTP traffic according to the URL filtering profile. The system does not decrypt HTTPS traffic. If SSL inspection is not configured for the URL filtering profile, URL will not be forwarded but not filtered. If SSL inspection is configured for the URL filtering profile, URL will be filtered based on the URL filtering profile.

If the SSL proxy and URL filtering functions are enabled on a security policy rule but the control type of the selected URL filtering profile is the Web surfing record, the system will not record the GET and POST methods and the posted contents via HTTPS.

If the zone which the security policy rule binds with is also configured with URL filtering, the system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled URL filtering disabled	URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the

Policy Rule Configurations	Zone Configurations	Actions
		decrypted traffic according to the URL filtering rule of the zone.
SSL proxy enabled URL filtering enabled	URL filtering enabled	The system decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic according to the URL filtering rule of the policy rule.
SSL proxy disabled URL filtering enabled	URL filtering enabled	The system performs the URL filtering function on the HTTP traffic according to the URL filtering rule of the policy rule. The system does not decrypt HTTPS traffic. If SSL inspection is not configured for the URL filtering profile, URL will not be forwarded but not filtered. If SSL inspection is configured for the URL filtering profile, URL will be filtered based on the URL filtering profile.

Viewing URL Filtering Profile Information

To view the URL filtering profile information, in any mode, use the following command:

show url-profile [*profile-name*]

- *profile-name* – Shows the specified URL filtering profile information. If this parameter is not specified, the command will show the information of all the URL filtering profiles.

URL Blacklist/Whitelist

You can further control the access to some websites by configuring URL blacklist/whitelist.

- After the URL blacklist is configured, when you send an access request to the specified URL in the blacklist, the system will block the request.
- After the URL whitelist is configured, when you send an access request to the specified URL in the whitelist, system will not perform URL filtering for the access request and let the request pass.
- The URL blacklist, the URL whitelist and the URL filtering profile all configured with URL categories, the matching priority for URL category filtering is: the URL blacklist > the URL whitelist > the URL filtering profile.



Notes:

- An URL category can only be referenced by an object (URL blacklist, URL whitelist or URL filtering profile). For example, when the URL category "Advertisement" has been added to the URL blacklist, this URL category cannot be added to the URL whitelist, and it will not be referenced in the URL filtering profile.
- Non-root VSYS does not support the URL blacklist\whitelist function, and the URL blacklist/whitelist configuration under root VSYS does not take effect and has no effect on non-root VSYS.

Configuring the URL Blacklist

The URL blacklist is used to filter URL access requests that are not allowed. After the URL category is added to the URL blacklist, the HTTP/HTTPS traffic that hits the blacklist of the URL is blocked.

To configure the URL blacklist, you need to enter the URL blacklist configuration mode. Enter the URL blacklist configuration mode. In global configuration mode, use the following command:

url-blacklist

To add the URL category to the URL blacklist, in the URL blacklist configuration mode, use the following command:

url-category *url-category-name*

- *url-category-name*- Specifies the URL category to add to the URL blacklist.

To delete the URL category from the URL blacklist, in the URL blacklist configuration mode, use the following command:

no url-category *url-category-name*

Configuring the URL Whitelist

The URL whitelist is used to filter the allowed URL access requests. After the URL category is added to the URL whitelist, the HTTP/HTTPS traffic hitting the URL whitelist is processed and not controlled by the URL filtering profile.

To configure the URL whitelist, you need to enter the URL whitelist configuration mode. Enter the URL whitelist configuration mode. In global configuration mode, use the following command:

url-whitelist

To add the URL category to the URL whitelist, in the URL whitelist configuration mode, use the following command:

url-category *url-category-name*

url-category-name- Specifies the URL category to add to the URL whitelist.

To delete the URL category from the URL whitelist, in the URL whitelist configuration mode, use the following command:

no url-category *url-category-name*

Viewing the URL Blacklist Information

To view URL blacklist information, in any mode, use the following command:

show url-blacklist

Viewing URL Whitelist Information

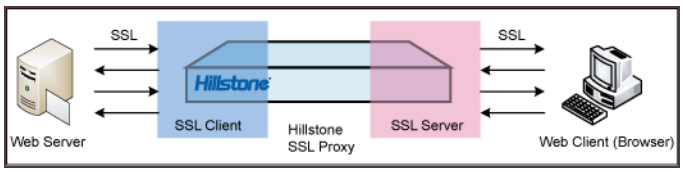
To view URL whitelist information, in any mode, use the following command:

show url-whitelist

SSL Proxy

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificate to the client's Web browser. During the process, the device acts as an SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are three work modes. For the first scenario, the SSL proxy function can work in the "Client Inspection - Proxy" mode ; for the second scenario, the SSL proxy function can work in the "Server Inspection - Offload" mode and "Server Inspection - Proxy" mode.

When the SSL proxy function works in the "Client Inspection - Proxy" mode, it can perform the SSL proxy on specified websites.

For the websites that do not need SSL proxy, it dynamically adds the IP address and port of the websites to a bypass list, and the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be bypassed.

For the websites proxied by the SSL proxy function, the device will check the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS/POP3S/SMTPS/IMAPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list, and the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be bypassed.

The device will decrypte the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that are not blocked or bypassed.

When the SSL proxy function works in the "Server Inspection - Offload" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

When the SSL proxy function works in the "Server Inspection - Proxy" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and re-encrypt the traffic and send it to the Web server.

You can integrate SSL proxy function with the followings:

- Integrate with the application identification function. Devices can decrypte the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.
- Integrate with the Web content function, Web post function, and email filter function. Devices can audit the actions that access the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS website.

- Integrate with AV, IPS, Antispam, Sandbox , Content Filter , File Filter and URL. Devices can perform the AV protection, IPS protection, Sandbox protection, Content filter , File filter, File content cilter and URL filter on the decrypted HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, can perform the File content filter, Web content, Web posting, HTTP/FTP control on the decrypted HTTPS traffic, and can perform the Email filter on the decrypted POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.

Working as Gateway of Web Clients

To implement SSL proxy, you need to bind an SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, the system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate and import a device certificate to the Web browser.
2. Configure an SSL proxy profile, including the following items: choose the work mode, configure the actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when its SSL negotiation matches the item in the checklist, enable the aduit warning page, and so on.
3. Bind an SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate
- Obtain the CN value of the website certificate
- Import a device certificate to a Web browser

Specifying the PKI Trust Domain of Device Certificate

By default, the device will use the PKI trust domain of trust_domain_ssl_proxy_2048 to re-sign the Web server certificate, i.e. SSL proxy certificate. You can change the PKI trust domain by using the following command in the global configuration mode:

sslproxy trust-domain *trust-domain-name*

- *trust-domain-name* – Select a trust domain. You can select trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048. The trust domain of trust_domain_ssl_proxy uses RSA and the modulus is 1024; the trust domain of trust_domain_ssl_proxy_2048 uses RSA and the modulus is 2048.

To restore the trust domain settings to the default one, use the **no sslproxy trust-domain**.

Obtaining the CN Value

To get the CN value in the Subject field of the website certificate, take the following steps (take www.gmail.com as the example):

1. Open the Web browser (Google Chrome is used in this example), and visit https://www.gmail.com.
2. Click the **Security Report** button next to the URL.



3. In the pop-up dialog, click **View certificates**.
4. In the Details tab, click **Subject**. You can view the CN value in the text box.

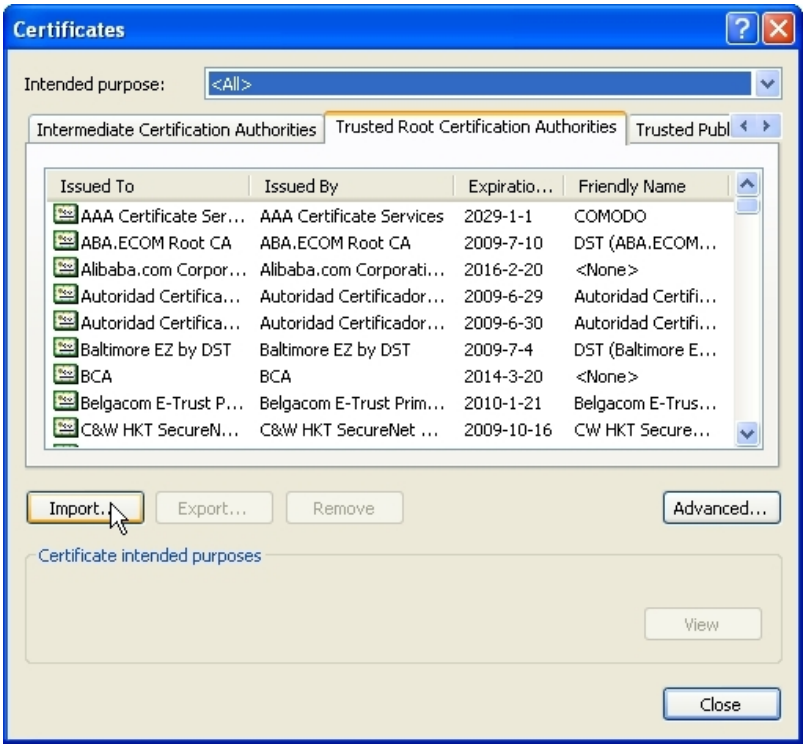
Importing a Device Certificate to a Web Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser. To import a device to the client browser, take the following steps:

1. Export the device certificate to your local PC. Use the following command:

```
CLI:

export pki trust-domain-name {cacert | cert | pkcs12 password | pkcs12-der password} to {ftp server ip-address [user user-name password password] | tftp server ip-address | usb0 | usb1} [file-name]

Example:

hostname# export pki trust_domain_ssl_proxy cacert to tftp server 10.10.10.1

Export ok,target filename 1252639478

hostname#
```

2. Import the certificate (before importing the certificate, change the extension name of the certificate to .crt) to the web browser (take Google Chrome as the example). Start Google Chrome, from the toolbar, select **Settings > Privacy and security > Security > Manage certificates**. In the Certificates dialog, click the **Trusted Root Certification Authorities** tab, and then click **Import**, as shown in the figure below. Import the certificate as prompted by the Certificate Import Wizard.



If the encryption standard you select in step 1 is pkcs12 or pkcs12-der, you need to enter the certificate password in the pop-up window when importing the certificate to the web browser. The password is the one that you specified in the **pkcs12** *password* | **pkcs12-der** *password*command.

Configuring an SSL Proxy Profile

Configuring an SSL proxy profile includes the following items: configure the session reuse function, choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when its SSL negotiation matches the item in the checklist, enable the aduite warning page, and so on. The system supports up to 32 SSL proxy profiles. To create an SSL proxy profile, use the following command in the global configuration mode:

sslproxy-profile *profile-name*

- *profile-name* - Specifies the name of the SSL proxy profile and enter the SSL proxy profile configuration mode. If the name already exists, the system will enter the SSL proxy profile configuration mode directly.

To delete an SSL proxy profile, use the **no sslproxy-profile** *profile-name*.

Configuring the Session Reuse Function

With the Session Reuse function enabled, when the client initiates an SSL connection request to the server, the server checks whether the request connection has been created, and if so, the previous SSL connection is resumed without the need for a complete TLS handshake, thereby reducing the time consumption during the handshake process.

The system supports the following two session reuse methods:

- Ticket: Select the check box to enable the session reuse based on session ticket. In this method, when an SSL connection is established between a client and a server for the first time, the server encapsulates the symmetric key and other status information generated in the TLS handshake into a session ticket which is encrypted, and then forwards the session ticket to the client, which is stored in the cache of the client. When the client initiates the SSL connection again (or initiates the connection request again after disconnection), the session ticket will first be sent to the server for decryption. If the server successfully decrypts and verifies the ticket, the first SSL connection will be resumed.

- ID: Select the check box to enable the session reuse based on session ID. In this method, when an SSL connection is established between a client and a server for the first time, the session ID, symmetric key and other status information generated during the TLS handshake will be stored both in the cache of the client and the server. When the client initiates the SSL connection request again (or initiates the connection request again after disconnection), the server compares the session ID in the new request with the cached one and, if consistent, the first SSL connection will be resumed.

Notes:

- When the device works as the gateway of Web clients, the Web servers need to support the session reuse function.
- If session reuse based on session ticket and based on session ID are both configured, session reuse based on session ticket will be prioritized.

Configuring the Session Reuse Method

To enable or disable the session reuse function based on session ID or based on session ticket, in the SSL proxy profile configuration mode, use the following command:

session reuse {**id** | **ticket**} {**enable** | **disable**}

- **id** | **ticket** - Specifies to enable (**enable**) or disable (**disable**) the session reuse function based on session ID (**id**) or based on session ticket (**ticket**).

Configuring the Session Cache Size

To configure the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in the SSL proxy profile configuration mode, use the following command:

session reuse cache-size *value*

- *value* - Specifies the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID.

  See the range and default values:

Model	Range (Unit: piece)	Default value (Unit: piece)
SG-6000-A1100 and below platforms of A series; SG-6000-VM01 of CloudEdge	0 - 32. 0 means session cache information is not saved.	32

Model	Range (Unit: piece)	Default value (Unit: piece)
SG-6000-A2000 to SG-6000-A3600 of A series; SG-6000-VM02 of CloudEdge	0 - 128. 0 means session cache information is not saved.	128
SG-6000-A3700 and above platforms of A series; All platforms of K series; All platforms of X series; SG-6000-VM04 and SG-6000-VM08 of CloudEdge	0-256. 0 means session cache information is not saved.	256

To cancel the specified size, in the SSL proxy profile configuration mode, use the command of **no session reuse cache-size**.

Configuring the Session Timeout

To configure the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in the SSL proxy profile configuration mode, use the following command:

session reuse timeout *value*

- *value* - Specifies the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. If this timeout expires, the session caches will be deleted, and when the client establishes a SSL connection with the server, it needs a complete TLS handshake. The value range is 1800 to 72000 seconds. The default value is 3600 seconds.

To cancel the specified value, in the SSL proxy profile configuration mode, use the command of **no session reuse timeout**.

Clearing the Session Caches

To clear the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in any mode, use the following command:

clear sslproxy {session-ticket | session-id} cache

- **session-ticket | session-id** - Specifies to clear the session caches stored in the system during session reuse based on session ticket (**session-ticket**) or during session reuse based on session ID (**session-id**).

Viewing the Session Caches

To view the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in any mode, use the following command:

show sslproxy {session-ticket | session-id} cache

- **session-ticket | session-id** - Specifies to view the session caches stored in the system during session reuse based on session ticket (**session-ticket**) or during session reuse based on session ID (**session-id**).

Choosing a Work Mode

When the device works as the gateway of Web clients, the SSL proxy function can work in the Client Inspection - Proxy mode.

In the SSL Profile configuration mode, use the following command to choose the work mode:

mode client-inspection proxy

Specifying an Application to be Proxied by the SSL Proxy Function

If the SSL proxy function works in the client-inspection proxy mode, you can specify an application to be proxied by the function. By default, only the HTTPS traffic passing through the default port will be proxied, but you can specify additional applications as needed, such as IMAPS, POP3S, SMTPS, RDPS and FTPS. Besides, you can configure user-defined ports for the applications to be proxied. For specific configurations, refer to Configuring Rules in User-defined Application Signature Configuration Mode in Firewall > Service and Application > Userdefined Application.

To specify an application to be proxied by the SSL proxy function, in the SSL proxy profile configuration mode, use the following command:

inspect-app {**https** | **imaps**| **pop3s** | **smtps** | **rdps** | **ftps** }

- **https** - Proxies the HTTPS traffic.
- **imaps** - Proxies the IMAPS traffic.
- **pop3s**- Proxies the POP3S traffic.
- **smtps** - Proxies the SMTPS traffic.
- **rdps** - Proxies the RDPS traffic.
- **ftps** - Proxies the FTPS traffic.

Setting the URL Whitelist

When the SSL proxy is in the Client Inspection - Proxy mode, you can specify URL categories (predefined URL categories or user-defined URL categories) as needed, set the URL websites that will not be proxied by the SSL proxy function. By default, the predefined URL categories "Health & Medicine" and "Finance" have been added to the URL whitelist.

To set the URL whitelist, in the SSL proxy profile configuration mode, use the following command:

url-category *category-name*

- *category-name* - Specifies the name of the URL category that needs to be added to the URL whitelist. Up to 8 URL categories can be added.

To delete a URL category from the URL whitelist, use the **no url-category** *category-name*command.



Notes: To ensure that the URL whitelist works, please upgrade the predefined URL database before configuring this function.

Enabling the Root Certificate Push

When the HTTPS traffic is decrypted by the SSL proxy function, your request to an HTTPS website will be redirected to the Install Root Certificate page. In this page, you will be prompted that your accesses to HTTPS websites are being monitored, and that you should pay attention to your privacy and abide by applicable laws and regulations. The Install Root Certificate page is as follows:

To enable/disable the Root Certificate Push, in the SSL proxy profile configuration mode, use the following command:

Enable the Root Certificate Push: **no ca-cert-push disable**

Disable the Root Certificate Push: **ca-cert-push disable**

After enabling the Root Certificate Push, if your HTTPS accesses originating from one single source IP are matched with any configured policy rule, you will be prompted with the Install Root Certificate page every 12 hours when visiting the website over HTTPS.

You can clear the prompt history of root certificate downloading. After that, even that you have received the prompt before, you will be prompted with the page immediately when you visit the website over HTTPS again and your access matches with any configured policy rule. To clear the prompt history of root certificate downloading, in any mode, use the following command:

clear sslproxy ca-cert-push

Configuring the Actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS Traffic

Before performing the SSL proxy process, the device will chek the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be blocked and cannot display in the Web browser.
- If the action is Bypass, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list. When connecting to the Websites that are dynamically added to the

bypass list, the first connection will be disconnected. Uses need to re-connect to the Web-sites and the content will be displayed.

The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that are not blocked or bypassed.

Notice the following items during the configurations:

- When the parameters match multiple items in the checklist and you configure difference actions to different items, the Block action will take effect. The corresponding HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be blocked.
- If the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic is not bypassed or blocked after the SSL negotiation check, the system will decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.

Checking the SSL Protocol Version

Check the SSL protocol version used by the server. When the version of the SSL protocol used by the SSL server meets the minimum and maximum requirements, the system can proxy its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. To configure the SSL protocol version supported by the system, in the SSL proxy profile configuration mode, use the following commands:

- **max-support-ssl-version** {**tlsv1.0** | **tlsv 1.1** | **tlsv1.2** | **tlsv1.3**} – Specifies the maximum SSL protocol version supported by the system. The default version is tlsv1.3.
- **min-support-ssl-version** {**tlsv1.0** | **tlsv 1.1** | **tlsv1.2** | **tlsv1.3**} – Specifies the minimum SSL protocol version supported by the system. The default version is tlsv1.0.

To restore the default setting, use the **no** {**max-support-ssl-version** | **min-support-ssl-version**} command.

When the SSL server uses the SSL protocol version which is not supported in the system, you need to configure the action for HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, in the SSL proxy profile configuration mode, use the following command:

unsupported-ssl-version {**bypass** | **block**}

- **bypass** | **block** – Uses the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the system will not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. By default, the system will bypass and not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic in this condition.

To restore the default setting, use the **no unsupported-ssl-version** command.

Checking the Unkown Failure

When SSL negotiation fails and the cause of the failure can't be confirmed, you need to configure the action for HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, in the SSL proxy profile configuration mode, use the following command:

unknown-ssl-failure {**bypass** | **block**}

- **bypass** | **block** – Uses the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the system will not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. By default, the system will bypass and not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic in this condition.

To restore the setting to the default value, use the **no unknown-ssl-failure**command.

Checking the Encryption Algorithm

When the SSL server uses the encryption algorithm which is not supported in system, configure the action for HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS, in the SSL proxy profile configuration mode, use the following command:

unsupported-cipher {**bypass** | **block**}

- **bypass** | **block** – Uses the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the system will not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. By default, the system will bypass and not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic in this condition.

To restore the default setting, use the **no unsupported-cipher**command.

Checking Whether the SSL Server Certificate is Overdue

Check whether the SSL server certificate is overdue. When the SSL server certificate is overdue, the system can decrypt, block or bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic according to your configuration. To configure the action for HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the SSL server certificate is over-due, in the SSL proxy profile configuration mode, use the following command:

expired-cert {**decrypt** | **block** | **bypass**}

- **decrypt** | **block** | **bypass** – Uses the decrypt parameter to decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the system will not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. By default, the system will decrypt the traffic.

To restore the value to the default one, use **no expired-cert**command.

Checking Whether the SSL Server Verifies the Client Certificate

Check whether the SSL server verifies the client certificate. When the server verifies the client certificate, the system can block or bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. By default, the system bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the traffic will not be decrypted. To configure the action for

HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS when the SSL server verifies the client certificate, in the SSL proxy profile configuration mode, use the following command:

verify-client {**bypass** | **block**}

- **bypass** | **block** – Uses the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic and the system will not decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. Use the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.

To restore the setting to the default one, use the **no verify-client**command.

Configuring an Action When Server Certificate Verification Fails

You can configure an action for the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when system fails to verify the Web server certificate. In the SSL proxy profile configuration mode, use the following command:

verify-server-cert-failed {**block** | **bypass** | **decrypt**}

- **block** - Uses the block parameter to block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified.
- **bypass** - Uses the bypass parameter to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified.
- **decrypt** - Uses the decrypt parameter to decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified. By default, system will use the self-signed certificate to complete the SSL negotiation with the Web browser. To use the trusted certificate "SG6000" to complete the SSL negotiation with the Web browser, in the SSL proxy profile configuration mode, use the command **use-self-sign-cert disable**. To restore to the default value, in the SSL proxy profile configuration mode, use the command **no use-self-sign-cert disable**.

Configuring the Description

To add the description to an SSL proxy profile, in the SSL proxy profile configuration mode, use the following command:

description *description*

- *description* – Enters the description.

Use **no description**to delete the description.

Prioritizing the Low-intensity Encryption Algorithm

When the device works as both the gateway of Web clients and an SSL server, to ensure the performance of the SSL proxy function, the high-intensity encryption algorithm will be used by default when the device receives the cipher suite from the SSL client. If you need to weaken the encryption of the SSL proxy function, you can specify that the SSL server prefers the low-intensity encryption algorithm. In the SSL proxy Profile configuration mode, use the following command:

downstream-cipher-mode low-intensity-first

To restore the default high-intensity encryption algorithm, use the command **no downstream-cipher-mode low-intensity-first**.

Updating the Trusted Root Certificate Database

To ensure that the root certificates stored on your device are sufficient and up-to-date, and to reduce errors occurred during server certificate verification, you need to update the trusted root certificate database timely. You can change the update configurations of the trusted root certificate database as needed. The update configurations include:

- Configuring the update mode of the trusted root certificate database
- Updating now
- Importing a trusted root certificate database file

- Viewing update information of the trusted root certificate database
- Viewing information of the trusted root certificate database

Configuring the Update Mode of the Trusted Root Certificate Database

To configure the update mode of the trusted root certificate database, in the global configuration mode, use the following command:

trusted-root-ca-store update [**mode** {**auto** | **manual**} | **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* | **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] | **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*] | **protocol HTTP**]

- **mode** {**auto** | **manual**} – Specifies the update mode of the trusted root certificate database. System supports automatic and manual update modes. The default mode is automatic update.
- **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* – Specifies the proxy server for updating the trusted root certificate database.
- **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] – Specifies the schedule for automatically updating the trusted root certificate database.
- **server1** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 1.
- **server2** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 2.
- **server3** {*domain* | *ip*} [**vrouter** *vrouter-name*] – Specifies the domain, IP address and VRouter of update server 3.
- **protocol HTTP** - Specifies the update protocol as HTTP, and the default protocol is HTTPS.

Updating Trusted Root Certificate Database

To update the trusted root certificate database immediately, in the execution mode, use the following command:

exec trusted-root-ca-store update

Importing a Trusted Root Certificate Database File

In some cases, your device may be unable to connect to the update server to update the trusted root certificate database. To solve this problem, StoneOS provides the function for importing a trusted root certificate database file, i.e., importing a trusted root certificate database file to the device from an FTP or TFTP server, so that the device can update the trusted root certificate database locally. To import a trusted root certificate database file, in the execution mode, use the following command:

import trusted-root-ca-store from {**ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *username* **password** *string*] | **tftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*]} *file-name*

- **ftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] – Specifies the IP address, VRouter, user name and password of the FTP server to import a trusted root certificate database file. If no user name and password are specified, you will log onto the server anonymously.
- **tftp server** { *A.B.C.D* | *X:X:X:X::X* } [**vrouter** *vrouter-name*] – Specifies the IP address and VRouter of the TFTP server to import a trusted root certificate database file.
- *file-name* – Specifies the name of the trusted root certificate database file to be imported.

Viewing Update Information of the Trusted Root Certificate Database

To view update information of the trusted root certificate database, in any mode, use the following command:

show trusted-root-ca-store update

Viewing Information of the Trusted Root Certificate Database

To view information of the trusted root certificate database, in any mode, use the following command:

show trusted-root-ca-store info

Working as Gateway of Web Servers

To implement SSL proxy, you need to bind an SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, the system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure an SSL proxy profile, including the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.
2. Bind an SSL proxy profile to a proper policy rule. The device will decrypte the HTTPS traffic that matches the policy rule.

Configuring an SSL Proxy Profile

Configuring an SSL proxy profile includes the following items: configure the session reuse function, choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

To create an SSL proxy profile, use the following command in the global configuration mode:

sslproxy-profile *profile-name*

- *profile-name* - Specifies the name of the SSL proxy profile and enter the SSL proxy profile configuration mode. If the name already exists, the system will enter the SSL proxy profile configuration mode directly.

To delete an SSL proxy profile, use the **no sslproxy-profile** *profile-name*command.

Configuring the Session Reuse Function

With the Session Reuse function enabled, when the client initiates an SSL connection request to the server, the server checks whether the request connection has been created, and if so, the previous SSL connection is resumed without the need for a complete TLS handshake, thereby reducing the time consumption during the handshake process.

The system supports the following two session reuse methods:

- Ticket: Select the check box to enable the session reuse based on session ticket. In this method, when an SSL connection is established between a client and a server for the first time, the server encapsulates the symmetric key and other status information generated in the TLS handshake into a session ticket which is encrypted, and then forwards the session ticket to the client, which is stored in the cache of the client. When the client initiates the SSL connection again (or initiates the connection request again after disconnection), the session ticket will first be sent to the server for decryption. If the server successfully decrypts and verifies the ticket, the first SSL connection will be resumed.
- ID: Select the check box to enable the session reuse based on session ID. In this method, when an SSL connection is established between a client and a server for the first time, the session ID, symmetric key and other status information generated during the TLS handshake will be stored both in the cache of the client and the server. When the client initiates the SSL connection request again (or initiates the connection request again after disconnection), the server compares the session ID in the new request with the cached one and, if consistent, the first SSL connection will be resumed.



Notes:

- When the device works as the gateway of Web servers, the Web clients need to support the session reuse function.



- If session reuse based on session ticket and based on session ID are both configured, session reuse based on session ticket will be prioritized.

Configuring the Session Reuse Method

To enable or disable the session reuse function based on session ID or based on session ticket, in the SSL proxy profile configuration mode, use the following command:

session reuse {**id** | **ticket**} {**enable** | **disable**}

- **id** | **ticket** - Specifies to enable (**enable**) or disable (**disable**) the session reuse function based on session ID (**id**) or based on session ticket (**ticket**).

Configuring the Session Cache Size

To configure the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in the SSL proxy profile configuration mode, use the following command:

session reuse cache-size *value*

- *value* - Specifies the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID.

  See the range and default values:

Model	Range (Unit: piece)	Default value (Unit: piece)
SG-6000-A1100 and below platforms of A series; SG-6000-VM01 of CloudEdge	0 - 32. 0 means session cache information is not saved.	32
SG-6000-A2000 to SG-6000-A3600 of A series;	0 - 128. 0 means session cache information	128

Model	Range (Unit: piece)	Default value (Unit: piece)
SG-6000-VM02 of CloudEdge	is not saved.	
SG-6000-A3700 and above platforms of A series; All platforms of K series; All platforms of X series; SG-6000-VM04 and SG-6000-VM08 of CloudEdge	0-256. 0 means session cache information is not saved.	256

To cancel the specified size, in the SSL proxy profile configuration mode, use the command of **no session reuse cache-size**.

Configuring the Session Timeout

To configure the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in the SSL proxy profile configuration mode, use the following command:

session reuse timeout *value*

- *value* - Specifies the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. If this timeout expires, the session caches will be deleted, and when the client establishes a SSL connection with the server, it needs a complete TLS handshake. The value range is 1800 to 72000 seconds. The default value is 3600 seconds.

To cancel the specified value, in the SSL proxy profile configuration mode, use the command of **no session reuse timeout**.

Clearing the Session Caches

To clear the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in any mode, use the following command:

clear sslproxy {**session-ticket** | **session-id**} **cache**

- **session-ticket | session-id** - Specifies to clear the session caches stored in the system during session reuse based on session ticket (**session-ticket**) or during session reuse based on session ID (**session-id**).

Viewing the Session Caches

To view the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID, in any mode, use the following command:

show sslproxy {**session-ticket | session-id**} **cache**

- **session-ticket | session-id** - Specifies to view the session caches stored in the system during session reuse based on session ticket (**session-ticket**) or during session reuse based on session ID (**session-id**).

Choosing a Work Mode

When the device works as the gatetway of Web servers, the SSL proxy function can work in the "Server Inspection - Offload" mode or "Server Inspection - Proxy" mode.

- When the SSL proxy function works in the "Server Inspection - Offload" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.
- When the SSL proxy function works in the "Server Inspection - Proxy" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and re-encrypt the traffic and send it to the Web server.

In in the SSL Profile configuration mode, use the following command to specify the work mode:

mode server-inspection { **offload | proxy**}

- **offload** - Specifies the SSL proxy working mode as "Server Inspection - Offload" mode.
- **proxy** - Specifies the SSL proxy working mode as "Server Inspection - Proxy" mode.

Specifying Trust Domain

Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device. For more information about importing the certificate and the key pair, see the PKI chapter in StoneOS_CLI_User_Guide_User_Authentication.

After you complete the importing, specify the trust domain used by this SSL Profile. In the SSL Profile configuration mode, use the following command to specify the trust domain:

ssl-offload server-trust-domain *trust-domain-name*

- *trust-domain-name* – Specifies the trust domain name that will be used by this SSL Profile.

To cancel the setting, use the **no ssl-offload server-trust-domain**command.

Specifying HTTP Port Number

To specify the HTTP port number of the Web server, in the SSL Profile configuration mode, use the following command:

server-port *port*

- *port* – Specifies the port number. In Server Inspection - Offload Mode, the default port number is 80. In the Server Inspection - Proxy Mode, the default port number is 443.

Use the **no server-port**command to cancel the setting.

Enable Warning Page

When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, the system notifies the users that their accesses to HTTPS websites are being monitored and asks the uses to protect their privacy.

In the SSL proxy profile configuration mode, use the following command to enable/disable the warning page:

Enable the warning page: **no ssl-notification-disable**

Disable the warning page: **ssl-notification-disable**

After enabling the warning page, if your HTTPS access behavior originating from one single source IP is matched to any configured policy rule and SSL proxy profile, you will be prompted with the warning page every 30 minutes when visiting the website over HTTPS.

You can clear the SSL proxy warning history. After that, even that you have received the warning page before, you will be prompted immediately when you visit the website over HTTPS again. To clear the SSL proxy audit warning history, in any mode, use the following command:

clear sslproxy notification

Configuring the Description

To add the description to an SSL proxy profile, in the SSL proxy profile configuration mode, use the following command:

description *description*

- *description* – Enters the description.

Use **no description**to delete the description.

Binding the SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, the system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, enter the policy rule configuration mode in two steps. First, in the global configuration mode, use the following command to enter the policy configuration mode:

policy-global

Then, in the policy configuration mode, use the following command to enter the policy rule configuration mode:

rule [**id** *id-number*]

To bind the SSL proxy profile to a policy rule, in the policy rule configuration mode, use the following command:

sslproxy *profile-name*

- *profile-name* - Specifies the name of profile that is bound to the SSL proxy.

After the binding, you need to modify the priority of the policy rule to assure the traffic matching to this rule is prioritized. After then, you need to specify the user, destination zone and schedule of the rule. You can also enable or disable the rule. For more information, see the "Policy".

Configuring the SSL Proxy Filter Rule

After the SSL proxy function is enabled, if the HTTPS traffic of the proxy is abnormal, system supports the SSL proxy filter rule to locate the anomaly by filtering the HTTPS traffic of the proxy in the specified address or network segment.

Adding the SSL Proxy Filter Rule

To add the SSL proxy filter rule, in any mode, use the following command:

exec sslproxy-filter add {**src-ip** {*ipv4-address*|*ipv4-address/Mask*} [**dst-ip** *ipv4-address*] | **src-ipv6** {*ipv6-address* | *ipv6-address/Mask*} [**dst-ipv6** *ipv6-address*] } [**dst-port** *port-number*]

- **src-ip** {*ipv4-address* | *ipv4-address/Mask*} [**dst-ip** *ipv4-address*] - Specifies the source and destination IPv4 address of which the proxy HTTPS traffic needs to be filtered.
- **src-ipv6** {*ipv6-address* | *ipv6-address/Mask*} [**dst-ipv6** *ipv6-address*] - Specifies the source and destination IPv6 address of which the proxy HTTPS traffic needs to be filtered.
- **dst-port** *port-number* - Specifies the destination port number of which the proxy HTTPS traffic needs to be filtered.

Deleting the SSL Proxy Filter Rule

To delete the SSL proxy filter rule, in any mode, use the following command:

exec sslproxy-filter del

Viewing the SSL Proxy Filter Rule Information

To view the SSL proxy filter rule information, in any mode, use the following command:

show sslproxy filter

Configuring Asynchronous Acceleration

SSL proxy support for asynchronous acceleration using QAT engine. To configure the current acceleration engine for IPSec or SSL Proxy, in the global configuration mode, use the following command:

crypto-engine {ipsec |sslproxy}

- **ipsec** - Configure the current acceleration engine for IPSec.
- **sslproxy**- Configure the current acceleration engine for SSLVPN.



Notes:

- Only SG-6000 A series (except SG-6000-A200/A200W/A200G4B/A2205/A1805/A1605), SG -6000-X25803 / X25812 devices support this function.
- After configuring the asynchronous acceleration, system must reboot to make it take effect.

To view the status of the QAT engine, in any mode, use the following command:

show sslproxy qat-engine status

To view the module currently using the QAT engine, in any mode, use the following command:

show crypto-engine

To view the current request/response count of the QAT engine, in any mode, use the following command:

show sslproxy qat-engine counter

To view the statistic information of SSL Proxy asynchronous function, in any mode, use the following command:

show sslproxy async statistic

Configuring Domain White List

Websites that do not need or support SSL proxy can be added to the domain white list. The system provides the predefined domain white list to save the sites that do not support SSL proxy. For example, sites that require client certificate authentication is required or sites with fixed the website certificates. You can also add sites to the domain white list as needed. Predefined domain white list entries cannot be edited or deleted.

Configuring a User-defined Domain White List

If you choose not to decrypt a site out of service concerns, privacy concerns, or other voluntary reasons, you can add it to the domain white list. The device will not perform the SSL proxy function for the sites on the white list. To configure a user-defined domain white list, in the global configuration mode, use the following command:

sslproxy exempt-domain *domain-name* **description** *reason* {**enable** | **disable**}

- *domain-name* – Enters the domain of the user-defined domain white list. You can enter 1 to 63 characters and the domain is case sensitive. You can use the wildcard "*" in the domain. The wildcard "*" can only be used once and should be placed at the beginning of the domain, such as "*.hillstonenet.com".
- *reason* – Enters the description of the user-defined domain white list.
- **enable** – Enables the domain white list.
- **disable** – Disables the domain white list.

To delete the user-defined domain white list, use the **no sslproxy exempt-domain** *domain-name* command.

Updating SSL Proxy Domain Whitelist Signature Database

You can change the update configuration as needed. By default, the system updates the SSL proxy domain whitelist signature database everyday automatically. The configurations of updating SSL proxy domain whitelist signature database include:

- Configuring a domain whitelist signature database update mode
- Configuring an Update Protocol
- Configuring an update server
- Specifying a HTTP proxy server
- Specifying an update schedule
- Updating now
- Importing a domain whitelist signature file
- Viewing domain whitelist signature database information
- Viewing domain whitelist signature database update information

Configuring a Domain Whitelist Signature Database Update Mode

System supports both manual and automatic update modes. To configure a domain whitelist signature database update mode, in the global configuration mode, use the following command:

sslproxy-exempt-domain update mode {**auto** | **manual**}

- **auto** – Specifies the automatic domain whitelist update mode. This is the default mode.
- **manual** – Specifies the manual domain whitelist update mode.

To restore to the default mode, in the global configuration mode, use the following command:

no sslproxy-exempt-domain update mode

Configuring an Update Protocol

The system supports to update the signature database through HTTP and HTTPS, and the default protocol is HTTPS. To configuring the update protocol as HTTP, in the global configuration mode, use the following command:

sslproxy-exempt-domain update protocol HTTP

In the global configuration mode, use the following command to restore the default value:

no sslproxy-exempt-domain update protocol HTTP

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest domain whitelist signature as needed. To configure the update server, in the global configuration mode, use the following command:

sslproxy-exempt-domain update {**server1** | **server2** | **server3**} {*ip* | *dns-name*}

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip* | *dns-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

To cancel the specified update server, in the global configuration mode, use the following command:

no sslproxy-exempt-domain {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device accesses the Internet through an HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update automatically and normally.

To specify the HTTP proxy server for the domain whitelist signature database updating, use the following command in the global configuration mode:

sslproxy-exempt-domain update proxy-server {**main** | **backup**} *ip port_num*

- **main** | **backup** – Use the main parameter to specify the main proxy server and use the backup parameter to specify the backup proxy server.
- *ip port_num* – Specifies the IP address and the port number of the proxy server.

To cancel the proxy server configurations, use the **no sslproxy-exempt-domain update proxy-server** {**main** | **backup**} command.

Specifying an Update Schedule

By default, system automatically updates the domain whitelist signature database every day. To reduce the update server's workload, the time of daily update is random. To specify the schedule and specific time for the update, in the global configuration mode, use the following command:

sslproxy-exempt-domain schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**}} [*HH:MM*]

- **daily** – Updates the database every day.
- **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} – Updates the database every week. Parameter **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**is used to specify the specific date in a week.
- *HH:MM* – Specifies the time of update, for example, 09:00.

Updating Now

For both manual and automatic update modes, you can update the domain whitelist signature database immediately as needed. To update the domain whitelist signature database now, in any mode, use the following command:

exec sslproxy-exempt-domain update

- **exec sslproxy-exempt-domain update** – Only updates the incremental part between the current domain whitelist signature database and the latest domain whitelist signature database released by the update server.

Importing a Domain Whitelist Signature File

In some cases, your device may be unable to connect to the update server to update the domain whitelist signature database. To solve this problem, StoneOS provides the domain whitelist signature file import function, i.e., importing the domain whitelist signature files to the device from an FTP, TFTP server or USB disk, so that the device can update the domain whitelist signature database locally. To import the domain whitelist signature file, in the execution mode, use the following command:

import sslproxy-exempt-domain from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address* } [**vrouter** *vr-name*] *file-name*

- *ip-address* – Specifies the IP address of the FTP or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password of the FTP server.
- **vrouter** *vr-name* – Specifies the VRouter of the FTP or TFTP server.
- *file-name* – Specifies the name of the domain whitelist signature file that be imported.

Viewing Domain Whitelist Signature Database Information

You can view the domain whitelist signature database information of the device as needed, including the domain whitelist signature database version, and release dates. To view domain whitelist signature database information, in any mode, use the following command:

show sslproxy-exempt-domain info

Viewing Domain Whitelist Signature Database Update Information

You can view the domain whitelist signature database update information of the device as needed, including the update server information, update mode, update frequency and time, as well as the status of the domain whitelist signature database update. To view the domain whitelist signature database update information, in any mode, use the following command:

show sslproxy-exempt-domain update

Configuring the IP Whitelist

The device will not perform the SSL proxy function for the traffic from the IP address on the whitelist. You can add the IP, the traffic from which does not need or support SSL proxy, to the IP whitelist. The IP whitelist contains dynamic IP whitelist and static IP whitelist.

Configuring the Static IP Whitelist

The device will not perform the SSL proxy function for the traffic from the IP address on the IP whitelist. You can create a static IP on the whitelist as needed and the static IPs on the whitelist never expire. To create a static IP on the whitelist, in the global configuration mode, use the following command:

sslproxy exempt-ip {**ipv4** | **ipv6**} *address***port** *port_id*

- **ipv4** | **ipv6** – Specifies the IP type of the static IP listed on the whitelist entry as IPv4 or IPv6.
- *address* – Specifies the IP address of the static IP listed on the whitelist.
- **port** *port_id* – Specifies the TCP port of the static IP listed on the whitelist.

To delete the static IP listed on the whitelist, use the **no sslproxy exempt-ip** {**ipv4** | **ipv6**} *address* **port** *port_id* command.

Configuring the Validity Time of Dynamic IP Whitelist

When the device works as the gateway of Web clients, the system automatically adds the IP address to the dynamic IP whitelist in the following conditions: The traffic from this IP cannot be SSL proxied by the system and the action for the traffic is to bypass. In this scenario, the system will not perform SSL proxy function for the traffic from the IPs listed on the IP whitelist in the future. For more information on the configuration of the SSL proxy profile, see Configuring an SSL Proxy Profile. The traffic of the IP, which is added to the dynamic IP whitelist because its traffic cannot be proxied by the device, will be re-proxied again after the validity time is due. You can configure the validity time of IPs on the dynamic IP whitelist. The system automatically deletes existing dynamic IPs on the whitelist after their validity time is due. To configure the

validity time of the dynamic IPs on the whitelist, in the global configuration mode, use the following command:

sslproxy exempt-ip timeout *num*

- *num* – Specifies the validity time of the dynamic IPs on the whitelist. The unit is by day. The range of the validity time is from 1 to 30 days. The default validity time is 15 days.



Notes: After you modify the SSL Profile policy or change the validity time of the dynamic IPs on the whitelist, the system deletes all IPs on the current lists.

Clearing the IP Whitelist

To clear all the IP addresses on the whitelist, in the global configuration mode, use the following command:

clear sslproxy exempt-ip



Notes: The total number of IPs that can be listed on the whitelist varies on different platforms. When the number of IP addresses that can be listed on the whitelist exceeds its upper limit, the system generates event logs to remind you of clearing IPs on the whitelist.

Viewing SSL Proxy Information

To view the SSL proxy information, use the following commands:

- **show sslproxy** [**slot** *slot-number*] {**exempt-domain** | **exempt-ip**} (Only K6580, K9180 and X series devices support **slot**)
  - **exempt-domain** – Views the information of the domain white list, including the number of total sites on the domain white list, and the domain, type, description, status of each site on the white list.

    - **exempt-ip** − Views the information of the IP whitelist, including the IP address, port number, creation time, expiration time, and the reason why each IP is added to the white list.

- View the SSL proxy state, including the SSL proxy work mode, statistics, and the PKI domain of the SSL proxy certificate, number of bypassed sessions, number of dropped new sessions, value of real-time proxy HTTPS traffic, times of certificate verification failures: **show sslproxy slot** *slot-number* **state**(Only K6580, K9180 and X series devices support **slot**)
- View the SSL profile information, including the work mode, policy rules bound to the SSL proxy, configuration of inspection conditions, the status of alarms, URL whitelist: **show sslproxy-profile** [*profile-name*]
- View the TCP proxy information: **show tcpproxy** [**slot** *slot-number*] **session-id** *id*(Only K6580, K9180 and X series devices support **slot**)

Chapter 14 Monitor

The chapter introduces the following topics:

- "Monitor" on Page 2531 describes how to configure all monitoring statistics function for the system.
- "Logs" on Page 2598 introduces all the log functions of the system and how to output various log information of the device.
- "Diagnostic Tool" on Page 2641 describes all troubleshooting commands.
- "NetFlow" on Page 2663describes how to configure the NetFlow function to perform statistics and analysis on network traffic.

Monitor

Overview

Monitor include:

- User Monitor: Monitor based on user, Gathers statistics on the data and traffic passing through user, usergroup, address Book.
- Application Monitor: Monitor based on application, Gathers statistics on the data and traffic passing through application, application-group.
- Threat Monitor : Monitor based on threat, Gathers statistics on the threats.
- QoS Monitor: Monitor based on QoS, Gathers statistics on the pipes.
- Service/Network Node Monitor: Monitor based on service/network node, Gathers statistics on the packet loss rate and latency of service/network nodes.
- Device Monitor: Monitor based on devices. Gathers statistics on the total traffic, interface traffic, zone , Online IP , new/concurrent sessions, NATand hardware status.
- URL Hit: Monitor based on URL. Gathers statistics on user/IPs, URLs and URL categories.
- Application Block: Gathers statistics on the applications and user/IPs.
- Keyword Block: Gathers statistics on the Web keyword, Web keywords, email keywords, posting keywords and users/IPs.
- Authentication User: Gathers statistics on the authenticated users.
- User-defined Monitor: Gathers statistics on the data passing through the Hillstone device.

If IPv6 is enabled, system will count the total traffic/sessions/AD/URLs/applications of IPv4 and IPv6 address. Only User Monitor/Application Monitor/Cloud Application Monitor/Device Monitor/URL Hit/Application Block/User-defined Monitor support IPv6 address.



Tip: It is strongly recommended to use WebUI to configuring and view the monitor results, because it can render the data information more vividly. CLI is not recommended.

User Monitor

Gathers statistics on the data and traffic passing through user, usergroup, address Book. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Configuring Monitor Address Book

The monitor address is a database that stores the user's address which is used for the statistics. In the global configuration mode, use the following command:

statistics address *address-entry-name*

- *address-entry-name* – Specifies the name of the address entry.

To disable address-based statistics, in the global configuration mode, use the following command:

no statistics address *address-entry-name*

Viewing Address Book Statistical Information

To view the statistical information on the traffic from or to the specified address, in any mode, use the following command:

show statistics address [*address-entry-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

- *address-entry-name* – Specifies the name of the address entry. If this parameter is not specified, the command will show traffic statistics of all the address entries being referenced by the statistics function (by command statistics address address-entry-name).
- **current** – Shows the real-time traffic statistics of the specified address entry

- **lasthour** – Shows the traffic statistics of the specified address entry per 30 seconds for the last 60 minutes.
- **lastday** – Shows the traffic statistics of the specified address entry per 10 minutes for the last 24 hours.

Configuring Subnet Monitor Address Book

The system will match the traffic which is sent from the Internet to Subnet according to the specified address. If matched, the traffic will be counted to the Subnet side. To configure the subnet monitor address book, in the global configuration mode, use the following command:

statistics-filter {**address** | **ipv6-address**} *address-entry-name*

- *address-entry-name* – Specifies the name of the address entry.

To disable subnet monitor address book, in the global configuration mode, use the following command:

no statistics-filter {**address** | **ipv6-address**} *address-entry-name*

Viewing Subnet Monitor Address Entry Information

In global configuration mode, use the following command:

show statistics-filter address {**address** | **ipv6-address**}

Viewing the Stat-set for User Monitor

The predefined stat-set for user monitor includes:

Type	Name	Description
User Monitor	predef_user_bw	Statistics on the traffic of all the users
	predef_ztna_user_bw	Statistics on the traffic of all ZTNA users

Type	Name	Description
	predef_user_sess	Statistics on the sessions of all the users
	predef_user_app_bw	Statistics on the traffic of all the users' applications
	predef_exstat_exstat_ip_bw	Statistics on the user traffic of the selected address book
	predef_exstat_exstat_ip_sess	Statistics on the user sessions of the selected address book
	predef_exstat_exstat_app_bw	Statistics on the app traffic of the selected address book
	predef_exstat_exstat_app_sess	Statistics on the app sessions of the selected address book
	statistics-set predef_dip_bw	Statistics on the traffic of the selected destination IP addresses

To view the predefined stat-set information for user monitor, see Viewing Stat-set Information.



Tip: Non-root VSYS also supports user monitor, but does not support address book statistics.

Application Monitor

Application-based statistics allows you to gather statistics on the traffic of the specified application in real time, or per 30 seconds, per 10 minutes and per 24 hours in the last 60 minutes, 24 hours and 30 days respectively. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Configuring Monitor Application Group

To configure the monitor application group, in the global configuration mode, use the following command:

statistics application-group *application-group-name*

- *application-group-name* – Specifies the name of the application group.

To delete monitor application group, in the global configuration mode, use the following command:

no statistics application-group *application-group-name*

Viewing Application-based Statistical Information

To view the statistical information on the traffic of the specified application, in any mode, use the following command:

show statistics application-group [*application-group-name*] [**current** | **lasthour** | **lastday** | **lastmonth**]

- *application-group-name* – Specifies the name of the application group. If this parameter is not specified, the command will show traffic statistics of all the application groups being referenced by the statistics function (by command statistics servgroup servicegroup).
- **current** – Shows the real-time traffic statistics of the specified application group.
- **lasthour** – Shows the traffic statistics of the specified application group per 30 seconds for the last 60 minutes.
- **lastday** – Shows the traffic statistics of the specified application group per 10 minutes for the last 24 hours.
- **lastmonth** – Shows the traffic statistics of the specified application group per 24 hours for the last 30 days.

Viewing the Stat-set for Application Monitor

The predefined stat-set for applicaton monitor includes:

Type	Name	Description
application monitor	predef_app_bw	Statistics on the traffic of all the applications
	predef_app_sess	Statistics on the sessions of all the applications
	predef_exstat_exstat_ip_bw	Statistics on the user traffic of the selected application group
	predef_exstat_exstat_ip_sess	Statistics on the user sessions of the selected application group
	predef_exstat_exstat_app_bw	Statistics on the app traffic of the selected application group.
	predef_exstat_exstat_app_sess	Statistics on the app sessions of the selected application group.
	statistics-set predef_dip_bw	Statistics on the traffic of the selected destination IP addresses.

To view the predefined stat-set information for application monitor,see Viewing Viewing Stat-set Information.



Tip: Non-root VSYS also supports application monitor, but does not support to monitor application group.

Threat Monitor

Viewing the Stat-set for Threat Monitor

The predefined stat-set for threat monitor includes:

Type	Name	Description
threat monitor	predef_ip_dip_threat	Statistics on the all the threats

To view the predefined stat-set information for threat monitor, see Viewing Stat-set Information.

QoS Monitor

Only supports to use WebUI to viewing the QoS monitor information, see StoneOS_WebUI_User_Guide.

Service/Network Node Monitor（For T Series）

The commands of service/network node monitor:

host…type dns

Create a service node, type is DNS. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type dns** **domain** *domain-name* [**port** *port*] **source-interface** *interface-name* [**probe-interval** *inter-val*] [**parent** *parent-id*] [**desc** *description*] **group** *group-name*

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id - Specifies the service/network node ID.

node-name - Specifies the name of service/network node.

ip-address - Specifies the node IP address.

host-name - Specifies the host name of node.

domain-name -Specifies the DNS domain name.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

group-name -Specifies the name of the group. If the group does not exist, the system will create it automatically.

Default values:

port:53

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type dns domain www.baidu.com source-interface ethernet0/3**

host…type ftp

Create a service node, type is FTP. Use the no form to delete the node.

Command:

host [**test-only**][**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type ftp** [[**port** *port*] | **user** *username* **password** *password* **uri** *uri* [**port** *port*]] **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

user *username* -Specifies the user name of server.

password *password* -Specifies the password of server.

uri *uri* -Specifies the name of file saved on server.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

port: 21

probe-interval *interval*: 30s

parent-id: 0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type ftp user admin admin uri file source-interface ethernet0/3**

host···type http

Create a service node, type is HTTP. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type http url** *url-address* [**port** *port*] **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

url-address-Specifies the name of file saved on server.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

port:80

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type http url www.sina.com.cn source-interface ethernet0/3**

host…type icmp

Create a service node, type is ICMP. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type icmp source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

probe-interval *interval*: 30s

parent-id: 0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type icmp source-interface ethernet0/3**

host···type imap4

Create a service node, type is IMP4. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type imap4** [**port** *port*] **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

port:143

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type imap4 source-interface ethernet0/3**

host···type ldap

Create a service node, type is LDAP. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type ldap** [[**port** *port*] | **user** *username* **password** *password* **uri** *uri* [**port** *port*]] **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

user *username* -Specifies the user name of server.

password *password* -Specifies the password of server.

uri *uri* -Specifies the name of file saved on server.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

None

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type ldap user admin admin uri file port 21 source-interface ethernet0/3**

host…type pop3

Create a service node, type is POP3. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type pop3** [**port** *port*] **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

port:110

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type pop3 source-interface ethernet0/3**

host…type smtp

Create a service node, type is SMTP. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type smtp** [**port** *port*] *source-interface interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

port:25

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host test-only name test 1.1.1.1 type smtp source-interface ethernet0/3 probe-interval 60**

host…type {tcp | udp}

Create a user-defined node. Use the no form to delete the node.

Command:

host [**test-only**] [**id** *node-id*] **name** *node-name* {*ip-address* | *host-name*} **type** {**tcp** | **udp**} **port** *port* **source-interface** *interface-name* [**probe-interval** *interval*] [**parent** *parent-id*] [**desc** *description*]

no host id *node-id*

Description:

test-only -If this parameter is specified, the system will show the results of detection.

node-id -Specifies the service/network node ID.

node-name -Specifies the name of service/network node.

ip-address -Specifies the node IP address.

host-name -Specifies the host name of node.

port -Specifies the port of server, the value range is 1 to 65535.

interface-name -Specifies the interface name of egress interface.

probe-interval *interval* -Specifies the probe interval, the value range is 15 to 120 seconds.

parent-id -Specifies the parent node ID. If this parameter is not specified, the parent node is root node as default.

description -Specifies the description.

Default values:

probe-interval *interval*:30s

parent-id:0

Mode:

Monitor configuration mode.

Guidance:

None

Example:

hostname(config-monitor)# **host name test 1.1.1.1 type tcp port 4455 source-interface ethernet0/3**

show monitor host config

To view the service/network node monitor configuration information.

Command:

show monitor host config

Description:

None

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# show monitor host config

show monitor host status

To view the service/network node status.

Command:

show monitor host status

Description:

None

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# show monitor host status

Device Monitor

Non-root VSYS also supports device monitor, but doesn't support hardware status. If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address. The commands of device monitor:

Viewing Interface-based Statistical Information

To view the statistical information on the traffic passing through the specified interface, in any command mode, use the following command:

show statistics interface-counter interface *interface-name* {**second** | **minute** | **hour**| **day**}[**IPv4** | **IPv6** | **noip**]

- *interface-name* – Specifies the name of the interface.
- **second** – Shows the traffic statistics of the specified interface per second for the last 60 seconds.
- **minute** – Shows the traffic statistics of the specified interface per minute for the last 60 minutes.
- **hour** – Shows the traffic statistics of the specified interface per hour for the last 24 hours.
- **day** – Shows the traffic statistics of the specified interface for the last 30 days.
- **IPv4** | **IPv6** | **noip** - Shows the traffic statistics of of IPv4, IPv6 address type, or non IP packets. If this parameter is not specified, all traffic information will be displayed by default.

Viewing the Stat-set for Device Monitor

The predefined stat-set for device monitor includes:

Type	Name	Description
Device Monitor	predef_zone_ bw	Statistics on the traffic of all the security zones
	predef_if_bw	Statistics on the traffic of all the interfaces
	predef_zone_sess	Statistics on the sessions of all the security zones
	predef_if_sess	Statistics on the sessions of all the interfaces

To view the predefined stat-set information for device monitor, see Viewing Stat-set Information.

Viewing the Information of Hard Disk Module

The hard disk module mainly saves logs to the local and achieves the goals of device monitoring, behavior auditing, etc. To view the installation and ultilization of hard disk module, in any mode, use the following command:

show disk

Viewing the Utilization of Virtual Hard Disk of CloudEdge Devices

The virtual hard disk of CloudEdge device is divided into system partition and data partition. The system partition is used to store system files, while the data partition is used to store logs and reports. To view the utilization of the virtual hard disk of CloudEdge device, in any mode, use the following command:

show disk

Example:

hostname# **show disk**

```
Displays the utilization of system partition of the virtual
hard disk of CloudEdge device
```

```
The percentage of system disk utilization: 18.6%
total(KB) used(KB) free(KB)
1888268 351952 1536316
Displays the utilization of data partition of the virtual hard disk of CloudEdge device
The percentage of data disk utilization: 14.2%
total(KB) used(KB) free(KB)
3997376 567056 3430320
hostname#
```

Viewing Memory Usage

In any mode, use the following command to view the usage of the system memory:

show memory

In any mode, use the following command to view the system memory size occupied by file systems:

show memory filesys

In any mode, use the following command to view CP and DP utilization:

show memory detail

Note: CP memory is used to store data generated from system configuration and management, and DP memory is used to store data generated by system traffic forwarding and business.

Viewing CPU and Memory Utilization

To view device's CPU and memory utilization, in any mode, use the following commands:

- To view CPU utilization , use the command **show cpu**

```
Example:
hostname#show cpu
Average cpu utilization : 0.3%
```

Current cpu utilization : 0.2%

Last 1 minute : 0.3%

Last 5 minutes : 0.3%

Last 15 minutes : 0.3%

- To view the utilization of each CPU core , use the command **show cpu detail**

Example :

hostname#**show cpu detail**

Average cpu utilization since last boot(%):

...

Current cpu utilization (%):

...

Cpu utilization in last 60 seconds(%):

...

Cpu utilization in last 60 minutes(%):

...

Cpu utilization in last 24 hours(%):

...

Cpu utilization in last 7 days(%):

...

Modifying the product name on the login page

The system supports to modify the product name displayed on the login page, in the global configuration mode, use the following command:

product -category-name*name*

- *name* - Specifies the product name displayed on the login page, the value range is 1-128 characters.

URL Hit

The predefined stat-set for URL hit includes:

Type	Name	Description
URL Hit	predef_url_hit	Statistics on the URL hits
	predef_user_url	Statistics on the URLs accessed by the users
	predef_url_cat_hit	Statistics on the URL category hits
	predef_user_url_cat_hit	Statistics on the URL categories accessed by the users

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

To view the predefined stat-set information for URL hit, see Viewing Stat-set Information.



Tips: Non-root VSYS also supports URL hit in K9180 devices, K6580 devices and X series platforms.

Link Status Monitor

Link status monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, jitter, bandwidth utilization, so as to realize the monitoring and display of the overall status of the link. System also supports for link detection to calculate the traffic information of the specific destination IP address or domain, including latency, jitter, and packet loss rate.

Enabling/Disabling Link User Experience Monitor

To enable the link user experience monitor, first enter the link monitor configuration mode, and then specify the binding interface. In the global configuration mode, use the following command to specify the binding interface:

link-perf-monitor interface *interface-name*

- *interface-name* – Specify the interface name.

To delete the interface, use the **no link-perf-monitor interface** *interface-name*command in the link monitor configuration mode.

To enable the link user experience monitor for interface, in the link monitor configuration mode, use the following command:

monitor on

To disable this function for the specified interface, use the **no monitor on** command in the link monitor configuration mode.

Enabling/Disabling Application Switch for Interface

After enabling the application switch, you can see details of the specific application in this interface. By default, the application switch is disabled. To enable the application switch, in the link monitor configuration mode, use the following command:

application on

To disable this function for the specified interface, use the **no application on**command in the link status monitor configuration mode.

Specify the Description of Interface

To specify the description for the binding interface, in the link monitor configuration mode, use the following command:

description *string*

- *string* - Specify the description for the binding interface.

To delete the description, use the **no description** in the link monitor configuration mode.

Viewing Link Configuration Information

To view link status monitor configuration information, in any mode, use the following command:

show link-perf-monitor information

Viewing Statistics Information of Link User Experience

To view statistics information of link user experience, in any mode, use the following command:

show link-perf-monitor statistics [**interface** *interface-name* [**application** *application-name*][**history** {**minute** | **hour** | **day** | **month**}]] [**ipv4** | **ipv6**]

- **interface** *interface-name* – View the link user experience monitoring statistics according to the specified interface.
- **application** *application-name* – View the link user experience monitoring statistics according to the specified application. If not specified, the system will display the statistics information according to the specified interface.
- **history** {**minute** | **hour** | **day** | **month**} – View the history statistics information.
- **ipv4** | **ipv6** – View the link user experience monitoring statistics according to the specified IP type. If not specified, system will display the statistics information including IPv4 and IPv6 by default.

Configuring the Link Detection Destination

System supports for link detection to calculate the traffic information of the specific destination IP address or domain, including latency, and jitter.

Entering the Link Detection Monitor Configuration Mode

To configure the detection destination, first enter the link detection monitor configuration mode, and then specify the destination IP address. In the global configuration mode, use the following

command to specify the destination IP address:

link-detect-object

Configuring the Link Detection Destination of IPv4

To configure the link detection destination of IPv4, in the link detection monitor configuration mode, use the following command:

ip*A.B.C.D***protocol** {**tcp** [**port***port-number*] | **icmp**} [**description***description*]

- *A.B.C.D*- Specify the IP address of detection destination.
- **tcp** [**port** *port-number*]- Specify the protocol type as TCP and specify the port number.
- **icmp**- Specify the protocol type as ICMP.
- **description** *description*-Specify the description for the detection destination.

To delete the detection destination, use the **no ip** *A.B.C.D* in the link detection monitor configuration mode.

Configuring the Link Detection Destination of IPv6

To configure the link detection destination of IPv6, in the link detection monitor configuration mode, use the following command:

ipv6*X:X:X:X::X***protocol** {**tcp** [**port***port-number*] |**icmp6**} [**description***description*]

- *X:X:X:X::X*- Specify the IPv6 address of detection destination.
- **tcp** [**port** *port-number*]- Specify the protocol type as TCP and specify the port number.
- **icmpv6** - Specify the protocol type as ICMPv6.
- **description** *description*- Specify the description for the detection destination.

To delete the detection destination, use the **no ipv6** *X:X:X:X::X* in the link detection monitor configuration mode.

Configuring the Link Detection Destination of Domain

To configure the link detection destination of domain, in link detection monitor configuration mode, use the following command:

domain-name*domian-name***ip-type** {**ipv4** | **ipv6**} **protocol** {**tcp** [**port***port-number*] | **icmp6**} [**description***description*]

- *domian-name* - Specifies the domain of the detection destination, which needs to be 1 to 64 characters in length. This value is not case-sensitive.
- **ipv4** | **ipv6** - Specifies the detection type of the domain, which can be ipv4 or ipv6.
- **tcp** [**port***port-number*] - Sets the protocol type to TCP and specifies the protocol port number.
- **icmp6**- Sets the protocol type to ICMPv6.
- **description***description* - Specifies the description for the detection destination.

To delete the detection destination, use the **no domain-name***domian-name* in link detection monitor configuration mode.

Configuring a Link Detection Rule

The system supports to perform persistent link quality detection by using link detection rule, including latency, jitter, and packet loss rate.



Notes:

- Non-root VSYS does not support the link detection function.
- The link detection function cannot be used in HA Active-Active mode.
- All interfaces bound to a link detection rule need to belong to the same virtual router.
- When traffic latency is greater than or equal to 2000 ms, it is marked with a red dot in the latency trend chart.

Enter the Link Detection Rule Mode

To create a link detection rule and enter the link detection rule mode, in global mode, use the following command:

active-detect-rule*rule-name*

- *rule-name* - Specifies the name of the link detection rule. Then, you will enter the link detection rule mode. If the name already exists, you will directly enter the link detection rule mode.

Configuring the Link of the Link Detection Rule

To configure the interface whose link status you want to monitor, in link detection rule mode, use the following command:

interface*interface-name*

- *interface-name* - Specifies the interface whose link status you want to monitor. You can specify at most 8 interfaces for a link detection rule.

To delete the link of the link detection rule, use the **no interface***interface-name* in link detection rule mode.

Configuring the Detection Destination of the Link Detection Rule

To configure the detection destination IP address or domain whose link status you want to monitor, in link detection rule mode, use the following command:

detect-object*detect-object-name*

- *detect-object-name* - Specifies the detection destination IP address or domain whose link status you want to monitor. You can specify at most 8 detection IP addresses or 1 detection domain for a link detection rule, but you cannot specify the detection IP address and domain at the same time.

To delete the detection destination of the link detection rule, use the **no detect-object***detect-object-name* in link detection rule mode.

Configuring the Packet Loss Rate Threshold of the Link Detection Rule

To configure the packet loss rate threshold of the link detection rule, in link detection rule mode, use the following command:

loss-rate-thres*loss-rate-threshold*

- *loss-rate-threshold* - Specifies the packet loss rate threshold of the link detection rule. Valid values: 0 to 100. Default value: 75. When the packet loss rate exceeds the threshold, it is marked with a red dot in the packet loss trend chart on the WebUI.

To delete the packet loss rate threshold, use the **no loss-rate-thres** in link detection rule mode.

Enabling/Disabling the Link Detection Rule

By default, configured link detection rules are disabled. To enable a link detection rule, in link detection rule mode, use the following command:

switch on

To disable the link detection rule, use the **no switch on** in link detection rule mode.

Viewing the Configuration of Link Detection Rule

To view the configuration of link detection rule, in any mode, use the following command:

show link-detect-object {**all** | *rule-name*}

- **all** – View the configuration of all link detection rules.
- *rule-name* - View the configuration of the specified link detection rule.

Example:

```
hostname(config)# show link-detect-object all
Total l3s-active-detect-rule number: 7 (Display the number
of link detection rules)
=============================================================-
=======
Name Status Loss-rate-threshold Interface-number Detect-
```

```
object-number (Display the name, status packet loss rate
threshold, number of associated interfaces, number of asso-
ciated detection destinations of the link detection rule)
------------------------------------------------------------
------------------------------------------------------------
4.123.com ON 75 1 1
70-trust ON 75 1 1
70-test ON 75 1 1
1 ON 75 2 2
test ON 75 1 1
111 ON 75 1 1
1234 ON 60 1
============================================================-
=======
```

Viewing Link Detection Monitor Configuration Information

To view link detection monitor configuration information, in any mode, use the following command:

show link-detect-object {**all** | *A.B.C.D* | *X:X:X:X::X* | *domain-name*}

- **all** – Display the link detection monitor configuration information of all the destination IP address.
- *A.B.C.D* | *X:X:X:X::X* | *domain-name*} - Display the link detection monitor configuration information of the specified destination IPv4 address, IPv6 address, or domain.

Application Block

The predefined stat-set for Application Block includes:

Type	Name	Description
Application Block	predef_app_block	Statistics on the application blocks
	predef_user_app_block	Statistics on the application blocks of all the users
	predef_user_app_app_block	Statistics on the application blocks of the specified user

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

To view the predefined stat-set information for Application Block, see Viewing Stat-set Information.

Keyword Block

The predefined stat-set for Keyword Block includes:

Type	Name	Description
Keyword Block	predef_kw_block	Statistics on the file content/ webpage/ E-mail/Web posting keyword blocks
	predef_user_kw_block	Statistics on the keyword blocks of all the users
	predef_user_kw_kw_block	Statistics on the keyword blocks of the specified user

To view the predefined stat-set information for Keyword Block, see Viewing Stat-set Information.



Tip: Non-root VSYS also supports keyword block in K9180 devices, K6580 devices and X series platforms.

Authentication User

The commands of authentication User:

show auth-user

View the online authuser information.

Command:

show auth-user [**username** *user-name* **interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

username *user-name* -View the online user of specific username information .

web-auth -View the online WebAuth user information.

scvpn -View online users of all SSL VPN instances.

Default values:

None

Mode:

Any mode

Guidance:

This command also displays the groups associated with an online user. If an online user is associated with more than 256 groups, it will display only the firstly configured 256 groups.

Example:

hostname# **show auth-user scvpn**

show auth-user groupname

View the information about online authenticated users in a specific user group.

Command:

show auth-user groupname *group_name*

Description:

groupname *group_name* -Specifies the name of the user group.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname#**show auth-user groupname group1**

show dp-auth-user

View the online auth user information of system data plane.

Command:

show dp-auth-user [{**username***user-name* | **webauth-ntlm** | **webauth-password** | **webauth-sms** | **webauth-oauth**} [**interface***interface-name* | **vrouter***vrouter-name*]]

Description:

username *user-name* -View the online user information with the specified username.

webauth-ntlm - View the online user information with the Webauth-NTLM type.

webauth-password - View the online user information with the Webauth-password type.

webauth-sms - View the online user information with the Webauth-sms type.

webauth-oauth - View the online user information with the Webauth-OAuth type.

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

Only for system debug.

Example:

hostname# **show dp-auth-user**

show pseudo-group

View the user group ID information.

Command:

show pseudo-group [**aaa-server** *server-name* **group** *group-name*]

Description:

aaa-server *server-name* - View the user group ID of the specified AAA server.

group *group-name* - View the user group ID of the specified user group.

Default values:

None

Mode:

Any mode

Guidance:

Only for system debug.

Example:

hostname# **show pseudo-group**

show auth-user agent

View the information of the online agent users.

Command:

show auth-user agent [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user agent interface ethernet0/0**

show auth-user dot1x

View the information of the online 802.1x users.

Command:

show auth-user dot1x [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user dot1x**

show auth-user interface

View the online users information that use specific interface as authentication ingress interface.

Command:

show auth-user interface *interface-name*

Description:

interface-name -Specifies the interface name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user interface ethernet1/1**

show auth-user ip

View the online user of specific IP information .

Command:

show auth-user agent [**ip** *ip-address*| **ip** *ip-address* **to***ip-address*] [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

ip-address -Specifies the IP address.

ip *ip-address* **to** *ip-address* -Specifies the range of IPv4 or IPv6 addresses.

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ip 10.180.32.1**

hostname# **show auth-user ip 10.180.32.1 to 10.182.32.2**

show auth-user l2tp

To view all the clients of the L2TP instance.

Command:

show auth-user l2tp [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user l2tp interface ethernet0/1**

show auth-user mac

View the online user of specific MAC address.

Command:

show auth-user mac *mac-address*

Description:

mac-address -Specifies the MAC address.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user mac 0050.569d.0b7e**

show auth-user radius-snooping

To view the information of the online users.

Command:

show auth-user radius-snooping [**interface** *interface-name* | **vrouter** *vrouter-name* | **slot** *slot-no*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

slot *slot-no* - Specifies the number.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user radius-snooping**

show auth-user static

View the static auth-user, include IP or MAC binding users.

Command:

show auth-user {**static** | **mac** *mac-address* | **ip** *ip-address* } [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

mac *mac-address* -Specifies the MAC address for binding.

ip *ip-address* -Specifies the IP address for binding.

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* - Specifies the VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user static**

show auth-user scvpn

View online users of all SSL VPN instances.

Command:

show auth-user scvpn [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user scvpn**

show auth-user endpoint-tag

View online uses appended with the specified endpoint tags.

Command:

show auth-user [**interface***interface-name* | **vrouter***vrouter-name* | **endpoint-tag***endpoint-tag-name*]

Description:

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

endpoint-tag *endpoint-tag-name*-Specifies the endpoint tag name. Both partial match and exact match are supported.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user endpoint-tag tag1**

show auth-user ztna

View ZTNA online users.

Command:

show auth-user ztna [**interface***interface-name* | **vrouter***vrouter-name* | **endpoint-tag***end-point-tag-name*]

Description:

interface *interface-name* -Specifies the interface name.

vrouter *vrouter-name* -Specifies the interface VRouter name.

endpoint-tag *endpoint-tag-name*-Specifies the endpoint tag name. Both partial match and exact match are supported.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ztna endpoint-tag tag1**

show auth-user ad-scripting

View the information of the online sso-agent users.

Command:

show auth-user ad-scripting [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name*- Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ad-scripting**

show auth-user ad-polling

View the information of the online users.

Command:

show auth-user ad-polling [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user ad-polling**

show auth-user sso-radius

View the information of the online users.

Command:

show auth-user sso-radius [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name*- Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user sso-radius**

show auth-user sso-monitor

View the information of the online users.

Command:

show auth-user sso-monitor [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name*- Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user sso-monitor**

show auth-user webauth-ntlm

View the information of the online users.

Command:

show auth-user webauth-ntlm [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user webauth-ntlm**

show auth-user xauth

View the information of the online XAUTH users.

Command:

show auth-user xauth [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user xauth**

show auth-user webauth

View the online WebAuth user information.

Command:

show auth-user webauth [**interface** *interface-name* | **vrouter** *vrouter-name*]

Description:

interface *interface-name* - Specifies the interface name.

vrouter *vrouter-name* - Specifies the interface VRouter name.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user webauth**

show auth-user vrouter

View the user of specific VRouter.

Command:

show auth-user vrouter

Description:

None

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **show auth-user vrouter trust-vr**

User-defined Monitor

The stat-set of StoneOS allows you to gather statistics on the data passing through the device. With this function configured, you can view the real-time or periodical statistical information based on data types or grouping methods. All the statistical information can be filtered as needed to help you have a more detailed and accurate understanding of the resource allocation and network security status of system.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

User-defined monitor statistics include:

- Creating a stat-set
- Configuring the type of statistical data
- Configuring a data grouping method
- Configure a filter

Creating a Stat-set

To create a stat-set, in the global configuration mode, use the following command:

statistics-set *name*

- *name* – Specifies the name of the stat-set. The length is 1 to 31 characters.

After executing the above command, the system will create a stat-set with the specified name, and enter the configuration mode; if the name of the stat-set exists, the system will directly enter the stat-set configuration mode.

To delete the specified stat-set, in the global configuration mode, use the following command:

no statistics-set *name*

Configuring the Type of Statistical Data

The type of statistical data of stat-sets includes bandwidth, session, new session ramp-up rate, attack rate, virus number, intrusion count, URL hit, keyword block and application block. To configure the type of statistical data, in the stat-set configuration mode, use the following command:

target-data {bandwidth | session | rampup-rate | url-hit | application-block| attack-rate } [record-history] [root-vsys-only]

- **bandwidth | session | rampup-rate | url-hit | application-block | attack-rate** – Specifies the type of statistical data of stat-sets. It can be bandwidth, session, new session ramp-up rate, attack rate, virus number, intrusion count, URL hit, keyword block or application block and AD attack count.
- **record-history** – Monitors data of the last 30 days.
- **root-vsys-only** – Just monitors data of root VSYS. If this parameter is not configured, data of all VSYSs will be statistical.

To remove the configurations that specify the type of statistical data of the stat-set, in the stat-set configuration mode, use the following command:

no target-data



Notes: When configuring a stat-set, keep in mind that:

- The URL hit statistics are only available to users who have a URL license.
- Non-root VSYS only supports types including bandwidth, session, new session ramp-up rate and URL hit
- If you specified the root-vsys-only parameter, data grouping method cannot be configured to VSYS.

Configuring a Data Grouping Method

The data grouping methods of statistical set include IP, interface, security zone, application, user, URL, URL category and VSYS type. The actual options may vary from different date types. Non-root VSYS also supports grouping methods including IP, interface, security zone, application, user, URL and URL category.

To configure a data grouping method, in the stat-set configuration mode, use the following command:

group-by {[**ip** [**directional**] [**initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name*]] | **interface** [**directional**] | **zone** [**directional**] | **application** | **user** [**directional**] | **url** | **url-category** | **vsys**}

- **ip** – Specifies IP address as the data grouping method for the stat-set. You can use **initiator** | **responder** | **belong-to-zone** *zone-name* | **not-belong-to-zone** *zone-name* | **belong-to-interface** *interface-name* | **not-belong-to-interface** *interface-name*parameters to specify the IP range for the statistics. It can be the IP that initiates the session (**initiator**), the IP that receives the session (**responder**), the IP that belongs to a specific security zone (**belong-to-zone** *zone-name*), the IP that does not belong to a specific security zone (**not-belong-to-zone** *zone-name*), the IP that belongs to a specific interface (**belong-to-interface** *interface-name*), or the IP that does not belong to a specific interface (**not-belong-to-interface** *interface-name*).

- **directional** – Specifies the statistical results for both directions, i.e., when the data is grouped by IP, interface or security zone, the inbound and outbound traffic, the number of received and sent sessions, the ramp-up rate of new received and sent sessions will be gathered for the statistics respectively; if this option is not configured, the default statistics result is non-directional, i.e., when the data is grouped by IP, interface or security zone, all the traffic, sessions and ramp-up rate of news sessions will be gathered for the statistics.
- **interface** – Specifies interface as the data grouping method for the stat-set.
- **zone** – Specifies security zone as the data grouping method for the stat-set.
- **application** – Specifies application as the data grouping method for the stat-set. In such a case the type of statistical data should not be AD attack rate, URL hit count and keyword block count.
- **user** – Specifies user as the data grouping method for the stat-set.
- **url** – Specifies URL as the data grouping method for the stat-set.
- **url-category** – Specifies URL category as the data grouping method for the stat-set.
- **vsys** – Specifies VSYS as the data grouping method for the stat-set.

To cancel of the configurations that specify the data grouping method of the stat-set, in the stat-set configuration mode, use the following command:

no group-by

The following table lists statistical information based on IP type:

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
No direction	Initiator	Statistics on the traffic of the initiator's IP	Statistics on the session number of the initiator's IP	Statistics on the new sessions of the initiator's IP	Statistics on the URL hit count of the specified IPs	Statistics on the keyword block count of the specified IPs	Statistics on the application block count of the specified IPs
	Responder	Statistics on the traffic of the responder's IP	Statistics on the session number of the responder's IP	Statistics on the new sessions of the responder's IP			
	Belong to zone	Statistics on the traffic of an IP that belongs to a specific security zone	Statistics on the session number of an IP that belongs to a specific security	Statistics on the new sessions of an IP that belongs to a specific security			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
			zone	zone			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Not belong to zone	Statistics on the traffic of an IP that does not belong to a specific security zone	Statistics on the session number of an IP that does not belong to a specific security zone	Statistics on the new sessions of an IP that does not belong to a specific security zone			
	Belong to interface	Statistics on the traffic of an IP that belongs to a specific interface	Statistics on the session number of an IP that belongs to a specific interface	Statistics on the new sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the traffic of	Statistics on the session num-	Statistics on the new ses-			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		an IP that does not belong to a specific interface	ber of an IP that does not belong to a specific interface	sions of an IP that does not belong to a specific interface			
Bi-directional	Initiator	Statistics on the inbound and outbound traffic of the initiator's IP	Statistics on the number of received and sent sessions of the initiator's IP	Statistics on the new received and sent sessions of the initiator's IP			
	Responder	Statistics on the inbound and outbound traffic of the	Statistics on the number of received and sent sessions of the	Statistics on the new received and sent sessions of the			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		responder's IP	responder's IP	responder's IP			
	Belong to zone	Statistics on the inbound and outbound traffic of an IP that belongs to a specific security zone	Statistics on the number of received and sent sessions of an IP that belongs to a specific security zone	Statistics on the new received and sent sessions of an IP that belongs to a specific security zone			
	Not belong to zone	Statistics on the inbound and outbound traffic of an IP that	Statistics on the number of received and sent sessions of an IP	Statistics on the new received and sent sessions of an IP			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		does not belong to a specific security zone	that does not belong to a specific security zone	that does not belong to a specific security zone			
	Belong to interface	Statistics on the inbound and outbound traffic of an IP that belongs to a specific interface	Statistics on the number of received and sent sessions of an IP that belongs to a specific interface	Statistics on the new received and sent sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the inbound and out-	Statistics on the number of received	Statistics on the new received			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		bound traffic of an IP that does not belong to a specific interface	and sent sessions of an IP that does not belong to a specific interface	and sent sessions of an IP that does not belong to a specific interface			

The interface, zone, user, application, URL, URL category, VSYS type-based statistical information table.

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
Zone	No direction	Statistics on the traffic of the specified security	Statistics on the session number of the specified security	Statistics on the new sessions of the specified	Statistics on the URL hit count of the specified	N/A	N/A

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		zones	zones	security zones	security zones		
	Bi-directional	Statistics on the inbound and outbound traffic of the specified security zones	Statistics on the number of received and sent sessions of the specified security zones	Statistics on the new received and sent sessions of the specified security zones			
Interface	No direction	Statistics on the traffic of the specified interfaces	Statistics on the session number of the specified interfaces	Statistics on the new sessions of the specified interfaces	Statistics on the URL hit count of the specified interfaces	N/A	N/A
	Bi-directional	Statistics on the	Statistics on the	Statistics on the			

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		inbound and outbound traffic of the specified interfaces	number of received and sent sessions of the specified interfaces	new received and sent sessions of the specified interfaces			
Application	N/A	Statistics on the traffic of the specified applications	Statistics on the session number of the specified applications	Statistics on the new sessions of the specified applications	N/A	N/A	Statistics on the block count of the specified applications
User	No direction	Statistics on the traffic of the specified users	Statistics on the session number of the specified users	Statistics on the new sessions of the specified	Statistics on the URL hit count of the specified	Statistics on the keyword block count of	Statistics on the application block count of

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Bi-directional	Statistics on the inbound and outbound traffic of the specified users		users	users	the specified users	the specified users
URL	N/A	N/A	N/A	N/A	Statistics on the hit count of the specified URLs	N/A	N/A
URL Category	N/A	N/A	N/A	N/A	Statistics on the hit count of the spe-	N/A	N/A

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
					cified URL categories		
VSYS	N/A	Statistics on the traffic of the specified VSYSs	Statistics on the session number of the specified VSYSs	Statistics on the new sessions of the specified VSYSs	Statistics on the URL hit count of the specified VSYSs	N/A	N/A

Configuring a Filter

You can configure a filtering condition for the stat-set to gather statistics on the specified condition, such as statistics on the session number of the specified security zone, or the traffic of the specified IP.

Type	Description
filter zone	Data is filtered by security zone.
filter zone zone-name ingress	Data is filtered by ingress security zone.
filter zone zone-name egress	Data is filtered by egress security zone.
filter interface	Data is filtered by interface.
filter interface if-name ingress	Data is filtered by ingress interface.

Type	Description
filter interface if-name egress	Data is filtered by egress interface.
filter application	Data is filtered by application.
filter ip	Data is filtered by address entry.
filter ip add-entry source	Data is filtered by source address (address entry).
filter ip add-entry destination	Data is filtered by destination address (address entry).
filter ip A.B.C.D/M	Data is filtered by IP.
filter ip A.B.C.D/M source	Data is filtered by source IP.
filter ip A.B.C.D/M destination	Data is filtered by destination IP.
filter user	Data is filtered by user.
filter user-group	Data is filtered by user group.
filter role	Data is filtered by user role.
filter service	Data is filtered by service.

To configure a filter, in the stat-set configuration mode, use the following command:

filter {**ip** {*A.B.C.D/M* | *address-entry*} [**source** | **destination**] | **interface** *name* [**ingress** | **egress**] | **zone** *name* [**ingress** | **egress**] | **application** *name* | **user** *user-name aaa-server-name* | **user-group** *user-group-name aaa-server-name* | **role** *role-name* | **service** *service-name*}

- **ip** {*A.B.C.D/M* | *address-entry*} – Specifies an IP as the filter. The IP can be an IP address range (for example, 10.101.0.1, 255.255.255.0 or 10.101.0.1/24) or an address entry defined in the system address book. If IPv6 is enabled, system will support to monitor items of IPv6 address.

    - **source|destination** – Specifies a source IP address or destination IP address as the filter.
- **interface** *name* – Specifies an interface as the filter.
    - **ingress | egress** – Specifies an ingress interface or egress interface as the filter.
- **zone** *name* – Specifies a security zone as the filter.
    - **ingress | egress** – Specifies an ingress or egress of a security zone as the filter.
- **application** *name* – Specifies an application as the filter.
- **user** *user-name aaa-server-name* – Specifies a user as the filter.
- **user-group** *user-group-name aaa-server-name* – Specifies a user group as the filter.
- **role** *role-name* - Specifies a user role as the filter.
- **service** *service-name* - Specifies a service as the filter.

Repeat the command to configure multiple filters. The system supports up to 32 filters for each stat-set, among which the number of filters for each type of the user, user group and role filters cannot exceed 8. If multiple filters configured for the same stat-set belong to the same type, then the logical relationship among these conditions will be OR; if they belong to different types, the logical relationship among these conditions will be AND.

To delete the specified type of filters, in the stat-set configuration mode, use the following command:

no filter {**ip** {*A.B.C.D/M* | *address-entry* } [**source** | **destination**] | **interface** *name* [**ingress** | **egress**] | **zone** *name* [**ingress** | **egress**] | **application** *name* | **user** *user-name aaa-server-name* | **user-group** *user-group-name aaa-server-name* | **role** *role-name* | **service** *service-name*}

To delete all types of filters, in the stat-set configuration mode, use the following command:

no filter all

Enabling/Disabling Stat-set

By default all the predefined stat-set for user monitor, application monitor, device monitor are disabled except for the stat-set of bandwidth.

To enable or disable a stat-set, in the stat-set configuration mode, use the following commands.

- Enable: **active**
- Disable: **no active**



Tip: After the above command is executed in the root VSYS, specified predefined stat-set of all VSYSs will be enabled or disabled（except that the non-root VSYS does not support this predefined stat-set）. You can not enable or disable their own predefined stat-set in non-root VSYSs.

Viewing Stat-set Information

To view the configuration information of the predefined and user-defined stat-set, in any mode, use the following command:

show statistics-set *name* [{**current** | **history** | **history-max**}[**IPv4** | **IPv6**] [**sort-by** {**up** | **down** | **item**}]]

- **show statistics-set** – Shows the configuration information of all the stat-sets in the system.
- *name* – Specifies the name of the stat-set to show the configuration information of the stat-set.
- **current** | **history** | **history-max** – Shows specific statistics of the specified stat-set, including:
  - **current** – Shows the current statistics of the specifies stat-set.
  - **history** – Shows historic statistics of the specified stat-set. The system samples data every five minutes.

    - **history-max** – Shows historic maximum statistics of the specified stat-set. This parameter is only applicable to stat-set of session type.
- **IPv4 | IPv6** – Shows specific statistics of the specified address type.
- **sort-by {up | down | item}** – Specifies the sorting method for the statistics of the specified stat-set (in a descending order of the file size).
    - **up** - Sorted by outbound data.
    - **down** – Sorted by inbound data (only when the Group by is configured with Bi-directional parameters).
    - **item** - Sorted by Group by objects.

Diagnostic Center

The system supports the Diagnostic Center function. This function can be used to collect statistics of packet loss of different functional modules, which helps you identify issues. The detailed function is described as follows.

- Supports statistics on packet loss of functional modules. The packet loss statistics are displayed in lists, bar charts, or line charts.
- Allows you to view detailed packet loss statistics of functional modules, including the time of packet loss, 5-tuple (source IP, source port, destination IP, destination port, and protocol type), and module of packet loss.
- Allows you to manually enable the collection of 5-tuple statistics of packet loss or set the threshold to trigger packet loss statistics collection.
- Supports the storage of packet loss statistics to device disks. You can set limits on the size of the statistics storage space. For more information, see Storage Management.



Notes: The Diagnostic Center function is available only for SG-6000 A-Series devices installed with hard disks.

Always Collecting 5-Tuple Statistics of Packet Loss

You can enable the function of always collecting 5-tuple statistics of packet loss. This way, the system will always collect the 5-tuple statistics of packet loss of all functional modules (source IP, source port, destination IP, destination port, and protocol type). To enable this function, run the following command in the global configuration mode:

module-drop-counter force-cap-packet enable

In the global configuration mode, run the **no module-drop-counter force-cap-packet enable**command to disable the function of always collecting 5-tuple statistics of packet loss.



Notes: After the function of always collecting 5-tuple statistics of packet loss is enabled, the packet loss threshold of functional modules and packet loss growth rate threshold do not take effect.

Configuring a Packet Loss Threshold

You can configure a packet loss threshold for functional modules. If the packet loss count of a functional module exceeds the threshold, it is determined the packet loss is abnormal and the 5-tuple of abnormal packet loss is recorded. To configure a packet loss threshold, run the following command in the global configuration mode:

module-drop-counter module *module-name* **threshold** *number*

- *module-name* - Specifies the name of the functional module.
- *number* - Specifies the packet loss threshold. Valid values: 0 to 20000. Default value: 0, which indicates that no threshold is specified and the 5-tuple statistics of packet loss are always collected.

In the global configuration mode, run the *module-name* command to reset the packet loss threshold to the default value.

Configuring a Packet Loss Growth Rate Threshold

You can configure a packet loss growth rate threshold for functional modules. If the packet loss growth rate of a functional module exceeds the threshold, it is determined the packet loss is abnormal and the 5-tuple of abnormal packet loss is recorded. To configure a packet loss growth rate threshold, run the following command in the global configuration mode:

module-drop-counter growth-rate *number*

- *number* - Specifies the packet loss growth rate threshold. Valid values: 0 to 100. Default value: 0, which indicates that no threshold is specified and the 5-tuple statistics of packet loss are always collected.

In the global configuration mode, run the **no module-drop-counter growth-rate** command to reset the packet loss growth rate threshold to the default value.

Long-term Monitor

The system supports the long-term monitor function. This function can be used to continuously monitor and collect statistics on device traffic and sessions and then store these statistics, which meets your requirements for network monitoring and diagnostics. The detailed function is described as follows.

- Supports the storage of statistics for device traffic and sessions over the last 180 days to the device disks. You are allowed to set limits on the size of the statistics storage space.
- Supports query by IP or application type. You can query data from a maximum of 31 consecutive days within the last 180 days.
- Supports the display of statistics in lists, bar charts, and line charts.



Notes: The long-term monitor function is available only for SG-6000 A-Series devices installed with hard disks and SG-6000 K-Series devices installed with hard disks (excluding SG-6000-K9180).

Enabling/disabling Long-term Monitor

By default, the Long-term Monitor function is disabled. To enable/disable this function, run the following command in the global configuration mode:

statistics-long-term {**enable** | **disable**}

- **enable** - Enable the Long-term Monitor function.
- **disable** - Disable the Long-term Monitor function.

Logs

Overview

Devices are designed with the log function. System records and outputs various system logs, including event logs, threat logs, configuration logs, operation logs, network logs, data security logs (file filter logs, content filter logs, network behavior record logs), traffic logs and debug logs.

- Event logs - Event logs are divided into eight severity levels: errors, warnings, notification, informational, emergencies, alerts, critical and debugging. For more information about log severity, see Log Severity.
- Configuration logs - Configuration logs describe the changes of configurations, e.g. configurations on interfaces.
- Operation logs - Logs related with clear command, exec command and some corresponding WebUI operations, such as the delete operation of NBT cache.
- Network logs - Network logs record operations of network services, e.g. PPPoE and DDNS.
- Threat logs - Threat logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- File filter logs – Logs related with file filter function.
- Content filter logs – Logs related with content filter function, e.g. file content filter, Web content filter, Web posting, Email fileter and HTTP/FTP control.
- Network behavior record logs – Logs related with network behavior record function, e.g. IM behavior, aetc.
- Cloudsandbox logs – Logs related with sandbox function.

- Traffic logs - Traffic logs consist of session logs, NAT logs, and web surfing logs
    - Session logs - Session logs, e.g. session protocols, source and destination IP addresses and ports.
    - NAT logs - NAT logs, including NAT type, source and destination IP addresses and ports.
    - URL logs - logs about network surfing, e.g. Internet visiting time, web pages visiting history, URL filteringing logs.
- Debug logs - Debug logs record the system debugging information.

The log function of StoneOS is a tool to show device operation status, providing evidence for you to analyze the network and protect against network attacks.



Tip: For T Series platforms:

- The root VSYS doesn't support data security logs.
- The non-root VSYS doesn't support data security logs and debug logs.

Log Severity

Event logs categorize system events by severities. The eight severities are described as follows:

Severity	No.	Description	Log Definition
Emergencies	0	Identifies invalid system events.	LOG_EMERG
Alerts	1	Identifies problems which need immediate attention, e.g., the device is being attacked.	LOG_ALERT
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT

Severity	No.	Description	Log Definition
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_DEBUG

Log Output

Log messages can be sent to the following destinations. You can specify one of them at your own choice:

- Console - The console port of the device. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.
- File - By default, StoneOS creates a file to record log messages. You can also specify a file in a USB destination to output log messages.
- Syslog Server - Sends logs to a UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Localdb - Sends logs to the local database of the device.
- SMS - Sends logs to the specifies mobile phone in form of a SMS message.

Event logs can be sent to all the above destinations except for Localdb; threat logs can be sent to all the above destinations except for SMS and Localdb; traffic logs can be sent to console, buffer,

syslog server, and file; network and debug logs can only be sent to console, buffer and syslog server.

Log Format

To facilitate the access and analysis of the system logs, StoneOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**. See the example below:

2018-02-05 01:51:21, WARNING@LOGIN: Admin user "hillstone" logged in through console from localhost.

Configuring System Logs

You can configure the following log options via CLI:

- Enabling and disabling the log function
- Sending and filtering event logs
- Sending threat logs
- Sending configuration, debug and network logs
- Sending traffic logs
- Sending data security logs (file filter logs, content filter logs, network behavior record logs)
- Sending Cloudsandbox logs
- Sending EPP logs
- Sending IoT Logs
- Configuring the function of storing logs on the hard disk
- Configuring a Syslog Server
- Specify the Sending Sourceport Number
- Specifying the Facility Field of Log Messages

- Displaying hostname/username in the traffic logs
- Displaying Username in the Threat Logs
- Sending Logs to an Email Account
- Configuring Log Parameter
- Enabling/Disabling the Record User Information Function for Threat Log
- Viewing log configurations
- Viewing logs
- Exporting logs
- Clearing logs

Enabling/Disabling the Log Function

By default, the traffic logs are disabled (enabling the above logs will affect system performance). To enable or disable a system log, in the global configuration mode, use the following command:

- Enable:**logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **url-filter**} | **debug** | **threat** | **email** | **data-security [dlp** | **cf** | **nbr]**} **on**
- Disable: **no logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **urlfilter**} | **debug** | **threat**| **email** | **data-security [dlp** | **cf** | **nbr]**} **on**

Sending and Filtering Event Logs

You can specify the output destination for the event logs as needed, and filter the output logs based on the severity.

To send event logs to the console, remote terminal, syslog server, mobile phone, hard-disk card or enable email notification, and filter the output logs, in the global configuration mode, use the following command:

logging event to {**console** | **remote** | **syslog**| **sms** | **email** | **localdb** } [**severity** *severity-level*]

- **console** – Sends the event logs to the console.
- **remote** – Sends the event logs to the remote terminal.
- **syslog** – Sends the event logs to the Syslog Server.
- **sms** – Sends the event logs whose severity is Critical or is higher than Critical to the mobile phone by using SMS.
- **email** – Sends the event logs to the Email.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.

To disable the function, in the global configuration mode, use the following command:

no logging event to {**console** | **remote** | **syslog** | **sms** |**email** | **localdb**}

To send the event logs to the memory buffer and filter the logs, in the global configuration mode, use the following command:

logging event to buffer [**severity** *severity-level*] [**size** *buffer-size*]

- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors

severities.

- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to buffer**.

To write the event logs to a file and filter the logs, in the global configuration mode, use the following command:

logging event to file [**severity** *severity-level*] [**name** [**usb0** | **usb1**] *file-name*] [**size** *file-size*]

- **severity** *severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only write event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to file**.

Configuring SMS

You can specify to send event logs whose severity is Critical or is higher than Critical to the specified mobile phone in form of SMS. To do this, you need to configure the mobile phone number used to receive logs and the mode of sending SMS messages.

Configuring a Mobile Phone Number

To specify the mobile phone number that is used to receive the event logs, in the global configuration mode, use the following command:

logging sms *phone-number*

- *phone-number* – Specifies the phone number that is used to receive event logs.

To cancel the specified phone number, in the global configuration mode, use the command **no logging sms** *phone-number*.

Specifying the Mode of Sending SMS Messages

To specify the mode of sending SMS messages, in global configuration mode, use the following command:

logging sms send-mode {**modem** | **gateway***sp-name* | **disable**}

- **modem** – Specifies to send logs to the mobile phone by using sms modem.
- **gateway***sp-name* – Specifies to send logs to the mobile phone by using sms gateway. You can use the Tab key after the **gateway** parameter to view the existing SP instance list of sms gateway and enter the selected SP instance name.
- **disable**- Disable the function of sending logs by SMS.

Sending Threat Logs

You can specify the output destination for the threat logs as needed. To send threat logs to the console, remote terminal, syslog server, hard-disk or enable email notification, in the global configuration mode, use the following command:

logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]] | **email** | **localdb** } [**severity** *severity-level*]

- **console** – Sends the threat logs to the console.
- **remote** – Sends the threat logs to the remote terminal.

- **syslog** – Sends the threat logs to the Syslog Server.
- **custom-format** – Sends the log messages in plaintext. By default, the system sends the log messages in plaintext.
- **distributed** – Sends the log messages to multiple syslog servers in the distribution mode.
- **src-ip-hash** | **round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **email** – Sends the threat logs to the Email.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
- **severity***severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only write event logs of Notifications, Warnings and Errors severities.

To disable the function, in the global configuration mode, use the following command:

no logging threat to {**console** | **remote** | **syslog** | **email**| **localdb** } [**severity** *severity-level*]

To send the threat logs to the memory buffer, in the global configuration mode, use the following command:

logging threat to buffer [**severity** *severity-level*] [**size** *buffer-size*]

- **severity** *severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity

is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.

- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to buffer**.

To write the threat logs to a file, in the global configuration mode, use the following command:

logging threat to file [**severity** *severity-level*] [**name** [**usb0** | **usb1**] file-name] [size file-size]

- **severity** *severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to file**.

Sending Configuration/Operation/Debug/Network Logs

You can specify the output destination for the configuration, debug and network logs as needed.

To send configuration, operation, debug or network logs to the console, syslog server, memory buffer , file or local database, in the global configuration mode, use the following command:

logging {**configuration** | **network**} **to** {**console** | **syslog** | **localdb** }

- **configuration | network** – Specifies the type of the logs that will be sent. The available options include configuration and network.
- **console** – Sends the logs to console.
- **syslog** - Sends the logs to syslog server.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.

logging [debug | operation]to {console | syslog}

- **console** – Sends the debug and operation logs to console.
- **syslog** - Sends the logs to syslog server.

To disable the function, in the global configuration mode, use the command **no logging {configuration| operation | debug | network} to {console | syslog | localdb}**

To write the configuration , operation or network logs to a file, in the global configuration mode, use the following command:

logging {configuration | operation | network} to file [name [usb0 | usb1] *file-name*] [**size** *file-size*]

- **configuration | operation | network** – Specifies the log type.
- **name [usb0 | usb1]** *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size** *file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging {configuration | operation | network} to file**.

To send configuration, operation, debug or network logs to the memory buffer, in the global configuration mode, use the following command:

logging {configuration | operation | debug | network} to buffer [size *buffer-size*]

- **configuration | operation | debug | network** – Specifies the type of the logs that will be sent. The available options include configuration, debug and network.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging {configuration | operation | traffic | debug | network} to buffer**.

When you send debug logs to the memory cache, if the log information exceeds the memory cache space, new log information will overwrite earlier log information by default. You can configure that when the log information exceeds the memory cache space, new log information will not overwrite earlier log information. To do this, in global configuration mode, use the following command:

- **logging debug-buffer stop-overwrite**: When the log information exceeds the memory cache space, the system will stop storing new debug log information.
- **no logging debug-buffer stop-overwrite**: The debug log information that exceeds the memory cache space will automatically overwrite earlier log information.

In any mode, you can use the **show logging** command to view whether new debug log information overwrites earlier debug log information when the log information exceeds the memory cache space.

Example:

```
hostname(config)# show logging
Logging facility: local7
Debug log status: On
================================================
Destination Status Size Overwrite
------------------------------------------------
Console Off - -
```

```
Buffer On 524288 no (When the log information exceeds
the memory cache space, new debug log information does
not overwrite earlier debug log information)
File Off 1048576 -
Syslog Off - -
================================================
```

Sending Debug Logs to a File

You can send the debug logs to a fileand then run the **export log debug** command to the specified file server or USB disk. For details on how to export to a specific file server or USB disk, see Exporting Logs. By default, the system will not send the debug logs to a file. To enable the system to send the debug files to a file, in the global configuration mode, use the following command:

logging debug to file

To specify the size of the file to which the debug logs will be sent, in the global configuration mode, use the following command:

logging debug to file size *file-size*

- **size** *file-size* – Specifies the size of the file to which the debug logs will be sent. The size range and default value vary by device models.

In the global configuration mode, use the **no logging debug to file** command to disable the system from sending debug logs to a file.

In any mode, use the **show logging debug file** command to view the content of the debug log file that the system has sent.

Configuring the Conditions of Using the Debug Function

When the debug function is enabled, the CPU usage might increase and affect service forwarding. You can configure the work priority of the debug function and service forwarding as required. By default, the debug function's priority is higher than service forwarding.

To make service forwarding take precedence over the debug function, in the global configuration mode, use the following command:

log debug-limit cpu-threshold *value*

- *value* - Specifies the threshold for the CPU usage, in percent. The value range is 0 to 99. When 0 is specified, the debug function takes precedence over service forwarding. When other value is specified, service forwarding takes precedence over the debug function. In the scenario where service forwarding take precedence over the debug function, if the system has multiple CPUs, when the usage of any CPU reaches the specified threshold, the system will considers that the debug function has affected service forwarding and therefore disables it.

To make the debug function take precedence over service forwarding, in the global configuration mode, use the **no log debug-limit cpu-threshold** or **log debug-limit cpu-threshold 0** command.

When enabling the debug function, you can configure a timer to control the execution time length allowed for the debug function. When the timer elapses, the debug function will be disabled. In the global configuration mode, use the following command:

log debug-limit time *value*

- *value* - Specifies the execution time length of the debug function. The value range is 1 to 60s.

To cancel the execution time length configuration of the debug function, use the **no log debug-limit time** command in the global configuration mode.

Note: When both service first and execution timer are configured, the debug function will be disabled when any of the conditions is met.

Sending Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. You can send traffic logs to the console, syslog server, memory buffer and local SSD (Web surfing logs cannot be sent to SSD). You can select the output destination according to your requirements.

To send the traffic logs to the console , buffer or syslog server, use the following command in the global configuration mode:

logging traffic {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** [**size** *buffer-size*] }

To send session logs and NAT logs to the local SSD, in the global configuration mode, use the following command:

logging traffic {**session** | **nat**} **to localdb**}

- **session** | **nat** | **urlfilter** – Specifies the log type that you want to output.
- **console** | **syslog** | **buffer** – Specifies the output destination. You can output the logs to the console ,buffer or syslog server.
- **localdb** – Specifies the output destination of session logs and NAT logs as the SSD on the device. Web surfing logs cannot be sent to the local SSD. Only CloudEdge, SSD-equipped A-series (except A2200, A1800, and A1600) and X-series devices support this function.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

In the global configuration mode, use the following command to disable the output function: **no logging traffic** {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** }or **no logging traffic** {**session** | **nat**} **to localdb**.

Sending Data Security Logs

You can specify the output destination for the data security logs (file filter logs, content filter logs, network behavior record logs) as needed. To send data security logs (file filter logs, content filter logs, network behavior record logs)to the console, remote terminal, syslog server, local database, or enable email notification, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog**[**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]] }

- **console** – Sends the data security logs to the console.
- **syslog** – Sends the data security logs to the Syslog Server.
- **binary-format** – Sends the logs in binary format.

- **distributed** – Sends the logs to multiple servers in the distribution mode.
- **src-ip-hash | round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and**round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **custom-format** – Sends the logs in plaintext. By default, the system sends the logs in plaintext.

To disable the function, in the global configuration mode, use the following command:

no logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog** }

To send the data security logs (file filter logs, content filter logs, network behavior record logs) to the memory buffer, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to buffer** [**size** *buffer-size*]

- **size** *buffer-size* – Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 524288.

To disable the function, in the global configuration mode, use the command **no logging data-security** [**dlp** | **cf** | **nbr**] **to buffer**.

Sending Cloudsandbox logs

You can specify the output destination for the Cloudsandbox logs as needed. To send Cloudsandbox logs to the console, buffer, syslog server, and file. Before you send cloudsandbox logs, you need to enable the Sandbox function in the global configuration mode:

logging sandbox on

In the global configuration mode, use**no logging sandbox on** command to disable Sandbox function.

To specify the output destination for the Cloudsandbox logs, in the global configuration mode, use the following command:

logging sandbox to {**console** | **syslog** | **buffer** [**size** *buffer-size*] | **file** *file-name* [**size** *file-size*]}

- **console** – Sends the cloudsandbox logs to the console.
- **syslog** – Sends the cloudsandbox logs to the Syslog server.
- **buffer** [**size** *buffer-size*] - Sends the cloudsandbox logs to buffer and specify the buffer size. The value range is 4096 to 524288 bytes. The default value is 524288.
- **file** *file-name* [**size** *file-size*] - Specifies the name or size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576bytes. The default value is 1048576.

In the global configuration mode, use **no logging sandbox to** {**console** | **syslog** | **buffer** | **file**}command to disable the function.

Sending EPP logs

You can specify the output destination for the EPP logs as needed. To send EPP logs to the console, buffer, syslog server, file, remote terminal and Email. Before you send EPP logs, you need to enable the EPP logs function in the global configuration mode:

logging epp on

In the global configuration mode, use **no logging epp on** command to disable EPP logs function.

To specify the output destination for the EPP logs, in the global configuration mode, use the following command:

logging epp to {**console** | **syslog** | **buffer** [**size***buffer-size*] | **file** *file-name* [**size***file-size*] | **remote** | **email**}

- **console** – Sends the EPP logs to the console.
- **syslog** – Sends the EPP logs to the Syslog server.
- **buffer** [**size***buffer-size*] - Sends the EPP logs to buffer and specify the buffer size. The value range is 4096 to 524288 bytes. The default value is 524288.

- **file** *file-name* [**size***file-size*] - Specifies the name or size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576bytes. The default value is 1048576.
- **remote** – Sends the EPP logs to the remote terminal.
- **email** – Sends the EPP logs to the Email.

In the global configuration mode, use **no logging epp to** {**console** | **syslog** | **buffer** | **file**| **remote** | **email** } command to disable the function.

Sending IoT Logs

IoT logs can be sent to the console, buffer and syslog server. You can specify the output destination for IoT logs as needed. Before you specify the output destination, in the global configuration mode, you need to enable the IoT logs function with the following commands:

logging iot-monitor on

In the global configuration mode, use **no logging iot-monitor on** to disable the IoT logs function.

To send IoT logs to console, buffer and syslog server, in the global configuration mode, use the following command:

logging iot-monitor to {**console** | **buffer** [**size***buffer-size*] | **syslog** [**custom-format** [**distributed** [**src-ip-hash** | **round-robin**]]]}

- **console** – Sends IoT logs to the specified console.
- **syslog** – Sends IoT logs to the specified syslog server. For how to configure the syslog server, refer to Configuring Syslog Server.
- **custom-format** – Sends IoT logs in the plain text. By default, system sends logs in the plain text.
- **distributed** – Distributes IoT logs in the plain text to several syslog servers.

- **src-ip-hash | round-robin** – Specifies the algorithm, including **src-ip-hash** and **round-robin** (the default algorithm).

In the global configuration mode, use the following command to disable the function.

no logging iot-monitor to {console | buffer | syslog}

Configuring the Output Log Format

StoneOS logs follow a fixed pattern of information layout. By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, i.e. **<Device Number*8+log severity> date/time SN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

Output example of logs in the default format: <188> Apr 11 02:48:22 25083xxxxxx05643(root) 42340401 HillstoneNetworks#Event@MGMT: Admin user "hillstone" cleared Debug log\n\000



Tips: Based on the log standard defined by RFC 3164/5424:

- Standard format: **<Device Number*8+log severity> date/timehostname log ID HillstoneNetworks#log type@module: descriptions**
- Non-standard format: **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

You can configure the output log format as needed. In the the global configuration mode, use the following command:

- Display the four digit year: **logging syslog 4digit-year-timestamp**

  The output format is: **<Device Number*8+log severity> four digit year-date/time time zone SN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

  Sample output: <188> 2024-04-11T02:49:23.380569Z 25083xxxxxx05643(root) 421c041f

HillstoneNetworks#Event@MGMT: Admin user "hillstone" logout through SSH, the IP is X.X.X.X, and the corresponding login time is 2024-04-11 02:43:25.\n

- Display the hostname and the log severity: **logging syslog additional-information**
  The output format is: **<Device Number*8+log severity> date/timeSN(VSYS name)[h:host-name][p:log severity] log ID HillstoneNetworks#log type@module: descriptions**
  Sample output: <186> Apr 11 02:50:46 25083xxxxxx05643(root)[h:SG-6000][p:2] 42080a0d HillstoneNetworks#Event@MGMT: hillstone save system configuration via SSH.\n\000
- Display the hostname and not display the device SN.
  1. In global configuration mode, enter the configuration mode of the specified log server: **logging syslog-server***server-name*
  2. In configuration mode of the specified log server, enter **hostname standard**
     The output format is: **<Device Number*8+log severity> date/time hostname log ID HillstoneNetworks#log type@module: descriptions**
     Sample output: <189> Apr 11 02:46:32 SG-6000 43240501 Hill-stoneNetworks#Event@NET: Static entry is created, 1.1.1.1, 1111.1111.1111, trust-vr\n\000

To cancel the displaying of four digit year /hostname/ log severity, and restore the default log format in the the global configuration mode, use the following command:

- Cancel display the four digit year: **no logging syslog 4digit-year-timestamp**
- Cancel display the hostname and the log severity: **no logging syslog additional-information**
- Display the device SN and cancel display the hostname: In configuration mode of the specified log server, enter **no hostname standard**

Configuring the Function of Storing Logs on the Hard Disk

SG-6000-X9180 supports to store log files on the hard disk. To configure this function, in the global mode, use the following command:

logging {**event** | **config** | **network** | **threat** | **sandbox**} **to file harddisk severity** *severity-level*

- **event** | **config** | **network** | **threat** | **sandbox** - Specifies the log types to be stored on the hard disk. Log types include event logs, configuration logs, network logs, threat logs, and sandbox logs.
- **severity** *severity-level* - Specifies the severity of logs to be stored on the hard disk. Logs of specified and higher severity will be stored on the hard disk, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, the system will store logs of Notice, Warnings, and Errors severity on the hard disk.

Use the command**no logging** {**event** | **config** | **network** | **threat** | **sandbox**} **to file harddisk** to cancel the configuration of this function.

Configuring the Log Backup Server

You can configure a log backup server to back up deleted logs to a specified server. This function is supported by K-series devices that are installed with SSD.

In the global configuration mode, use the following command:

logging storage-mgmt localdb backup-to-server {*server-ip* **user** *user-name* **password** *password filename*}

Use the command**no loggingstorage-mgmt localdb backup-to-server**to cancel the configuration of this function.

Optimizing the Function of Exporting Session Logs and NAT Logs to the Local Disk

Typically, the system's log processing process (LOGD) and database storage process (MYSQLD) work on Core0 of the CPU. When session logs and NAT logs are exported to the local disk, Core0 can be overloaded with a large amount of high speed log data storage operations, potentially affecting the normal operation of other functional modules. To solve this problem, when session logs and NAT logs are exported to the local disk, you can move log processing process and database storage process from Core0 to Core MAX and limit the speed at which logs are sent to the log processing process. Core MAX is the CPU core with the largest number. For example, if the system has 12 CPU cores in total, which are numbered as Core0 to Core11, Core11 is the Core MAX.

It is recommended that when exporting session logs and NAT logs to the local disk, if the performance consumption of Core0 is too high or you need to increase the speed at which logs are sent to the log processing process, you can move log processing process and database storage process from Core0 to Core MAX, and then configure the speed at which logs are sent to the log processing process.

Binding the Log Processing Process and Database Storage Process to Core MAX

To bind the log processing process and database storage process to Core MAX, use the following command in the global configuration mode:

cp-multi-cores logd

In the global configuration mode, use command **no cp-multi-cores logd** to clear the binding of processing process and database storage process to Core MAX.



Notes:

- The function of binding the log processing process and database storage process to Core MAX is only supported by SG-6000-A2700 and later models.

- After bind the log processing process and database storage process to Core MAX or clear the binding, restart the device to make the configuration take effect.
- Before binding the log processing process and database storage process to Core MAX, you should use the command **flow-core-num** *number* in the global configuration mode to specify the number of CPU cores occupied by the system data. *number* is recommended to be max_core_number-1. max_core_number is the number of total CPU cores of the system. For example, if the system has 12 CPU cores in total, the command is **flow-core-num 11**. Restart the device to make the configuration take effect.

Configuring the Speed at Which Logs are Sent to Log Processing Process

To configure the speed at which logs are sent to log processing process, use the following command in the global configuration mode:

logging speed-limit to local *value*

- *value* - Specifies the speed at which logs are sent to log processing process. For details, refer to the following table.

Device	Value (piece/second)
SG-6000-A5100 and later models	Value ranges from 1000 to 15000. Value is set in interval of 1000. For example, 1000, 2000, and 3000. The default value is 8000.
SG-6000-A3800	Value ranges from 1000 to 8000. Value is set in interval of 1000. For example, 1000, 2000, and 3000. The default value is 5000.
SG-6000-A3700 and	Value ranges from 1000 to 5000. Value is set in interval of 1000. For example, 1000, 2000, and 3000. The default

Device	Value (piece/second)
former models	value is 2000.

In the global configuration mode, use command **no logging speed-limit** to restore to the default speed at which logs are sent to log processing process.

The function of configuring the speed at which logs are sent to log processing process is only supported by SG-6000 A series devices.

To view configuration of the speed at which logs are sent to log processing process, use the following command in any mode:

show logging speed-limit

Configuring a Syslog Server

To send logs to a Syslog Server, you need to configure the following information:

- Creating a Syslog Server
- Configuring the IP address or host name of the Syslog Server
- Specifying the binding method
- Specifying the log format of the Syslog Server
- Specifying the protocol type
- Specifying the destination port number
- Enabling/Disabling the Syslog_Server Certificate Check Disable function
- Specifying the type of generated logs
- Specifying a description for the Syslog Server

Creating a Syslog Server

To configure a Syslog Server, you need to enter the Syslog Server configuration mode. To do this, in global configuration mode, use the following command:

logging syslog-server*server-name*

- *server-name* – Specifies the name of the Syslog Server, which needs to be 1 to 127 characters in length.

After you run this command, the system creates the Syslog Server with the specified name and enters the Syslog Server configuration mode. If the specified name already exists, the system directly enters the Syslog Server configuration mode.

To delete the specified Syslog Server, in global configuration mode, use the no form of the command above:

no logging syslog-server*server-name*

Configuring the IP Address/Host Name of the Syslog Server

To configure the IP address or host name of the Syslog Server, in Syslog Server configuration mode, use the following command:

server { **ip***ip-address* | **hostname***hostname*}

- **ip***ip-address* | **hostname***hostname* – Specifies the IP address or host name of the Syslog Server.

To delete the IP address or host name of the specified Syslog Server, in Syslog Server configuration mode, use the no form of the command above:

no server { **ip** | **hostname** }

Specifying the Binding Method

To specify the VRouter to which the Syslog Server belongs or specify the source interface that sends logs, in Syslog Server configuration mode, use the following command:

bind {**vrouter***vr-name* | **source-interface***interface-name*}

- **vrouter***vr-name* – Specifies the name of the VRouter.
- **source-interface***interface-name* - Specifies the source interface that sends logs. The device uses the IP address of this interface as the source IP address to send logs to the log server. If the interface is configured with a management IP address, this IP address is preferentially used.

To delete the specified VRouter or source interface, in Syslog Server configuration mode, use the no form of the command above:

no bind {**vrouter** | **source-interface**}

Specifying the Log Format of the Syslog Server

To specify the log format of the Syslog Server, including CUCC, SGCC-S5000, and SGCC-S6000, in Syslog Server configuration mode, use the following command:

format-type { **CUCC** [**support-default**] | **SGCC-S5000** | **SGCC-S6000** }

- **CUCC** [**support-default**] - Specifies the format in which logs are sent. **CUCC** indicates to send NAT444 logs in a special format (China Unicom log format). **support-default** indicates to send other types of logs in the default format.
- **SGCC-S5000**- Specifies that the Syslog Server can receive logs only in the SGCC-S5000 format, such as the State Grid log server.
- **SGCC-S6000**- Specifies that the Syslog Server can receive logs only in the SGCC-S6000 format, such as the State Grid network monitoring device.

To delete the specified log format, in Syslog Server configuration mode, use the no form of the command above:

no format-type

Specifying the Protocol Type

To specify the protocol type of the Syslog Server, in Syslog Server configuration mode, use the following command:

protocol {**tcp** | **udp** | **secure-tcp**}

- **tcp** | **udp** | **secure-tcp** – Specifies the protocol type. Valid values: TCP, UDP, and Secure-TCP. The Secure-TCP uses the TLS encryption protocol.

To delete the specified protocol type, in Syslog Server configuration mode, use the no form of the command above:

no protocol

Specifying the Destination Port Number

To specify the destination port number of the Syslog Server, in Syslog Server configuration mode, use the following command:

dst-port*port-number*

- *port-number* – Specifies the destination port number.

To delete the specified destination port number, in Syslog Server configuration mode, use the no form of the command above:

no dst-port

Enabling/Disabling the Syslog_Server Certificate Check Disable Function

If the protocol type of the Syslog Server is set to **secure-tcp**, you can enable the function of Syslog_Server Certificate Check Disable. In other words, you can transferring logs without the need to verify the certificate. To enable or disable the function, in Syslog Server configuration mode, use the following command:

- Enable: **server-cert-check-disable**
- Disable: **no server-cert-check-disable**

Specifying the Type of Generated Logs

To specify the type of logs to be sent to the log server, in Syslog Server configuration mode, use the following command:

log-enable*log-type* [*log-subtype*]

- *log-type* - Specifies the log type.
- *log-subtype* - For a log type that contains subtypes, you need to specify this parameter to specify the log subtype.

To delete the specified log type, in Syslog Server configuration mode, use the no form of the command above:

no log-enable*log-type* [*log-subtype*]

Specifying a Description for the Syslog Server

To add a description for the Syslog Server, in Syslog Server configuration mode, use the following command:

description*description*

- *description* – Specifies the description for the Syslog Server, which needs to be 1 to 255 bytes in length.

To delete the description for the Syslog Server, in Syslog Server configuration mode, use the no form of the command above:

no description

Specifying the Sending Sourceport Number

The system supports to specify the sending sourceport number used to send log messages to the Syslog Server. When the sending sourceport number is specified, the system will use the specified sending sourceport to send log messages to the Syslog Server. If the sending sourceport number is not specified, the system will use the random sourceport to send log messages to the Syslog Server by default.

To specify the sending sourceport number, in the global configuration mode, use the following command:

logging syslog {**src-port** *port-number*}

- **src-port***port-number* - Specify the sending sourceport number used to send log messages to the Syslog Server. The range is from 1024 to 65535.

To cancel the specification of the sending sourceport number and use random sourceport by default, in the global configuration mode, use the negative form of the above command as follows:

no logging syslog {**src-port***port-number*}



Notes:

- The client can only check the specified sending sourceport number by WebUI.
  - Click **Monitor > Log Configuration > Sending Sourceport Configuration** to check the specified sending sourceport number.
- The binary logs sent to the Syslog Server is not influenced by the sending sourceport configuration. The binary logs are sent by UDP protocol using 5566 sourceport.
- When SNAT is enabled, the system will randomly select port as the sending sourceport according to the port resources of network addresses translated by NAT.

Specifying a Facility

The Facility field is used to identify the device generating the log information. When the log information is sent to the log server, the Facility field will be displayed in the log server. The system supports global configuration of the Facility field for log information, and also supports

separately specifying the Facility field for event logs and traffic logs. In addition, the separately specified Facility field takes precedence over the globally configured Facility field. If not configured, the Facility field defaults to "local7".

Globally Configuring the Facility Field of Log Messages

The system supports to globally configure the Facility field of log messages. This configuration can take effect for all types of logs. To globally configure the Facility field of log messages, in global configuration mode, use the following command:

logging facility local*x*

• **local***x* – Specifies the Facility field of log information. The value range of x is an integer from 0 to 7. The default value is 7.

To restore to the default value, in the global configuration mode, use the command **no logging facility**.

Separately Specifying the Facility Field of Event Logs and Traffic Logs

To separately specify the Facility field of event logs and traffic logs, in global configuration mode, use the following command:

logging {**event** | **traffic**} **facility local***x*

• **local***x* – Specifies the Facility field of event logs and traffic logs. The value range of x is an integer from 0 to 7.

To delete the specified Facility field, in global configuration mode, use the command **no logging** {**event** | **traffic**} **facility**.

Viewing the Facility Field of Event Logs and Traffic Logs

To view the Facility field of log messages, in any mode, use the following command:

show logging facility

The following result is returned:

```
hostname#show logging facility
Event：local0
Traffic：local2
```

Displaying Hostname/Username in the Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. By default the hostname and username are not displayed in the traffic logs. To display the hostname or username in the traffic logs, in the global configuration mode, use the following command:

- Display the hostname of the session logs, NAT logs, and web surfing logs: **logging content hostname**
- Display the username of the session logs: **logging session content username**

After executing the above commands, the hostname and username will be displayed in the traffic logs.



Notes: The NetBIOS name resolution function is the prerequisite of displaying hostname in the traffic logs. For detailed configuration procedure, see Configuring NetBIOS Name Resolution.

To cancel the displaying of hostname/username, in the global configuration mode, use the following commands:

- **no logging {session | nat | urlfilter} content hostname**
- **no logging session content username**

Displaying Username in the Threat Logs

By default the username are not displayed in the threat logs. To display the username in the threat logs, in the global configuration mode, use the following command:

logging threat content username

To cancel the displaying of username, in the global configuration mode, use the following commands:

no logging threat content username

Sending Logs to an Email Account

Logs can be sent to the specified Email address. You need to configure the Email address to receive log messages and the SMTP server instance.

Configuring an Email Address

To configure the Email address to receive the log messages, in the global configuration mode, use the following command:

logging email to *email-address* **smtp** *smtp-instance*

- *email-address* – Specifies the email address that is used to receive the log messages.
- **smtp** *smtp-instance* – Specifies the name of the SMTP server instance used to send the mail (must be a valid SMTP server instance in the system).

To delete the configuration of email address, in the global configuration mode, use the following command:

no logging email to *email-address*

Configuring a SMTP Server Instance

To configure a SMTP server instance, in global configuration mode, use the following command:

smtp name *smtp-name* **server** {*ip-address* | *hostname*} {**from***email-addr* | **vrouter***vr-name***from***email-addr* }[**username***user-name***password***password*] [**mode** { **plain** | **starttls** | **ssl**}] [**port***server-port*]

- *smtp-name* – Specifies the name of the SMTP server instance.
- *ip-address* | *hostname* – Specifies the IP address or hostname of the SMTP server.
- *email-addr* – Specifies the sender's address.
- **vrouter***vr-name* – Specifies the VRouter of the SMTP server.

- **username***user-name***password***password* – Specifies the username and password of the sender account.
- **mode** { **plain** | **starttls** | **ssl**}- Specifies the transmission mode of the email.
  - **plain**- Specifies that the mail is sent in plain text and is not encrypted. This mode is the default transmission mode.
  - **starttls**- STARTTLS is an extension to the plain text communication protocol that upgrades plain text connections to encrypted connections. Specified in this mode, the mail will be transmitted using encrypted mode.
  - **ssl** - SSL protocol is a security protocol that provides security and data integrity for network communication. Specified in this mode, the mail will be transmitted using encrypted mode.
- **port***server-port* - Specifies the port number of the SMTP server. The range is 1 to 65535. The default port number is different for different transmission modes, PLAIN: 25, STARTTLS: 25, SSL: 465.

To delete the specified SMTP server instance, in the global configuration mode, use the command **no smtp name***smtp-name*.

Configuring PBR Log Function

After you enable PBR log, the system will generate PBR logs once PBR policy rule is matched by traffic.

Enabling PBR Log Function

You can enable PBR log function basing on PBR policy rules. By default, this feature is disabled. To enable or disable PBR log function, in the PBR policy rule configuration mode, use the following command:

- To enable: **log enable**
- To disbale: **no log enable**

To display the PBR logs in output destination, in the global configuration mode, use the following command:

logging traffic pbr on

In the global configuration mode, use the **no logging traffic pbr on**command

to cancel the settings.



Tip: If you have configured prioritized destination routing (DBR) lookup,even if PBR policy rule is matched by traffic, the system will not generate PBR logs.

Sending PBR Logs

You can send PBR traffic logs to the console, syslog server and memory buffer. You can select the output destination according to your requirements.

To send PBR traffic logs to the console, syslog server or memory buffer, in the global configuration mode, use the following command:

logging traffic pbr to {**console** | **syslog** | **buffer** [**size** *buffer-size*]}

- **console** | **syslog** | **buffer** – Specify the output destination. You can output the logs to the console, syslog server or buffer.
- **size** *buffer-size* - Specify the buffer size. The value range is 4096 to 2097152 bytes. The default value is 1048576.

In the global configuration mode, use the **no logging traffic pbr to** {**console** | **syslog** | **buffer**}command to disable the corresponding output function.



Tip: Currently, the system does not output:

- PBR logs of binary format.
- PBR logs for IPv6.

Displaying Hostname/Username in PBR Logs

By default, the hostname and username are not displayed in the PBR traffic logs. To display the hostname or username in PBR logs, in the global configuration mode, use the following command:

logging pbr content {**hostname** | **username**}

In the global configuration mode, use the **no logging pbr content** {**hostname** | **username**} command to cancel the display of hostname/username.

Viewing PBR Logs

To view all the PBR logs, in any mode, use the following commands:

show logging traffic pbr

Configuring Log Parameter

The system supports to modify parameter of the event log, network log, and configuration log, including the description, level of the log, and enabling/disabling the log generation.



Notes:

- You cannot configure log parameters for devices that support to store event logs, network logs, and configuration logs into the local database.
- Non-root VSYS does not support to configure log parameters.

Disabling the Log Generation

To disabling the generation of the specified log ID, in the global configuration mode, use the following command:

logging logid[**hex**] *log-id***off** [**description***description*]

- **hex** - Specify that the format of the log ID is hexadecimal. If not specified, the format of the log ID is decimal.
- *log-id*- Disabling the generation of specified log ID. Note: When you specify a hexadecimal log ID, you do not need to enter the hexadecimal prefix 0x.
- **description***description* - Edit the description of the specified log ID.

In the global configuration mode, use the **no logging logid**[**hex**] *log-id***off** command to enabe the generation of the specified log ID.

Configuring Log Level

To configure the log level, in the global configuration mode, use the following command:

logging logid[**hex**] *logid***severity***severity-level* [**description***description*]

- **hex** - Specify that the format of the log ID is hexadecimal. If not specified, the format of the log ID is decimal.
- *logid* - Specify the log ID. Note: When you specify a hexadecimal log ID, you do not need to enter the hexadecimal prefix 0x.
- **severity***severity-level* - Specified the log level, including EMERG, ALERT, ALERT, ERR, WARNING, NOTICE, INFO.
- **description***description* - Edit the description of the specified log ID.

In the global configuration mode, use the **no logging logid**[**hex**] *logid***severity** command to cancel the modification of log level.

Enabling/Disabling the Record User Information Function for Threat Log

You can enable or disable the Record User Information function for Threat Log. With this function enabled, threat logs will record information about the authenticated user, including AAA server, username, and hostname. By default, this function is disabled. To enable the Record User Information function for Threat Log, in the global configuration mode, use the following command:

logging threat content username

In the global configuration mode, use the **no logging threat content username** command to disable the Record User Information function for Threat Log.

Viewing Log Entries for Configuring Log Parameters

To view the log entries for configuring log parameters, in global configuration mode, use the following commands:

show logging logid config

Viewing Log Configurations

To view the log configurations, in any mode, use the following commands:

- Show the system log configuration:**show logging**
- Show the syslog server configuration: **show logging syslog-server**
- Show the email address configuration:**show logging email**
- Show the log statistics:**show logging statistics**
- Show the SMTP server configuration: **show smtp**
- Show if the hostname and username are displayed : **show logging content**
- Show if the hostname and username are displayed in the logs: **show logging content**
- Show the SMS configuration: **show logging sms**

Viewing Logs

To view the specified type of logs, in any mode, use the following commands:

- Show the event logs:

  show logging event [**severity** *severity-level*]

- Show the debug, network or threat logs:

  show logging {**debug** [**slot** *slot-number*] [**cpu** *cpu-number*] | **network** | **threat** }

- Show the configuration logs:

  show logging configuration

- Show the operation logs:

  show logging [**operation**]

- Show the data security logs (file filter logs, content filter logs, network behavior record logs):

  show logging data-security [**dlp** | **cf** | **nbr**]

- Show all the traffic logs:

  show logging traffic

- Show the traffic logs (session log part):

  show logging traffic *session* **filter-session** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **policy-id policy-id** | **action** {**policy-deny** | **session-start** | **session-end** | **policy-default**}]

- Show the traffic logs (NAT log part):

  show logging traffic *nat* **filter-nat** [**src-ip** *A.B.C.D* | **src-port** *port-num* | **dst-ip** *A.B.C.D* | **dst-port** *port-num* | **protocol** {**icmp** | **tcp** | **udp** | **others**} | **trans-src-ip** *A.B.C.D* | **trans-src-port** *port-num* | **trans-dst-ip** *A.B.C.D* | **trans-dst-port** *port-num* | **snat-rule-id** *rule-id* | **dnat-rule-id** *rule-id*]

- Show the traffic logs (URL log part):

  show logging traffic urlfilter

- Shows the IoT logs:

  show logging iot-monitor

Exporting Logs

You can export the debug logs, event logs and threat logs to the specified FTP/FTPS/SFTP server, TFTP server or USB disk.

To export the debug logs, event logs or threat logs to the specified FTP/FTPS/SFTP server, in the execution mode, use the following command:

export log {**debug** | **event** | **threat** } **to** {**ftp** | **ftps** | **sftp**} **server** *ip-address* **vrouter** *vrouter-name* **user***user-name* **password** *password* [*file-name*]

- **debug** | **event** | **threat** - Specifies the log type that will be exported.
- *ip-address* - Specifies the IP address of the FTP/FTPS/SFTP server.
- *vrouter-name* - Specifies the virtual router name.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *file-name* - Specifies the name of the file to which the logs will be exported.

To export the debug logs, event logs or threat logs to the specified TFTP server, in the execution mode, use the following command:

export log {**debug** | {**event** | **threat** } **to tftp server** *ip-address* [*file-name*]

To export the debug logs, event logs or threat logs to the specified USB disk, in the execution mode, use the following command:

export log {**debug** | **event** | **threat** } **to** {**usb0** | **usb1**} [*file-name*]

Clearing Logs

To clear the specified logs in the system, in the execution mode, use the following command:

clear logging { configuration | operation | debug | event | network | threat | traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr] | iot-monitor}

- **configuration** -Clears all the configuration logs information in the system.
- **operation** -Clears all the operation logs information in the system.
- **debug** – Clears all the debug logs information in the system.
- **event** – Clears all the event logs information in the system.
- **network** – Clears all the network logs information in the system.
- **threat** – Clears all the threat logs information in the system.
- **traffic {session | nat | urlfilter}** – Clears the specified traffic logs information in the system.
- **data-security [dlp | cf | nbr]** – Clears all the data security logs information in the system. File filter logs (**dlp**), Content filter logs (**cf**), Network behavior record logs (**nbr**) .
- **iot-monitor** – Clears all the IoT logs in system.



Notes: This command cannot clear the following important event log information:

- Restart: system restart, module restart.
- Hardware exception: fan, power, etc.
- Configurations for deleting or rolling back.
- Swithing between master device and backup device.
- SCM HA.

Sending Traffic Logs to Syslog Servers

When there are lots of log messages generated by Hillstone devices, a single Syslog server may fail to deal with all the messages. To address this problem, Hillstone devices support the distributed

sending function. With this function configured, Hillstone devices can send the log messages to multiple Syslog servers according to a certain algorithm to reduce the pressure to a single Syslog server.

Only the traffic and data security log messages can be sent in the distributed way. And only the threat logs can be sent in plaintext and in the distributed way.

To configure the distributed sending function, in the global configuration mode, use the following command:

logging {**traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**]} **to syslog** [**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]

- **traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**] – Specifies the log type that will be sent.
- **syslog** – Sends the logs to Syslog servers.
- **binary-format** – Sends the traffic logs in the binary format.
- **distributed** – Sends the traffic logs to multiple Syslog servers according to the algorithm specified.
- **src-ip-hash** | **round-robin** – Specifies the algorithm used to choose Syslog servers. **src-ip-hash**, choose the Syslog server according to the source IP address; **round-robin**, choose the Syslog server by the round-robin algorithm, and this is the default algorithm used by the system.
- **custom-format** – Sends logs in the plaintext format. By default, the system will send the traffic logs in the plaintext format.

To remove the traffic log sending configuration, in the global configuration mode, use the following command:

no logging {**traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**]} **to syslog**

To send the threat logs in the plaintext format and in the distributed way, use the following command in the global configuration mode:

logging threat to syslog [**custom-format** [**distributed** [**src-ip-hash** | **round-robin**]]]

- **custom-format** – Sends the logs in the plaintext format. By default, the system sends the logs in the plaintext format.
- **syslog** – Sends the logs to the syslog server.
- **distributed** – Sends the logs to the syslog server in the distributed way.
- **src-ip-hash** | **round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.

In the global configuration mode, use the following command to cancel the output of the threat logs:

no logging threat to syslog

Example of Configuring Logs

This section describes two typical CLI log configuration examples: sending event logs to the console and sending event logs to the Syslog server.

Example 1: Sending Event Logs to the Console

Step 1: Enable the event log function:

```
hostname# configure
hostname(config)# logging event on
```

Step 2: Send the event logs to the console; set the severity to Debugging:

```
hostname(config)# logging event to console severity debugging
```

Example 2: Sending Event Logs to the Syslog Server

Step 1: Enable the event log function. The workstation with IP address of 202.38.1.10 is used as the Syslog Server of UDP type; set the severity to Informational:

```
hostname(config)# logging event on
```

```
hostname(config)# logging syslog 202.38.1.10 udp 514 type event
hostname(config)# logging event to syslog severity informational
```

Step 2: Power on the Syslog Server.

Example 3: Sending Traffic Logs to a Local File

Step 1:Configure a track object. Track the syslog server whose IP address is 202.38.1.10.

```
hostname(config)# track abc
hostname(config-trackip)# threshold 3
hostname(config-trackip)# ip 202.38.1.10 interface ethernet0/1 interval 2
```

Step 2: Enable the function of sending traffic logs to the syslog server. The IP address of the syslog server is 202.38.1.10. The name of the VRouter is trust-vr, the type is UDP, the port number is 514, and the log type is traffic (NAT logs).

```
hostname(config)# logging traffic nat on
hostname(config)# logging syslog 202.38.1.10 vrouter "trust-vr" udp 514 type traffic nat
hostname(config)# logging traffic nat to syslog
```

Step 3: Power on the syslog server.

Step 4: Configure the settings to send the traffic logs to a local file. The folder name is aa.

```
hostname(config)# logging traffic nat to file name usb0 aa
```

Step 5: Enable the track function for the syslog server and set the maximum rate of sending traffic logs to a file as 600 entries per second.

```
hostname(config)# logging traffic nat to syslog track abc local-backup rate-limit 600
```

Diagnostic Tool

Introduction

System supports the following diagnostic methods:

- Packet Capture Tool: Users can capture packets in the system by Packets Capture Tools. After capturing the packets, you can export them to your local disk and then analyze them by third-party tools.
- Packet Path Detection: Based on the packet process flow, the packet path detection function detects the packets and shows the detection processes and results to users by chart and description. This function can detect the following packet sources: emulation packet, online packet, and imported packet (system provides the Packet Capture Tool for you that can help you capture the packets).

The detectable packets from different packet sources have different detection measures. The system supports the following measures:

- Emulation packet detection: Emulate a packet and detects the process flow in the system of this packet.
- Online packet detection: Perform a real-time detection of the process flow of the packets in the system.
- Imported packet detection: Import the existing packets and detects the process flow in the system of the packets.

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Using WebUI to configure the diagnostic tool is strongly recommended.

Commands

Packet Capture Commands

Configuring Packet Capture Task

Including configuration capture tasks, capture rules, start/stop capture, export capture files, clear capture files.

packet-capture task

Create an online packet capture task and enter the packet capture task configuration mode. Use the no form of the command to delete the specified online packet capture task.

Command:

packet-capture task*task-name*

no packet-capture task*task-name*

Description:

task-name - Specifies the name of the online packet capture task and enter the packet capture task configuration mode.

Default values:

None

Mode:

Global configuration mode

Guidance:

At most 5 packets capture tasks can be configured within each VSYS.

Example:

hostname(config)# **packet-capture task task1**

include-self-traffic

Enable the Contain Self-traffic function so that captured packets contain traffic sent and received by the device itself. Use the no form of the command to disable this function.

Command:

include-self-traffic

no include-self-traffic

Description:

None

Default values:

Enable

Mode:

Packet capture task configuration mode

Guidance:

None

Example:

hostname(config-pkt-task)# **include-self-traffic**

interface

Configure the interface used for the online packet capture task. Use the no form of the command to delete the specified interface.

Command:

interface*interface-name*

no interface

Description:

interface-name - Specifies the name of the interface used for the online packet capture task, which cannot capture packets based on the tunnel interface and management interface.

Default values:

None

Mode:

Packet capture task configuration mode

Guidance:

None

Example:

hostname(config-pkt-task)# **interface ethernet0/0**

direction

Configure the traffic direction of the interface. Use the no form of the command to delete the specified traffic direction.

Command:

direction {**in** | **out**}

no direction

Description:

in - Specifies to capture packets from the inbound interface. If fails, the packets may be blocked by the firewall or not flow into the firewall. If no packets flow into the firewall, you can troubleshoot the upstream link or upstream device as needed.

out - Specifies to capture packets from the outbound interface. If succeeds, you can troubleshoot the downstream link or downstream device as needed.

If **direction** is not configured, both inbound and outbound are specified. In this case, you can determine the actual traffic direction based on captured packets.

Default value:

None

Mode:

Packet capture task configuration mode

Guidance:

None

Example:

hostname(config-pkt-task)# **direction in**

task-info

Configure the packet capture task.

Command:

task-info [**pacp-num***number-value*] [**pacp-time***time-value*] [**description***description*]

no task-info

Description:

pacp-num*number-value* - Specifies the total number of packets that can be captured for the packet capture task. The value ranges from 1 to 4294967295. During the effective period (pacp-time) of the packet capture task, if the number of packets captured reaches the configured number, the system automatically stops capturing packets.

pacp-time*time-value* - Specifies the effective duration of the capture task, the range is 1 to 720 minutes.

description*description* - Specifies the description information of the packet capture task. The range is 1 to 255 characters.

Default values:

None

Mode:

Packet capture task configuration mode

Guidance:

None.

Example:

hostname(config-pkt-task)# **packet-capture pacp-time 20**

filter-rule

Configure the packet capture rule.

Command:

filter-rule id *id* [**src-ip***ipv4-address/mask* | **src-ipv6***ipv6-address/prefix* | **src-ip-min***min-ipv4***src-ip-max***max-ipv4* | **src-ipv6-min***min-ipv6***src-ipv6-max***max-ipv6* | **user***aaa-server user-name* | **user-group***aaa-server user-name*] [**src-port***port-num*] [**dst-ip***ipv4-address/mask* | **dst-ipv6***ipv6-address/prefix* | **dst-ip-min***min-ipv4***dst-ip-max***max-ipv4* | **dst-ipv6-min***min-ipv6***dst-ipv6-max***max-ipv6* | **url***url*] [**dst-port***port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application***app-name*]

no filter-rule id*id*

Description:

filter-rule id *id* -Specifies the ID of packet capture rule. The range is 1-8.

src-ip*ipv4-address/mask* - Specifies the source IPv4 address and its mask of the packet.

src-ipv6*ipv6-address/prefix* - Specifies the source IPv6 address and its range of the packet.

src-ip-min*min-ipv4***src-ip-max***max-ipv4* - Specifies the source IPv4 range of the packet.

src-ipv6-min*min-ipv6***src-ipv6-max***max-ipv6*- Specifies the source IPv6 range of the packet.

user*aaa-serveruser-name* - Specifies the user of the packet.

user-group*aaa-serveruser-name* - Specifies the user group of the packet.

src-port *port-num* -Specifies the source port number of the packet.

dst-ip*ipv4-address/mask* - Specifies the destination IPv4 address and its mask of the packet.

dst-ipv6*ipv6-address/prefix* - Specifies the destination IPv6 address and its range of the packet.

dst-ip-min*min-ipv4***dst-ip-max***max-ipv4* - Specifies the destination IPv4 range of the packet.

dst-ipv6-min*min-ipv6***dst-ipv6-max***max-ipv6*- Specifies the destination IPv6 range of the packet.

url*url*- Specifies the destination URL of the packet.

dst-port*port-num* -Specifies the destination port number of the packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the packet.

application*app-name* -Specifies the application type of the packet.

Default values:

any.

Mode:

Packet capture task configuration mode

Guidance:

A maximum of 8 packet capture rules can be created in the same packet capture task.

Example:

hostname(config-pkt-task)# **filter-rule id 1 src-ip 1.1.1.1 src-port 23 dst-ip 2.2.2.2 dst-port 23 application http**

exec packet-capture

Begin or stop capturing packets.

Command:

Begin capturing packets: **exec packet-capture task***task-name***start**

Stop capturing packets: **exec packet-capture stop**

Description:

task*task-name*- Specifies the name of the packets capture task.

Default values:

None

Mode:

Any mode

Guidance:

None

Example:

hostname# **exec packet-capture task task1 start**

hostname# **exec packet-capture stop**

export packet-capture-file

Export the file which is captured by Packet Capture Tool.

Command:

export packet-capture-file {**slot***slot-number* | **all** } {**tar***task-name* | **file***task-name file-name*} **to** {**ftp server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} [**vrouter***vr-name*] [*file-name*]

Description:

slot*slot-number* | **all** - Export the data package file of the specified slot number to the FTP server-/TFTP server. Support for some devices (X series devices and K9180).

tar*task-name* | **file***task-name file-name*- Export all file compressed packages of the packet capture task or a specified file.

ftp server*ip-address* [**user***user-name***password** *password*] -Export the specified file to FTP server.

- *ip-address* - Specifies the FTP IP address.
- **user** *user-name***password***password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server*ip-address* -Export the specified file to TFTP server.

vrouter*vr-name* -Specifies the VR name.

file-name -Specifies the file name you exported.

Default values:

vrouter*vr-name* - trust-vr;

file-name – pktdump.pcap

Mode:

Global configuration mode

Guidance:

Only devices with hard disks support this CLI. For other devices without hard disks, please export the data package file via WebUI.

We recommend that the packet you capture at a time does not exceed 500 MB because a larger packet may fail to be exported caused by timeout.

Example:

hostname# **export packet-capture-file tar test to tftp server 10.1.1.1**

clear packet-capture task

Clear the packet capture file of the specified capture task

Command:

clear packet-capture task*task-name*

Description:

task-name- Specifies the name of the packet capture task that needs to clear the packet capture file.

Default values:

None.

Mode:

Any mode.

Guidance:

None.

Example:

hostname# **clear packet-capture task task1**

Packet Capture Global Configuration

The global configuration items of packet capture vary according to the type of device:

- For devices with hard disks, you can configure the percentage of the packet capture files to the total hard disk size only in the root VSYS.
- For devices without hard disks, in the root VSYS, you can configure the packet capture file save percent, the packet capture file save time, and the maximum memory usage; in the non-

root VSYS, you can configure only the packet capture file save time. For SG-6000 X series devices and SG-6000-K9180 devices, the global configuration items of packet capture are processed as no hard disks, regardless of whether the device has hard disks.

packet-capture save-mem

Configure the maximum percentage of packet capture files in remaining memory (devices without hard disk) or total size of hard disk (devices with hard disk).

Command:

packet-capture save-mem*mem-percent*

no packet-capture save-mem

Description:

mem-percent -Specifies the maximum percentage of packet capture files in remaining memory (devices without hard disk) or total size of hard disk (devices with hard disk), the range is 5%-50%.

Default values:

10%

Mode:

Global configuration mode

Guidance:

None

Example:

hostname(config)# **packet-capture save-mem 20**

packet-capture save-time

Configure the length of time the packet capture file is saved.

Command:

packet-capture save-time*save-time-value*

no packet-capture save-time

Description:

save-time-value -Specifies the length of time the packet capture file is saved, the unit is minutes, the range is 1-1440 minutes.

Default values:

None

Mode:

Global configuration mode

Guidance:

This command is supported only on no hard disk devices.

Example:

hostname(config)# **packet-capture save-time 60**

packet-capture dp-mem-max

Configure the maximum percentage of memory that the packet capture file can use. Use the no form of the command to restore the default value.

［Command］

packet-capture dp-mem-max*dp-mem-max-percent*

no packet-capture dp-mem-max

［Description］

dp-mem-max-percent - Specifies the maximum percentage of memory that the packet capture file can use. Valid values: 50% to 90%. When the percentage of memory usage exceeds the upper limit, the system automatically stops capturing packets.

［Default value］

60%。

［Mode］

Global configuration mode

［Guidance］

This command is supported only on no hard disk devices.

[Example:]

hostname(config)# **packet-capture dp-mem-max 80**

Show Commands

show packet-capture status

Display the status of packet capture.

Command:

show packet-capture status [**task***task-name* [**cpu***cpu-number* | **slot***slot-number*]]

Description:

task*task-name* -Display the status information of the packet capture task with the specified name.

cpu*cpu-number* | **slot***slot-number* - Display the packet capture status information of the specified CPU or slot number. Only some devices (X series devices, K9180) are supported.

Default values:

None.

Mode:

Any mode

Guidance:

Only X series devices and K9180 device support the display of the capture status information of the specified CPU or slot number.

Example:

hostname(config)# **show packet-capture status task test**

show packet-capture task

Display packet capture task information

Command:

show packet-capture task

Description:

None.

Default values:

None.

Mode:

Any mode

Guidance:

None.

Example:

hostname(config)# **show packet-capture task**

Packet Path Detection Commands

Emulation Packet

troubleshooting packet-trace emulation-template

Configure emulation detection.

Command:

troubleshooting packet-trace emulation-template *name* **type** {**tcp** | **udp**} **src-ip** *ip-address* **src-port** *port-num* **dst-ip** *ip-address* **dst-port** *port-num* **ingress-interface** *interface-name* [**description** *description*]

troubleshooting packet-trace emulation-template *name* **type icmp src-ip** *ip-address* **dst-ip** *ip-address* **type** *type-value* **code** *code-value* **ingress-interface** *interface-name* [**description** *description*]

no troubleshooting packet-trace emulation-template *name*

Description:

emulation-template *name* -Specifies the name of the emulation packet.

type {**tcp** | **udp**} /**type icmp** -Specifies the protocol type of the emulation packet.

src-ip *ip-address* -Specifies the source IP address of the emulation packet.

dst-ip *ip-address*- Specifies the source port of the emulation packet, only when the protocol type is specified as TCP/UDP.

src-port *port-num* -Specifies the destination port of the emulation packet, only when the protocol type is specified as TCP/UDP.

dst-port *port-num* -Specifies the destination IP address of the emulation packet.

type *type-value* **code** *code-value* -Specifies the ICMP type value and code value only when the protocol type is specified as ICMP.

ingress-interface *interface-name* -Specifies the ingress interface of the emulation packet.

description *description* -Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 20 emulation packets.

This command is only supported in T series devices and E series devices.

Example:

hostname(config)# **troubleshooting packet-trace emulation-template temp1 type udp src-ip 10.0.0.1 src-port 10 dst-ip 192.168.0.1 dst-port 100 ingress-interface ethernet0/0**

exec troubleshooting packet-trace emulation-template

Begin emulation packet path detection.

Command:

exec troubleshooting packet-trace emulation-template *name* **start**

Description:

emulation-template *name*- Specifies the name of the emulation packet.

Default values:

None

Mode:

Any mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# **exec troubleshooting packet-trace emulation-template test start**

exec troubleshooting packet-trace stop

Stop emulation packet path detection.

Mode:

Any mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# exec troubleshooting packet-trace stop

export troubleshooting packet-trace emulation-template

Export the file captured by emulation packet path detection.

Command:

export troubleshooting packet-trace emulation-template *name* **to** {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Export the specified file to FTP server.

- *ip-address* -Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -指Export the specified file to TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name -Specifies the file name you exported.

Default values:

vrouter *vr-name* - trust-vr。

Mode:

Executive mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# export troubleshooting packet-trace emulation-template temp1 to tftp server 10.1.1.1

Online Packet

troubleshooting packet-trace filter

Configure online detection.

Command:

troubleshooting packet-trace filter *name* **type live-traffic** {[[**src-ip** *ip-address*] | [**user** *aaa-server user-name*] | [**user-group** *aaa-server user-name*]] [**src-port** *port-num*] [[**dst-ip** *ip-address*] | [**url** *url*]] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*] [**ingress-interface** *interface-name*]} [**description** *description*]

no troubleshooting packet-trace filter *name*

Description:

filter *name* -Specifies the name of the online packet.

src-ip *ip-address* -Specifies the source IP address of the online packet.

user *aaa-server user-name* -Specifies the user of the online packet.

user-group *aaa-server user-name* -Specifies user group of the online packet.

src-port *port-num* -Specifies the source port of the online packet.

dst-ip *ip-address* -Specifies the destination IP address of the online packet.

url *url* -Specifies the URL of the online packet.

dst-port *port-num* -Specifies the destination port of the online packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the packet.

application *app-name* -Specifies the application type of the online packet.

ingress-interface *interface-name* -Specifies the ingress interface of the online packet.

description *description*- Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 5 packets capture entries.

This command is only supported in T series devices and E series devices.

Example:

hostname(config)# **troubleshooting packet-trace filter test type live-traffic dst-ip 10.1.1.1 application http ingress-interface ethernet0/0**

exec troubleshooting packet-trace filter

Begin online packet path detection.

Command:

Begin online packet path detection: **exec troubleshooting packet-trace filter** *name* [**packet-capture**] **start** [**time-out** *value*]

Description:

filter *name* -Specifies the name of the online packet.

packet-capture -Enable the packet path detection function.

time-out *value* -Specifies the detection time. When reaching the time value, system will stop detection automatically. Range is from 1 to 1440 minutes.

Default values:

time-out *value* - 30 minutes

Mode:

Any mode

Guidance:

The imported packet detection function is only supported in T series devices and E series devices with hard disks.

Example:

hostname# **exec troubleshooting packet-trace filter 123 start time-out 60**

exec troubleshooting packet-trace stop

Stop packet path detection.

Mode:

Any mode

Guidance:

The imported packet detection function is only supported in T series devices and E series devices with hard disks.

Example:

hostname# exec troubleshooting packet-trace stop

export troubleshooting packet-trace packet-capture-file

Export the file captured by online packet path detection.

Command:

export troubleshooting packet-trace packet-capture-file to {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] [*file-name*]

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Export the specified file to FTP server.

- *ip-address* - Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -Export the specified file to TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name- Specifies the file name you exported.

Default values:

vrouter *vr-name* - trust-vr;

file-name – ts_pktdump.pcap。

Mode:

Executive mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# **export troubleshooting packet-trace packet-capture-file to tftp server 10.1.1.1**

Imported Packet

import troubleshooting packet-trace

Import a file for packet path detection.

Command:

import troubleshooting packet-trace replay-file from {**ftp server** *ip-address* [**user** *user-name* **password** *password*] | **tftp server** *ip-address*} [**vrouter** *vr-name*] *file-name*

Description:

ftp server *ip-address* [**user** *user-name* **password** *password*] -Import the specified file from FTP server.

- *ip-address* - Specifies the FTP IP address.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP user. If not specified, system will use anonymous to login.

tftp server *ip-address* -Import the specified file from TFTP server.

vrouter *vr-name* -Specifies the VR name.

file-name -Specifies the file name you imported.

Default values:

vrouter *vr-name* - trust-vr。

Mode:

Executive mode

Guidance:

This command is only supported in T series devices and E series devices with hard disks.

Example:

hostname# **import troubleshooting packet-trace replay-file from ftp server 10.1.1.1 user user1 password password1 test.pcap**

troubleshooting packet-trace filter

Configure imported detection.

Command:

troubleshooting packet-trace filter *name* **type replay-file** {[**src-ip** *ip-address*] [**src-port** *port-num*] [**dst-ip** *ip-address*] [**dst-port** *port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application** *app-name*] **ingress-interface** *interface-name*} [**description** *description*]

no troubleshooting packet-trace filter *name*

Description:

filter *name* -Specifies the name of the imported packet.

src-ip *ip-address* -Specifies the source IP address of the imported packet.

src-port *port-num* -Specifies the source port of the imported packet.

dst-ip *ip-address* -Specifies the destination port of the imported packet.

dst-port *port-num* -Specifies the destination IP address of the imported packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the imported packet.

application *app-name* - Specifies the application type of the imported packet.

ingress-interface *interface-name* -Specifies the ingress interface of the imported packet.

description *description* - Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 5 packets capture entries.

This command is only supported in T series devices and E series devices with hard disks.

Example:

hostname(config)# **troubleshooting packet-trace filter test1 type replay-file src-ip 10.0.0.1 ingress-interface ethernet0/0**

exec troubleshooting packet-trace filter

Begin imported packet path detection.

Command:

Begin imported packet path detection: **exec troubleshooting packet-trace filter** *name* **start**

Description:

filter *name* - Specifies the name of the imported packet.

Default values:

None

Mode:

Any mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# **exec troubleshooting packet-trace filter test1 start**

exec troubleshooting packet-trace stop

Stop imported packet path detection.

Mode:

Any mode

Guidance:

This command is only supported in T series devices and E series devices.

Example:

hostname# exec troubleshooting packet-trace stop

NetFlow

Overview

NetFlow is a data exchange method, which records the source /destination address and port numbers of data packets in the network. It is an important method for network traffic statistics and analysis.

Hillstone NetFlow supports the NetFlow Version 9. With this function configured, the device can collect user's ingress traffic according to the NetFlow profile, and send it to the server with NetFlow data analysis tool, so as to detect, monitor and charge traffic.

Configuring NetFlow

The NetFlow configurations are based on interfaces.

To configure the interface-based NetFlow, take the following steps:

1. Enable NetFlow function.
2. Create a NetFlow profile, and then specify the active timeout value, template refresh rate and configure the NetFlow server in the profile.
3. Bind the NetFlow Profile to an interface.

Enabling NetFlow

To enable the NetFlow function, in the global configuration mode, use the following command:

netflow enable

To disable the NetFlow function, in the global configuration mode, use the following command: **no netflow enable**.

Creating a NetFlow Profile

NetFlow profile configurations contains the active timeout value, the template refresh rate, and the NetFlow server settings.

To create a NetFlow profile, in the global configuration mode, use the following command:

netflow-profile *netflow-profile-name*

- *netflow-profile-name* - Specifies the NetFlow profile name and enters the NetFlow profile configuration mode. If the specified name exists, system will directly enter the NetFlow profile configuration mode.

To delete the specified NetFlow profile, in the global configuration mode, use the command **no netflow-profile** *netflow-profile-name*.

Configuring the Template Refresh Rate

You can configure the NetFlow template refresh rate by time or number of packets, after which system will refreshes the NetFlow template. In the NetFlow profile configuration mode, use the following command:

- **Time**: **template-refresh-minute** *refresh-value*

  refresh-value -Specifies the time after which system refreshes the NetFlow template. The range is 1 to 3600 minutes. The default value is 30 minutes.

- **Packets**: **template-refresh-packet** *packet-value*

  packet-value - Specifies the number of packets. When the number of NetFlow packets exceeds the specified value, system will refreshes the NetFlow template. The range is 1 to 600. The default value is 20.

Configuring the Active Timeout Value

The active timeout value is the time after which the device will send the collected NetFlow traffic information to the specified server once. In the NetFlow profile configuration mode, use the following command:

active-timeout *timeout-value*

- *timeout-value* – Specifies the active timeout value. The range is 1 to 60 minutes. The default value is 5 minutes.

To restore to the default value, in the NetFlow profile configuration mode, use the following command: **no active-timeout**.

Configuring the NetFlow Server

To configure the NetFlow server for data analysis, in the NetFlow profile configuration mode, use the following command:

server*name* [**ip***ip-address* | **ipv6***ipv6-address* | **port***port-number*]

- *name* – Specifies the server name, the range is 1 to 32 characters.
- **ip** *ip-address* – Specifies the IPv4 address of NetFlow server.
- **ipv6***ipv6-address* – Specifies the IPv6 address of NetFlow server.
- **port** *port-number* – Specifies the port number of NetFlow server. The range is 1 to 65535. The default value is 9996.

To delete the specified server, in the NetFlow profile configuration mode, use the following command: **no server** *name*.



Notes: You can add up to 2 NetFlow servers.

Containing the Enterprise Field

You can specify whether the collected NetFlow traffic information contains the enterprise field.

To specify that the collected NetFlow traffic contains enterprise field, in the NetFlow profile configuration mode, use the following command:

export-enterprise-fields

To specify that the collected NetFlow traffic does not contains enterprise field, in the NetFlow profile configuration mode, use the following command: **no export-enterprise-fields**.

Specifying the Source Interface

To specify the source interface for sending NetFlow traffic information, in the NetFlow profile configuration mode, use the following command:

source interface*interface-name* {**address***interface-address* | **address-ipv6***interface-address-ipv6*}

- *interface-name* – Specifies the source interface name.
- **address***interface-address* – After specifying the source interface, the system will automatically acquire and display the management IPv4 address or the secondary IPv4 address of the source interface.
- **address-ipv6***interface-address-ipv6* – After specifying the source interface, the system will automatically acquire and display the IPv6 address of the source interface.

To delete the source interface configurations, in the NetFlow profile configuration mode, use the following command: **no source**.

Binding a NetFlow Profile to an Interface

If the NetFlow profile is bound to an interface, the device will collect user's ingress traffic information according to the NetFlow profile. To bind a NetFlow profile to an interface, in the interface configuration mode, use the following command:

netflow-profile *netflow-profile-name*

- *netflow-profile-name* – Specifies the name of the NetFlow profile that will be bound to the interface.

To remove the binding, in the interface configuration mode, use the following command: **no netflow-profile**

Viewing NetFlow Information

To view the configurations of NetFlow profile, in any mode, use the following command:

show netflow-profile [*netflow-profile-name*]

- *netflow-profile-name* – Specifies the name of the NetFlow profile whose information you want to view. If no *netflow-profile-name* is configured, information about all NetFlow profiles is displayed.

Example:

```
hostname(config)# show netflow-profile 123
netflow-profile "123" (ID 1) (Shows the name of the NetFlow profile)
template refresh minute: 30
template refresh packet: 20
active timeout: 5
enterprise fields: disable
source interface: ethernet0/1
source address-ipv4: 20.1.1.2
source address-ipv6: 2020::2
server[1]: 124
ipv4: 10.10.10.2
ipv6: 1000::1
port: 12
server[2]:
ipv4: 0.0.0.0
ipv6: ::
port: 0
```

To view the NetFlow statistic information, in any mode, use the following command:

show netflow [**generic**] | [**slot** *slot-no*]

- **generic** – Shows the general NetFlow statistic information.
- **slot** *slot-no* – Shows the NetFlow statistic information of the specified slot.