Hillstone Networks

StoneOS Cookbook

Version 5.5R11 V12



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 configuration instructions of Hillstone Networks StoneOS user scenarios.

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-CBK-UNI-5.5R11-EN-V12-7/15/2024

Contents

Contents

Overview

How to Use Cookbook

- Target audience 2
- StoneOS Versions 2
- Reading Sequence 2
- Text vs. Screenshots 2
- Getting Started and Other Chapters 2
- Interface, Name, Topology 3
- Clicking OK or Apply 3

Getting Started

- Upgrading Firmware to Higher Version 5
  - Preparation 5
  - Method 1: Upgrading from WebUI 6
  - Method 2: Upgrading from CLI 7
- Upgrading Firmware to Higher Version in HA mode 9
  - Preparation 9
  - Upgrade Steps 10
- Using Security Policy to Allow Access to Another Zone 15
  - Configuration Steps 16

Allowing Internet to Visit a Private Server Using DNAT 21
Configuration Steps 22
Allowing Private Network to Access Internet Using SNAT 26
Configuration Steps 27
Configuring the Device to Communicate with Zabbix Using SNMP 31
StoneOS 31
Zabbix: 33
Dynamically Manage Access Authority Via Radius Dynamic Authorization 38
Scenario 38
Configuration Steps 39
Deploying Tap Mode to Monitor Network Traffic 48
Preparation 48
Configuring Tap Mode and Threat Detection 49
DNS Proxy 57
Scenario 57
Preparation 58
Configuration Steps 59
Q&A 62
Adding an SNAT Rule to StoneOS through NETCONF 63
Preparation 63
Configuration Steps 63
Device A 63

NETCONF Client 64
Viewing the results 67
Binding the Log Processing Process and Database Storage Process to Core MAX 68
Configuration Roadmap 68
Configuration Steps 69
Viewing the results 70
DHCP ZTP 71
Networking Scenario 71
Preparations 71
Procedure 72
Routing
Realizing Multicast Forwarding Through PIM-SM Multicast Protocol 75
Configuration Steps 75
Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol 84
Configuration Steps 84
Deploying HA Scenario for Multicast Forwarding Through PIM-SM 91
Configuration Steps 93
Authentication
Allowing the Internet Access via User Authentication 99
Configuration Steps 99
Using AD Polling for SSO 107
Preparation 107

Configuration Steps 108
Allowing Internet Access via AD Polling 116
Preparation 116
Configuration Steps 117
Allowing Internet Access via AD Agent 127
Preparation 127
Configuration Steps 128
Allowing Internet Access via TS Agent 138
Preparation 138
Configuration Steps 139
VPN
Connection between Two Private Networks Using IPSec VPN (IKEv1) 147
Configuration Steps 147
Device A 147
Device B 153
Connection between Two Private Networks Using IPSec VPN (IKEv2) 160
Configuration Steps 160
Device A 160
Device B 166
Establishment of IPSec VPN Based on Certificate Authentication 173
Configuration Steps 173
Device A 173

Device B 179
Realizing Dynamic Switch between IPSec Links Using IPSec VPN Smart Link 186
Configuration Steps 186
Device A 186
Device B 189
Allowing Remote Users to Access a Private Network Using SSL VPN 199
Networking Scenario 199
Configuration Steps 200
Connecting to Microsoft Azure Using Site-to-Site VPN 212
Configure Microsoft Azure 213
Configure Hillstone Device 220
Using an iOS/Android Device to Remotely Access Intranet Services 223
Using an iOS Device to Remotely Access Intranet Services 223
Using an Android Device to Remotely Access Intranet Services 228
Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN 230
Configuring Basic Settings 230
Configuring IPSec VPN 233
Configuring L2TP VPN 236
Setting up a VPN Connection 238
Adjusting Whether to Use IPSec for L2TP VPN 248
Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN 249
Configuring Basic Settings 249

Configuring IPSec VPN 252
Configuring L2TP VPN 255
Set up a VPN connection in iOS/Android 257
Allowing Remote Users (PC) to Access a Private Network Using L2TP and SSL VPN 264
Configure the Branch Firewall 264
Configure Headquarters Firewall 271
Setting up a VPN Connection 275
Connection between Two Private Networks Using GRE over IPSec VPN 277
Configuring Basic Settings 278
Configuring IPSec VPN 281
Configuring GRE VPN 286
Configuring Route and Policies 289
Configuring VXLAN Static Unicast Tunnel 293
Configuration Steps 293
VTEP1 Configuratio 293
VTEP2 Configuration 294
Zero Trust Network Access (ZTNA)
Windows User Accessing Internal Server by Using Internal Network Access via ZTNA 298
Networking Scenario 298
Configuration Roadmap 299
Preparations 300
Configuration Steps 301

Windows User Remotely Accessing Internal Server Through ZTNA 314
Networking Scenario 314
Configuration Roadmap 315
Preparations 316
Configuration Steps 319
Android User Remotely Accessing Internal Server Through ZTNA 335
Networking Scenario 335
Configuration Roadmap 336
Preparations 337
Configuration Steps 338
High Availability
Ensuring Uninterrupted Connection Using HA 347
Configuration Steps 348
Making Two Firewalls Working in Hot Standby Mode by Deploying them in HA Peer to Ensure the Continuity of Service 355
Configuration Steps 355
Verification 358
Device A and Device B Working Normally 358
Device B Failing and Device A Working Normally 359
Using Two Devices as Gateways to Forward Business Traffic and Back Up Each Other Based on HSVRP, which Ensures Uniterrupted Business Traffic 360
Configuration Steps 361
Verification 366

M0D1 and D0M1 Working Normally 366
D0M1 Failing and M0D1 Working Normally 367
Quality of Service (QoS)
QoS Control 369
Configuration Steps 370
Outbound Link Load Balance 376
Configuration Steps 377
Q&A 379
Outbound Link Load Balance with Customizable SLA Metrics 381
Configuration Instructions 382
Configuration Roadmap 382
Configuration Steps of WebUI 382
Configuration Steps of CLI 386
Threat Prevention
Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection 390
Configuration Steps 391
Protecting Intranet to Defend Attacks via Intrusion Prevention System 398
Configuration Steps 398
Forensic Analysis 406
Configuration Steps 406
Forensic Analysis Configuration Example 408
Threat Intelligence Via Hillstone Cloud Service Platform 413

Preparation 414
Configuration Steps 414
Viewing the results 415
Identifying IoT Assets to Enable Security Control of IoT by Using Built-in Docker 416
Networking Requirements 416
Preparations 417
Configuration Steps 417
Configuration Steps of WebUI 419
IoT Asset Identification Configuration 419
IoT Monitor Management 423
IoT Policy Control 425
IoT Data Analysis 427
Configuration Steps of CLI 427
IoT Asset Identification Configuration 427
IoT Monitor Management 429
IoT Policy Control 429
IoT Data Analysis 430
Identifying IoT Assets to Enable Security Control by Deploying the Asset Identifying System on the VM 431
Networking Requirements 431
Preparations 432
Configuration Steps 433
Configuration Steps of WebUI 434

IoT Asset Identification Configuration 434
VM Configuration 434
Firewall Configuration 440
IoT Monitor Management 443
IoT Policy Control 445
IoT Data Analysis 447
Configuration Steps of CLI 447
IoT Asset Identification Configuration 447
VM Configuration 447
Firewall Configuration 447
IoT Monitor Management 448
IoT Policy Control 449
IoT Data Analysis 449
Data Security
Decrypting HTTPS Traffic and Identifying the Encrypted Application 452
Configuration Steps 453
URL Filtering for HTTPS Traffic without the CA Certificate 456
Preparation 456
Configuration Steps 457
IPv6
Connecting IPv6 and IPv4 Networks 463
Configuring Networks of Headquarters 463

Configuring Networks of Branch A 468
Configuring Networks of Branch B 471
Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG 474
Before You Start 475
Configuration Steps of Scenario 1 475
Configuration Steps of Scenario 2 476
Configuration Steps of Scenario 3 479
Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG 483
Before You Start 485
Configuration Steps of Scenario 1 485
Configuration Steps of Scenario 2 487
Configuration Steps of Scenario 3 490
Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel 494
Configuration Steps 494
Allowing Communication Between IPv6 networks by Configuring a 6RD Tunnel 497
Configuration Tips 498
Configuration Steps of Scenario 1 498
Configure Headquarters Device (Device) 498
Configure Device A 501
Configuration Steps of Scenario 2 504
Configure Headquarters Device (Device) 504
Configure Device B 507

Result of Scenario 1 510

Result of Scenario 2 511

Change Log

Cookbook V1 513

Cookbook V2 513

Cookbook V3 513

Cookbook V4 514

Cookbook V5 514

Cookbook V6 514

Cookbook V7 515

Cookbook V8 515

Cookbook V8.1 515

Cookbook V9 515

Cookbook V10 516

Cookbook V11 516

Cookbook V12 517

Overview

StoneOS Cookbook provides configuration examples for you to user Hillstone network security products. This books covers basic getting-started cases, firewall functions, and advanced user scenarios. All configuration uses graphic user interface (GUI), or also known as web user interface (WebUI), not command line interface.

Each recipe consists of two parts: scenario settings and configuration steps. Topology and screenshot are used to assist you in understanding the key information of the case.

StoneOS Cookbook is very helpful in understanding operational logic, and improving efficiency.

StoneOS Cookbook organizes its recipes into the following chapters:

- "Getting Started" on Page 4 - Basic network connecting features.
- "Routing" on Page 74 -PIM.
- "Authentication" on Page 98- User authentication.
- "VPN" on Page 146- IPSec VPN and SSL VPN.
- "Quality of Service (QoS)" on Page 368 - Bandwidth control.
- "High Availability" on Page 346 - High availability.
- "Threat Prevention" on Page 389 - Threat prevention.
- "Data Security" on Page 451 — Data Security.
- "IPv6" on Page 462 - Connecting IPv6 and IPv4 Networks

This book is updated on requirement, not periodically.

The current version you are using is based on StoneOS 5.5R5.

How to Use Cookbook

Before you read the book, there are a few tips you need to know.

Target audience

Cookbook is written with new users in mind. However, if you use this book, you still are required to know how to use WebUI, connect cables and log in the system. Such information can be found in Getting Started Guide.

StoneOS Versions

This cookbook you are reading now is based on StoneOS 5.5.

With system updates, the user interface is subject to change, and WebUI layout may vary depending on hardware platforms. This cookbook may not comply with every detail on WebUI, please check your web pages for difference when you use this book.

Reading Sequence

When you open the book, it is better to read it in the sequence below:

1. Go to Table of Contents, and locate the feature you need;
2. Jump to that feature, read the scenario description and topology;
3. Go through step key points (marked as "Step1", "Step2") to understand configuration logic;
4. Read the left text and right screen shots to get the details.
5. Configure your device accordingly, but substitute with your own IP address or names.

Text vs. Screenshots

The step details are explained by combing description text and screenshots. The text on the left gives configuration details, highlights and notes; the sceenshot on the right is the exact screen capture of this step.

Getting Started and Other Chapters

In this cookbook, the chapter "Getting Started" is the prerequisite for other chapters. Other chapters deem that the protected network has already finished its basic networking settings mentioned in the Getting Started chapter. In other chapters, steps like NAT, default

routes and DNS are not included. So, when you reference to user scenarios in chapters other than Getting Started, you should ensure that your protected network has already been basically established.

Interface, Name, Topology

This book explains function configuration by writing scenarios (also called "cases" or "recipes"). Interface addresses, object names, and topologies are the real laboratory settings. When you configure your own network, substitute the names and addresses with your real names and addresses.

Clicking OK or Apply

Generally, when you finish filling or editing an option, you must click **OK**, **Apply**, or **Confirm** button to make the setting take effect. This kind of operation is universal. This book will not write specifically about this operation otherwise else is needed.

Getting Started

Recipes in Getting Started chapter introduce basic networking configurations.

This chapter includes the following recipes:

- "Upgrading Firmware to Higher Version" on Page 5
- "Upgrading Firmware to Higher Version in HA mode" on Page 9
- " Using Security Policy to Allow Access to Another Zone" on Page 15
- "Allowing Private Network to Access Internet Using SNAT" on Page 26
- "Allowing Internet to Visit a Private Server Using DNAT" on Page 21
- "Deploying Tap Mode to Monitor Network Traffic " on Page 48
- "Configuring the Device to Communicate with Zabbix Using SNMP" on Page 31
- "Dynamically Manage Access Authority Via Radius Dynamic Authorization" on Page 38
- " DNS Proxy" on Page 57
- "Adding an SNAT Rule to StoneOS through NETCONF" on Page 63
- "Binding the Log Processing Process and Database Storage Process to Core MAX" on Page 68
- "DHCP ZTP" on Page 71

Upgrading Firmware to Higher Version

This example introduces how to use WebUI and CLI to upgrade firmware to a higher version.

As an exit of the company's network, security device provides protections and services. Now, admin need upgrade firmware to optimize system's performance and get new functions.

Preparation

Before upgrading, we recommend you:

- See the system software version by using WebUI or CLI(`show version`) to get a suitable upgrading instructions.
- See the release notes of the target version to get a platform upgrading instructions.
- Get upgrade file of your target version from Hillstone.
- Do not upgrade at peak times, because you need to reboot device to make new version effective.
- Do not downgrade, because system configuration may be lost.
- Upgrade from CLI if your device's storage is low, and remember to remove the former firmware version before you upgrade.
- Make sure you have backed up the configuration file before upgrading.

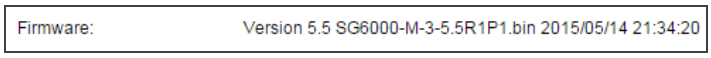
Contact us (Service Line:1-800-889-9860) first when you are in the following situations:

- Make sure whether license is out of date. If it expires, you only can upgrade system to the version whose release date is before the license expired date. If it doesn't expire, upgrading can be continued. Contact us for the release date.
- Do not cross upgrade. For example, to upgrade the versions 4.0 to 5.0, Hillstone recommends you to first upgrade to version 4.5, and then upgrade to 5.0. Contact us for cross version upgrade.
- Contact us for upgrading information if you are in HA environment.

Method 1: Upgrading from WebUI

Step 1: Logging in via WebUI with admin accout and viewing current system information.

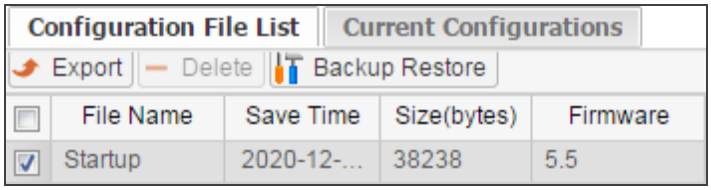
Select **System > System Information** to view the current version is 5.5R1P1.



Step 2: Exporting configuration file as a backup.

Select **System > Configuration File Management.**

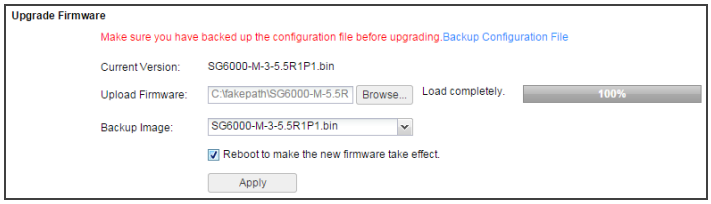
In the Configuration File List tab, select **Startup** check box and click **Export**. The configuration file will be exported to your local PC.



Step 3: Uploading upgrade file and rebooting system. Before uploading, make sure your upgrade file is suitable for your platform.

Select **System > Upgrade Management.**

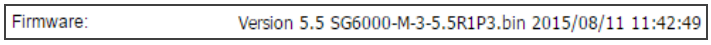
1. In the Upgrade Firmware tab, click Browse button and choose the upgrade file "SG6000-M-3-5.5R1P3.bin" in your local PC.
2. Select **Reboot to make the new firmware take effect** check box and click **Apply**. Do not select **Reboot to make the new firmware take effect** check box at traffic-peak time. Hillstone suggests you to manually reboot when you need.



Step 4: Verifying the upgrade results.

Log in via WebUI again when system finished rebooting.

1. Select **System > System Information**.
2. In the firmware part, you can see the current version is 5.5R1P3. Upgrade succeeded.

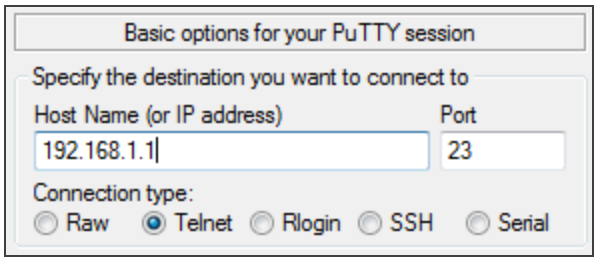


Method 2: Upgrading from CLI

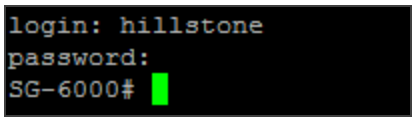
Step 1: Logging in system via Telnet, and viewing the current version.

Take an example of using PuTTY.

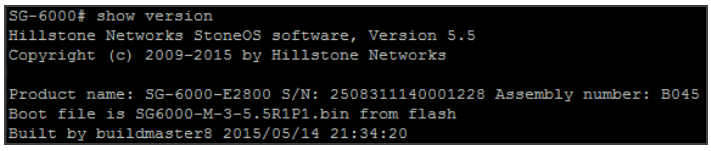
1. Open PuTTY, and enter the followings:
   Host Name: 192.168.1.1 (manage IP of your device)
   Connetion Type: Telnet
2. Click **Open**.



Type the username and password of admin. Log in successfully.

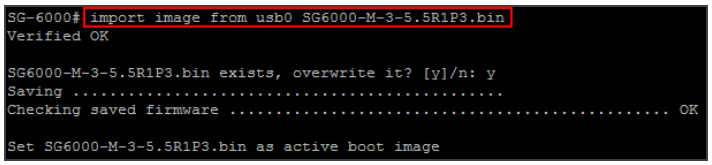


Type **`show version`** and knock the Enter key. It will show you the current system version is 5.5R1P1.

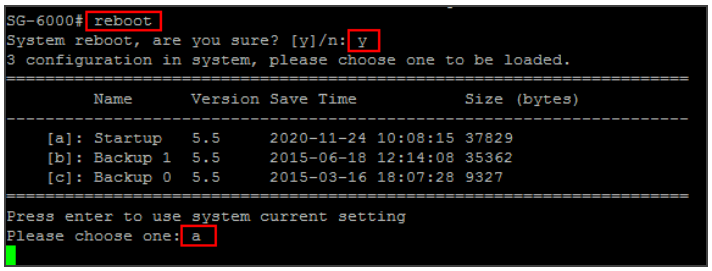


Step 2: Upgrading your device. We upgrade with USB port in this example. Please put your upgrade file in your U-Disk, and then put it into the USB port of security device.

Type **`import image from usb0 SG6000-M-3-5.5R1P3.bin`** and knock the Enter key.



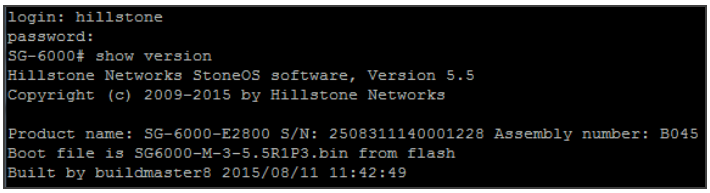
1. Type **`reboot`** and knock the Enter key.
2. System prompts that "System reboot， are you sure?". Type **y** to reboot.
3. Choose a configuration file. Type **a** after "Please choose one".



Step 3: Verifying the upgrade results.

Log in via Telnet again when system finished rebooting.

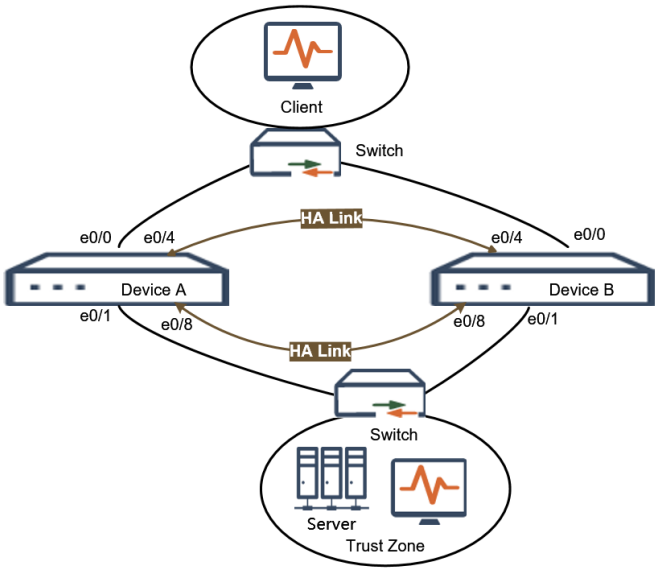
Type **`show version`** and knock the Enter key. It will show you the current system version is 5.5R1P3.



Upgrading Firmware to Higher Version in HA mode

This example introduces how to upgrade the firmware of the device in the HA Active-Passive mode.

The topology gives a typical user scenario for HA. In the designed scenario, one (Device A)of the HA devices will be working under the active mode, while the other (Device B) is under the passive mode. The two devices use heartbeat cables to maintain communication between devices. Device A and Device B need to be upgraded from StoneOS 5.5R8 to StoneOS 5.5R9.



Preparation

Before upgrading, prepare the following first:

1. Obtained the system software version by WebUI or CLI(`show version`).
2. Obtained upgrade file of the target version from Hillstone.
3. Obtained the current configurations of the two devices by WebUI or CLI(`show configuration`) , and back up the current configurations.
4. Disable the preempt mode if it is enabled. You can enable the preempt mode when the upgrading is completed. If track objects are bound to the HA group, removing the binding. You can resume the binding when the upgrading is completed.

Note: To switch over traffic, you are recommended to upgrade the devices in HA mode through the CLI.

Upgrade Steps

Step 1:Upgrading backup device (Device B).

1. Take the device B offline by removing the service cable from device B first and then removing the HA heartbeat cable from device B.

2. Save the configuration of Device B.

Device B

In any configuration mode, use the following command:

```
save
```

3. Upgrade Device B to StoneOS 5.5R9.

The detailed steps for device upgrade, see "Upgrading Firmware to Higher Version" on Page 5.

4. After device B reboots successfully, check whether the version of device B and its HA configuration are correct and whether the configuration is lost.

Device B

In any configuration mode, use the following command:

```
show configuration
```

Step 1:Upgrading backup device (Device B).

5. View the priority values of Device A and Device B. Make sure the priority value of device A is less than that of device B. That is to say, device A has a higher priority than device B.

Device A

In any configuration mode, use the following command:

```
show ha group config
```

Device B

In any configuration mode, use the following command:

```
show ha group config
```

Notes: If the priority value of device A is larger than that of device B, modify the latter to make sure device A has a higher priority.

6. Reconnect the HA heartbeat cable and the service cable on device B.

Reconnect the HA heartbeat cable on device B. Wait for device B to complete HA negotiation with device A. In this case, device A is the master device. Then, reconnect the service cable on device B.

Step 2: HA Synchronization and Master/Backup Device Switchover.

1. Synchronize the configuration of device A and device B by manual.

Device A

In any configuration mode, use the following command:

```
exec ha sync all
```

Step 2: HA Synchronization and Master/Backup Device Switchover.

2. Check whether the ARP table, session information, etc. are synchronized.

Device A

In any configuration mode, use the following command:

```
show arp
```

```
show session generic
```

```
show logging alarm
```

Notes: After executing the **`show logging alarm`** command on master device A. When the prompt "Admin batch synchronization of HA group 0 has completed." appears, it suggests that configuration synchronization is completed

3. Switch the master and backup devices by manual. In this case, device B is switched to the master device.

In any configuration mode, use the following command:

```
exec ha master switch-over
```

Step 3: Upgrading Device A.

1. Take the device B offline.

Take the device A offline by removing the service cable from device B first and then removing the HA heartbeat cable from device A.

2. Save the configuration of Device A.

Device A

In any configuration mode, use the following command:

```
save
```

Step 3: Upgrading Device A.

3. Upgrade Device A to StoneOS 5.5R9.

The detailed steps for device upgrade, see "Upgrading Firmware to Higher Version" on Page 5.

4. After device A reboots successfully, check whether the version of device A and its HA configuration are correct and whether the configuration is lost.

Device A

In any configuration mode, use the following command:

```
show configuration
```

5. View the priority values of Device A and Device B. Make sure the priority value of device A is larger than that of device B. That is to say, device A has a lower priority than device B.

Device A

In any configuration mode, use the following command:

```
show ha group config
```

Device B

In any configuration mode, use the following command:

```
show ha group config
```

6. Reconnect the HA heartbeat cable and the service cable on device A.

Reconnect the HA heartbeat cable on device A. Wait for device A to complete HA negotiation with device B. In this case, device B is the master device. Then, reconnect the service cable on device A

Step 4: HA Synchronization

1. Synchronize the configuration of device A and device B by manual.

Device B

In any configuration mode, use the following command:

```
exec ha sync all
```

2. Check whether the ARP table, session information, etc. are synchronized.

Device B

In any configuration mode, use the following command:

```
show arp
```

```
show session generic
```

```
show logging alarm
```

Notes: After executing the **`show logging alarm`** command on master device A. When the prompt "Admin batch synchronization of HA group 0 has completed." appears, it suggests that configuration synchronization is completed

Step 5: Completing the Upgrading

1. (Optional) Switch device A to the master device by manual.

Device B

In any configuration mode, use the following command:

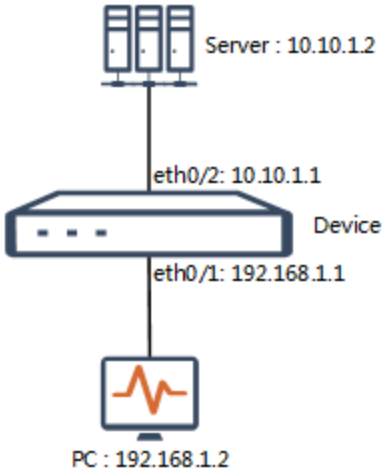
```
exec ha master switch-over
```

2. Complete the upgrading.

Using Security Policy to Allow Access to Another Zone

This example introduces how to use security policies to control communication between two zones.

The scenario sets up a requirement that the private network users are not allowed to access Internet during work time. As the topology described, polices and schedules work together to allow internal users to access to server in another zone during work hour (9 a.m. to 17 p.m.). When it's not working time, the server cannot be accessed.



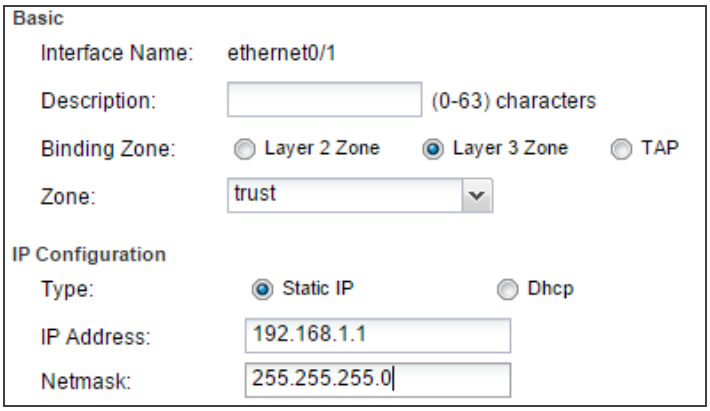
Configuration Steps

Step 1: Configuring Interface

1. Configuring the interface connected to private network

Select **Network > Interface**, double click ethernet0/1.

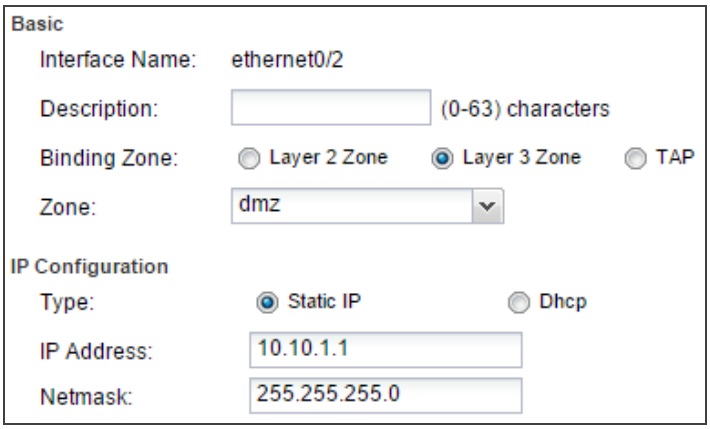
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0



2. Configuring the interface connected to Server

Select **Network > Interface**, double click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0

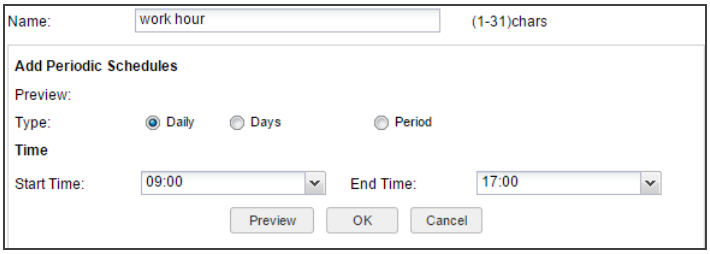


Step 2: Configuring Schedule

Select **Object > Schedule**, and click **New**. In the prompt, click **Add**.

- Name: work hour
- Type: Daily
- Start Time: 09:00
- End Time: 17:00

Click **OK** to add it.

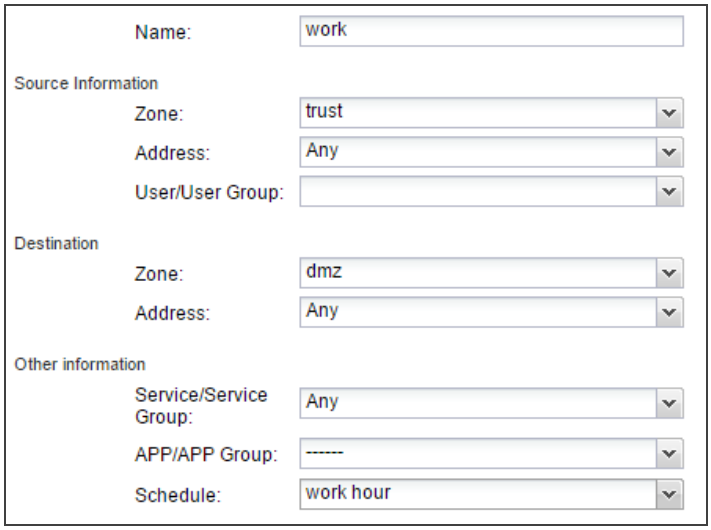


Step 3: Configuring Policies

1. Configuring a policy to allow internal users access to server during work hour

Select **Policy > Security Policy**, and click **Add**.

- Name: work
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Schedule: work hour
  - Action: Permit

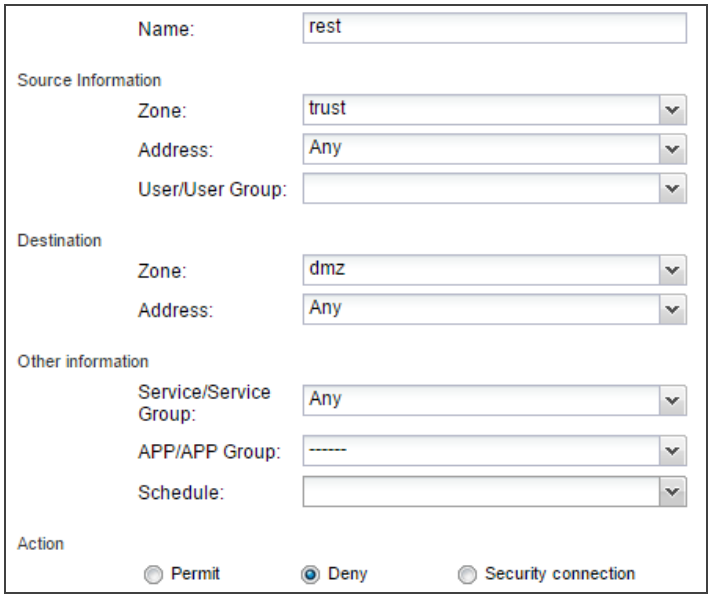


Step 3: Configuring Policies

2. Configuring a policy that internal users can-not visit server

Select **Policy > Security Policy**, and click **Add**.

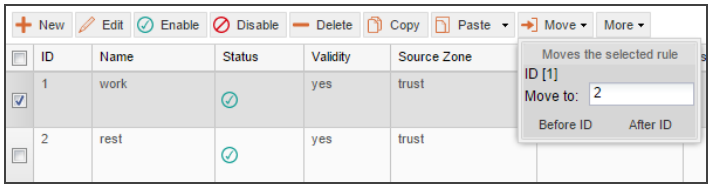
- Name: rest
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Schedule: work hour
  - Action: Deny



3. Adjusting priority of policies

Select **Policy > Security Policy**, and select the "work" policy. Select "work" policy, and click **Move**, and enter "rest" policy's ID, then click **Before ID**.

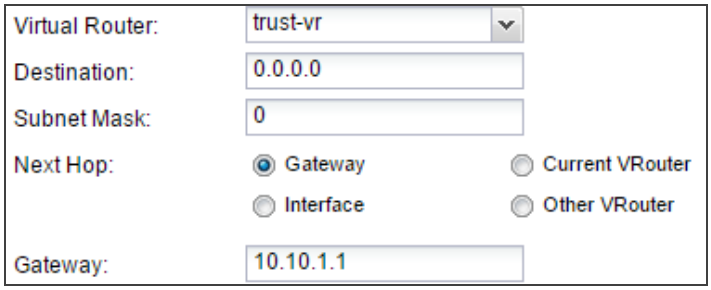
Note: The priority of a policy is only determined by its position in the list.



Step 4: Configuring a default route

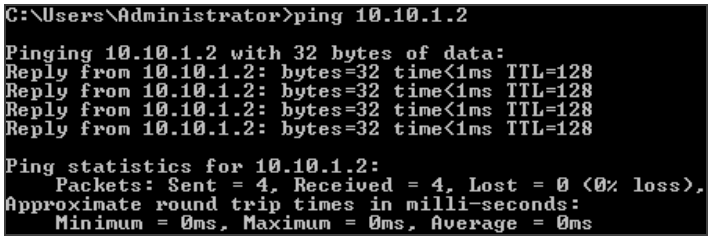
Select **Network > Routing >Destination Route**, and select **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 10.10.1.1

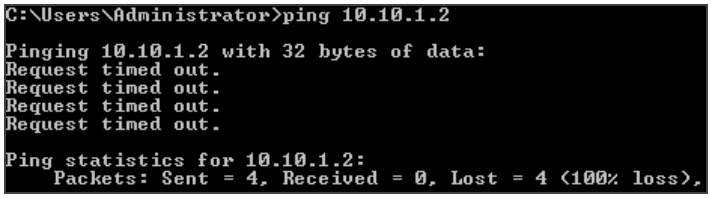


Step 5: Results

After configuration, the internal PC can ping the server address successfully during 9:00 to 17:00.



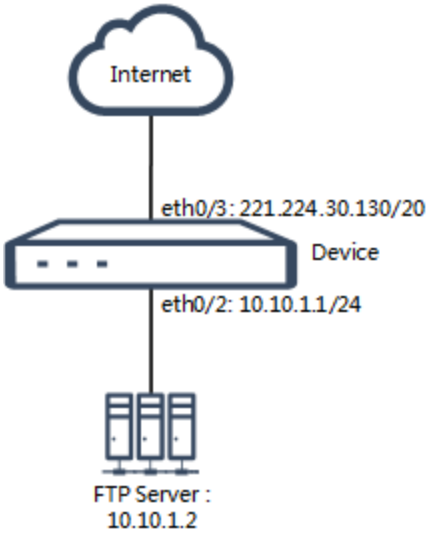
When internal PC pings the server during off-work time, it fails.



Allowing Internet to Visit a Private Server Using DNAT

Destination network address translation (DNAT) is normally used to allow Internet users visit an internal server by providing Internet IP address for internal server.

As shown in the topology, the FTP server hides its internal IP address using DNAT rule. DNAT rule will give the server an Internet IP address for FTP users to access. In this way, the server can be accessed from Internet.



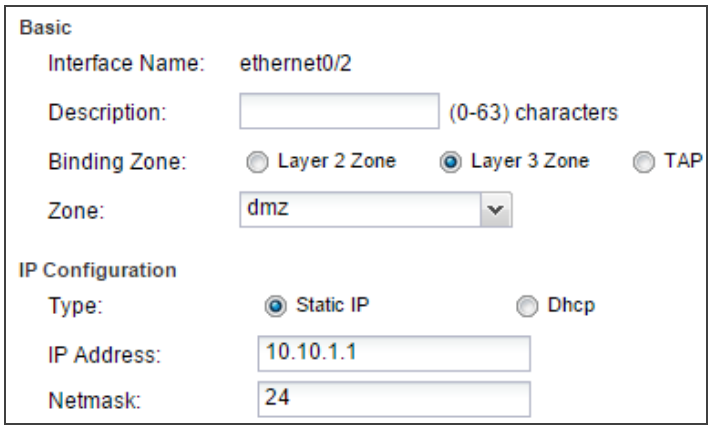
Configuration Steps

Step 1: Configuring interfaces

1. Configuring the interface connected to the server

Select **Network > Interface**, and double click ethernet0/2.

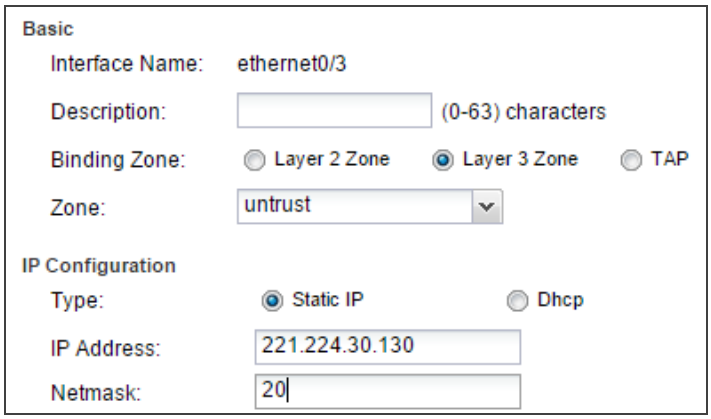
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 24



2. Configuring the interface connected to Internet

Select Network > Interface, and click ethernet0/3.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 221.224.30.130
- Netmask: 20

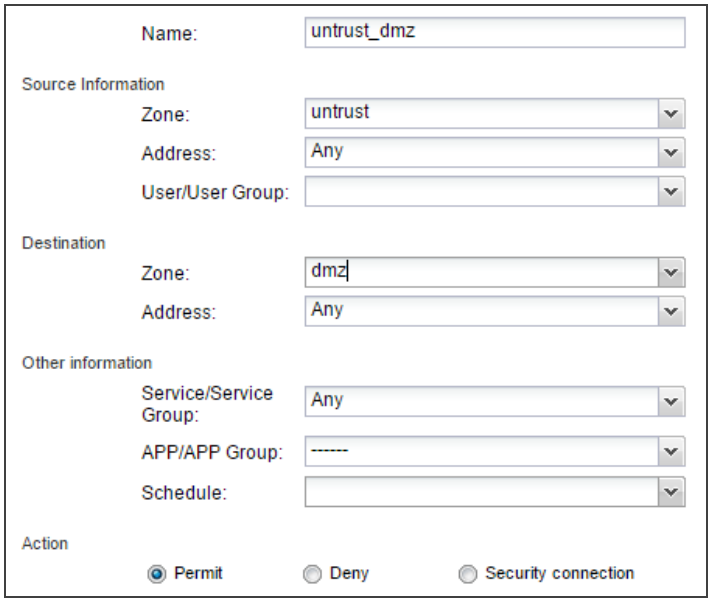


Step 2: Configuring security policies

Configuring a policy allowing Internet to visit internal network

Select Policy > Security Policy, and click Add.

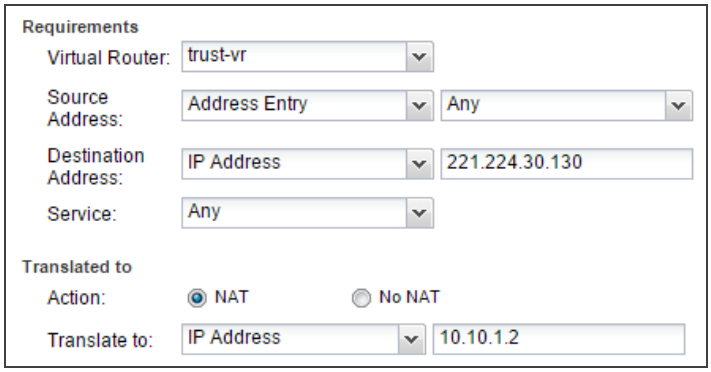
- Name: untrust_dmz
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other Information
  - Action: Permit



Step 3: Configuring DNAT rule

Select **Policy > NAT > DNAT**, and click **New > Advanced Configuration**.

- Requirement:
  - Destination Address: IP Address, 221.224.30.130 (Note: enter public IP address here.)
- Translated to:
  - Translated to: "IP Address", "10.10.1.2" (Note: enter the server's internal IP address)



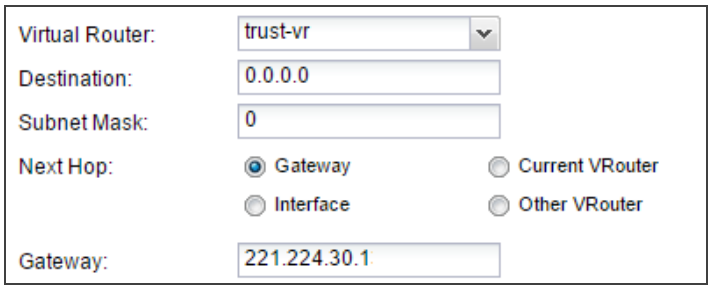
(Optional) Under Advanced tab, select NAT log check box to enable NAT logging (for checking results.)



Step 4: Configuring default route

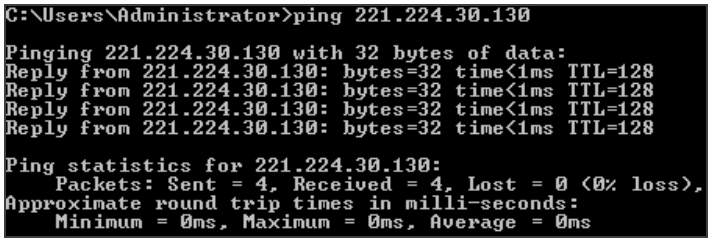
Select **Network > Routing > Destination Route**, and click **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 221.224.30.1



Step 5: Results

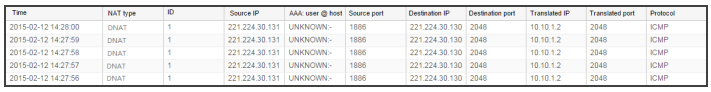
After configuration, use a PC in Internet to ping the server's public address 221.224.30.130.



Step 6: Check if DNAT rule works

Make sure NAT logging is enabled in monitor module (Select **Monitor > Log > Log Monitor**, under NAT tab, select **Enable**.)

Go to **Monitor > Log > NAT**, you will be able to see the destination IP 221.224.30.130 has been translated to internal IP 10.10.1.2.

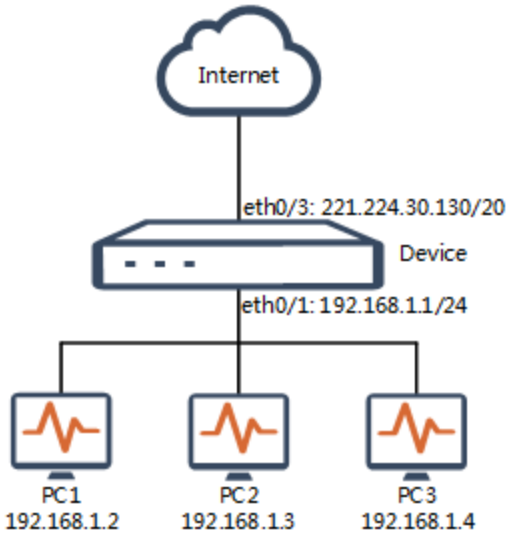


Time	NAT type	ID	Source IP	AAA user @ host	Source port	Destination IP	Destination port	Translated IP	Translated port	Protocol
2015-02-12 14:28:00	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:59	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:58	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:57	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP
2015-02-12 14:27:56	DNAT	1	221.224.30.131	UNKNOWN:-	1886	221.224.30.130	2048	10.10.1.2	2048	ICMP

Allowing Private Network to Access Internet Using SNAT

SNAT rule is used to allow users in private network to access Internet. An SNAT rule will translate the internal IP addresses to a public IP address, so that internal users can have access to public network via the public interface.

As shown in the topology, via SNAT, internal PCs use the eth0/3 (221.224.30.130/20) to visit Internet.



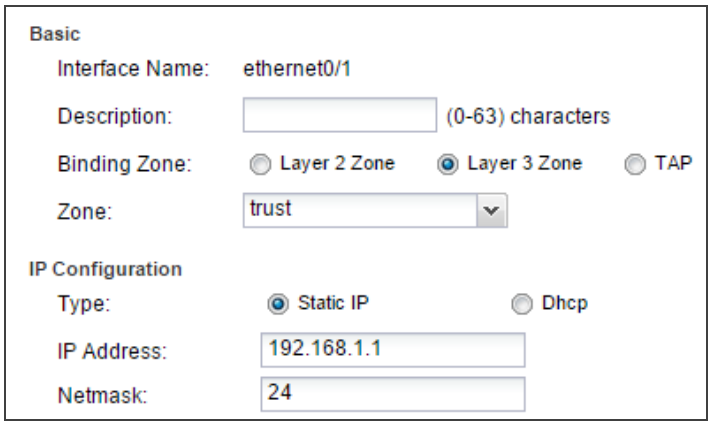
Configuration Steps

Step 1: Configuring Interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

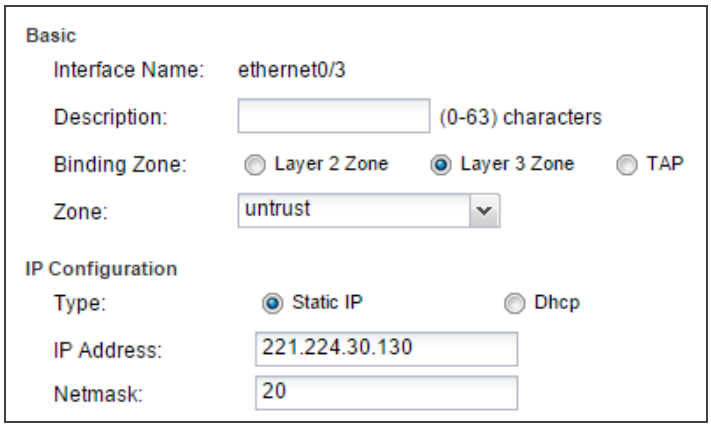
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 24



2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/3.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 221.224.30.130
- Netmask: 20

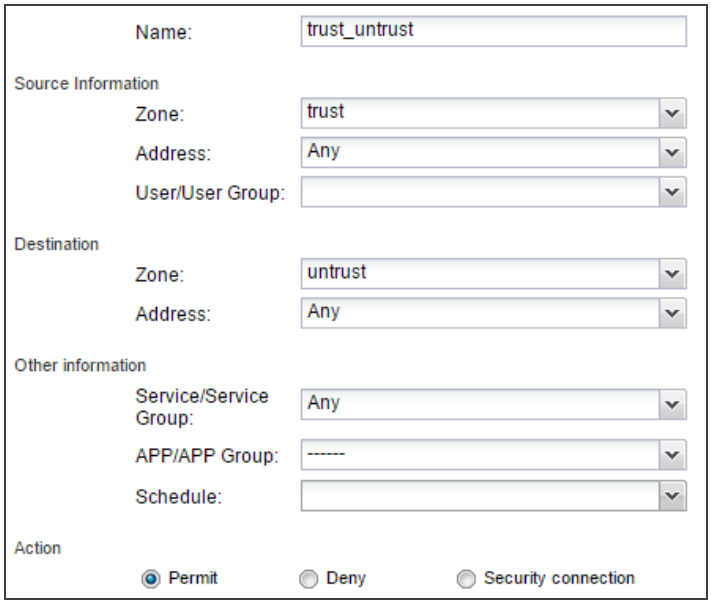


Step 2: Configuring security policy

Configuring a security policy to allow private network to Internet

Select **Policy > Security Policy**, and click **Add**.

- Name: trust_untrust
- Source Information
  - Zone: trust
  - Address: Any
- Destination
  - Zone: untrust
  - Address: Any
- Other Information
  - Action: Permit

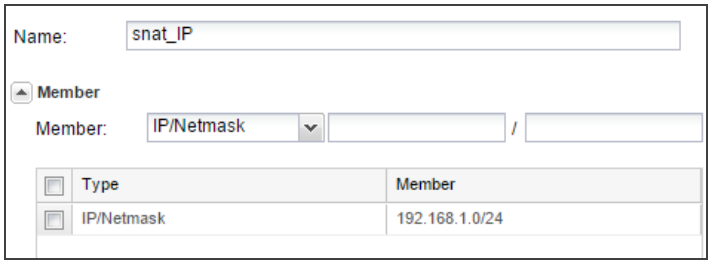


Step 3: Configuring Address book

Configuring an address range for private network users

Select **Object > Address Entry**, and click **New**.

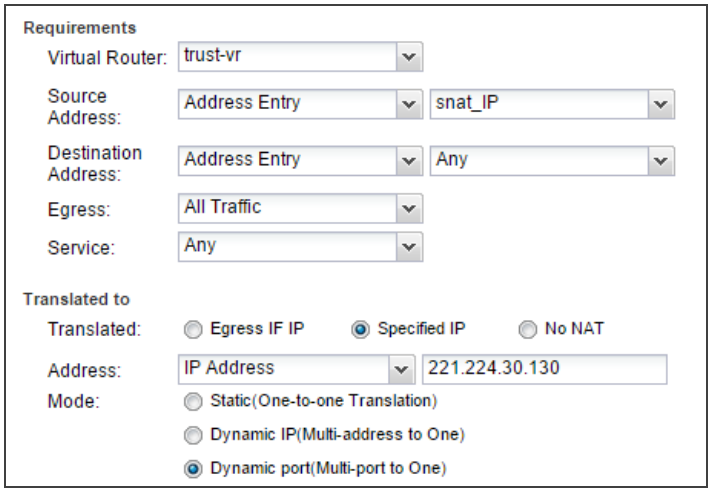
- Name: snat_IP
- Member: add "192.168.1.0/24"



Step 4: Configuring SNAT rule

Select **Policy > NAT > SNAT**, and click **New**.

- Requirement:
  - Source Address: Address Entry, snat_IP (Note: enter the server's internal IP address.)
- Translated to:
  - Specified IP: "IP Address", "221.224.30.130" (Note: enter public IP address here)
  - Mode: Dynamic Port (multi-port to one)



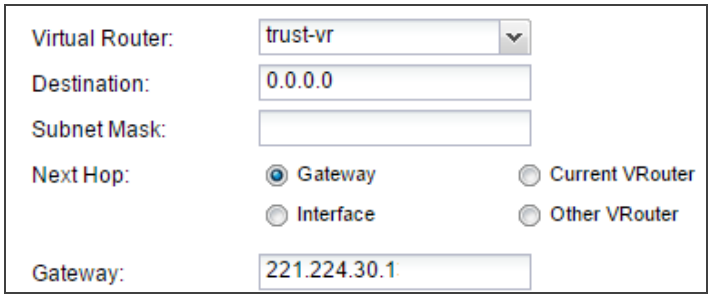
(Optional) Under Advanced tab, select NAT log check box to enable NAT loggling (for checking results).



Step 5: Configuring default route

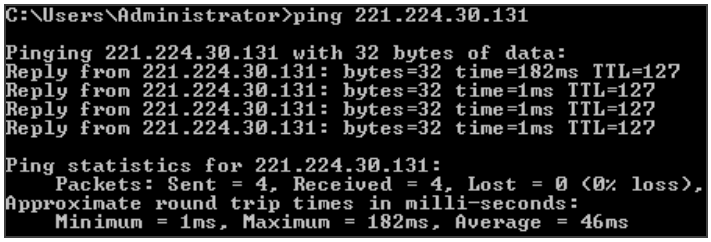
Select **Network > Routing > Destination Route**, and click **New**.

- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: Gateway
- Gateway: 221.224.30.1



Step 6: Results

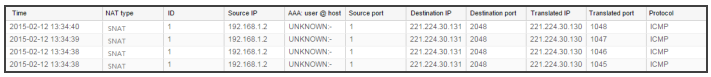
After configuration, PCs in private network can ping 221.224.30.131 successfully.



Step 6: Check if DNAT rule works

Make sure NAT logging is enabled in monitor module (Select **Monitor > Log > Log Monitor**, under NAT tab, select **Enable**.)

Go to **Monitor > Log > NAT**, you will be able to see the destination IP 192.168.1.2 has been translated to internal IP 221.224.30.130.

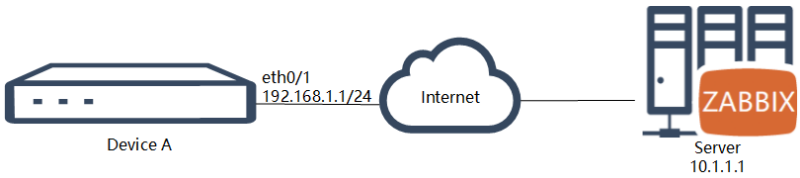


Time	NAT type	ID	Source IP	AAA: user @ host	Source port	Destination IP	Destination port	Translated IP	Translated port	Protocol
2015-02-12 13:34:40	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1048	ICMP
2015-02-12 13:34:39	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1047	ICMP
2015-02-12 13:34:38	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1046	ICMP
2015-02-12 13:34:38	SNAT	1	192.168.1.2	UNKNOWN:-	1	221.224.30.131	2048	221.224.30.130	1045	ICMP

Configuring the Device to Communicate with Zabbix Using SNMP

This example introduces how to configure the device to communicate with Zabbix using SNMP. Zabbix can monitor various network parameters of the device to ensure the safe operation of the device.

The following shows a network environment. The device connects to Zabbix using SNMPv2 to manage the device.

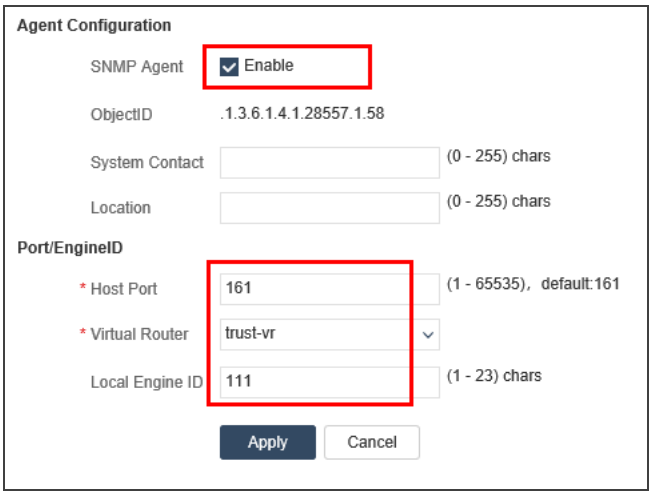


StoneOS

Step1: Configuring SNMP Agent

Select **System > SNMP > SNMP Agent**.

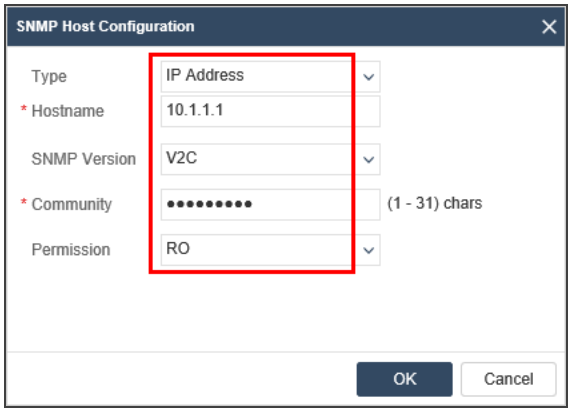
- SNMP Agent: Click **Enable**
- Host Port: 161
- Virtual Router: trust-vr
- Local Engine ID: 111



Step2: Configuring SNMP Host

Select **System > SNMP > SNMP Host**. Click **New**.

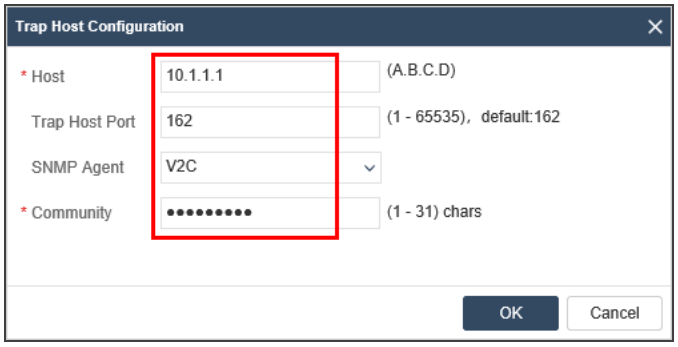
- Type: IP Address
- Hostname: 10.1.1.1
- SNMP Version: V2C
- Community: hillstone
- Permission: RO



Step3: Configuring Trap Host

Select **System > SNMP > Trap Host**. Click **New**.

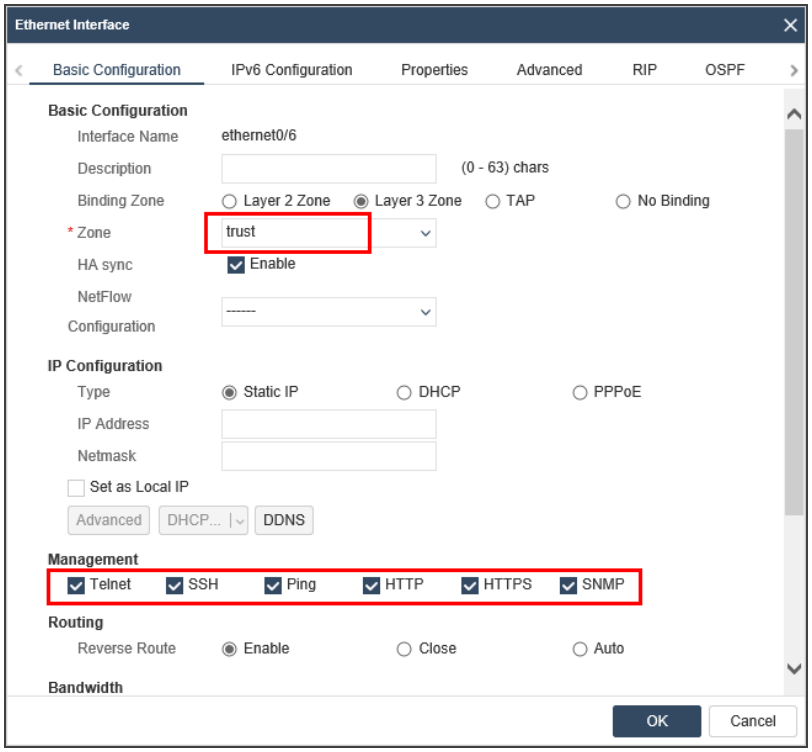
- Host: 10.1.1.1
- Trap Host Port: 162
- SNMP Agent: V2C
- Community: hillstone



Step4: Enabling the SNMP Mode of the Interface

Select **Network > Interface** and double click ethernet0/6.

- Zone: trust
- Management: Click **SNMP**

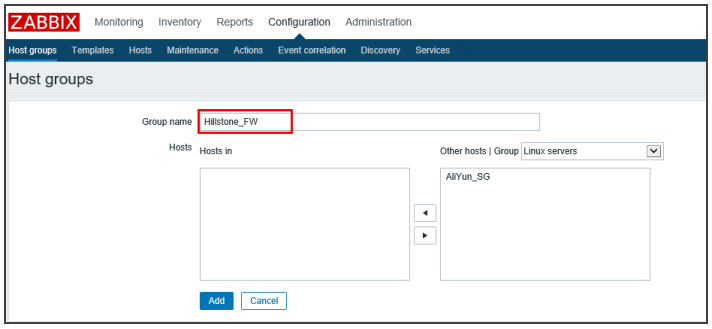


Zabbix:

Step1: Configuring Host Group

Select **Configuration > Host groups**. Click **Create host group**.

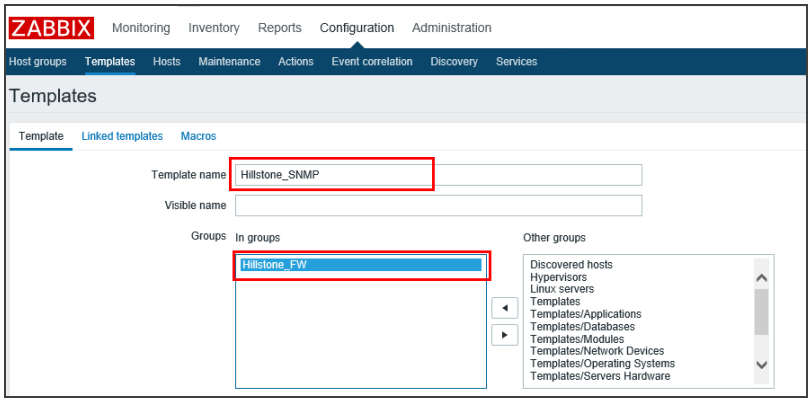
- Group name: Hillstone_FW



Step2: Configuring Templates

Select **Configuration > Templates** . Click **Create template**.

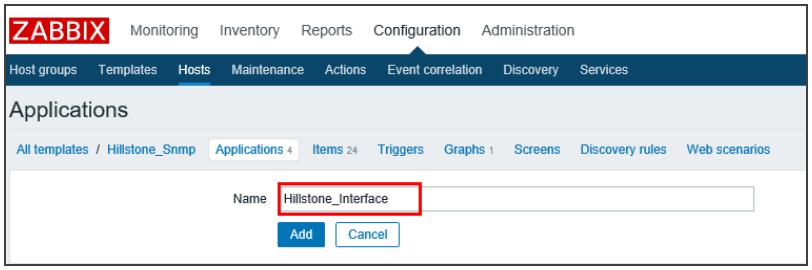
- Template name: Hillstone_SNMP
- Click ◂ icon to add **Hillstone_FW** to **In groups** list.



Step3: Configuring Application

Select **Configuration >Template > Applications**. Click **Create application**.

- Name: Hillstone_Interface

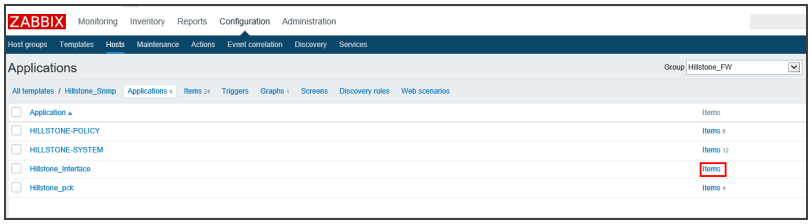


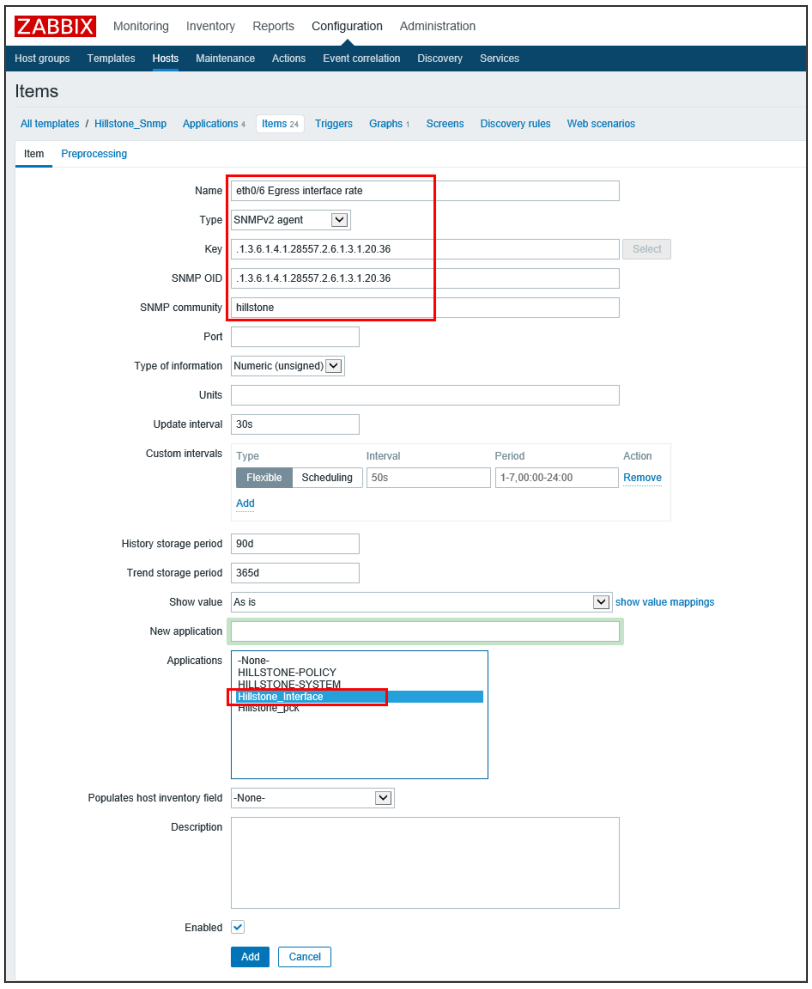
Step4: Configuring Item

Select **Configuration > Templates > Applications**. Click **Items** of **Hillstone_Interface** and click **Create item**.

- Name: eth0/6 Egress interface rate
- Type: SNMPv2 agent
- SNMP OID: .1.3.6.1.4.1.28557.2.6.1.3.1.20.36
- SNMP community: hillstone
- Applications: Select **Hillstone_Interface**

Note: You need to add the index of the specified interface after OID. To view the index of the interface, use the command **`show ip route interface`**.

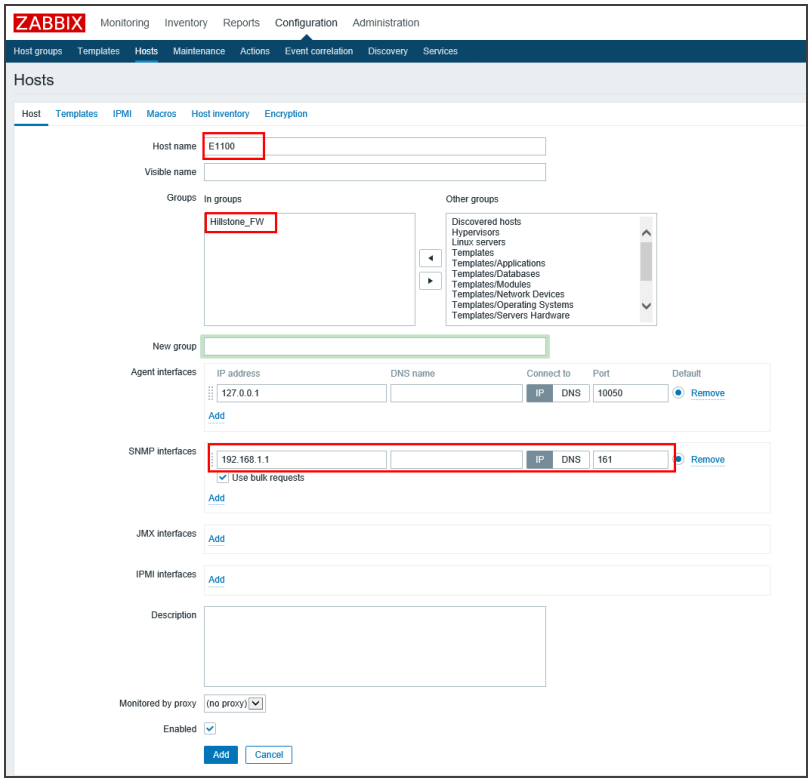




Step5: Configuring Host

Select **Configurations > Hosts**. Click **Create host**.

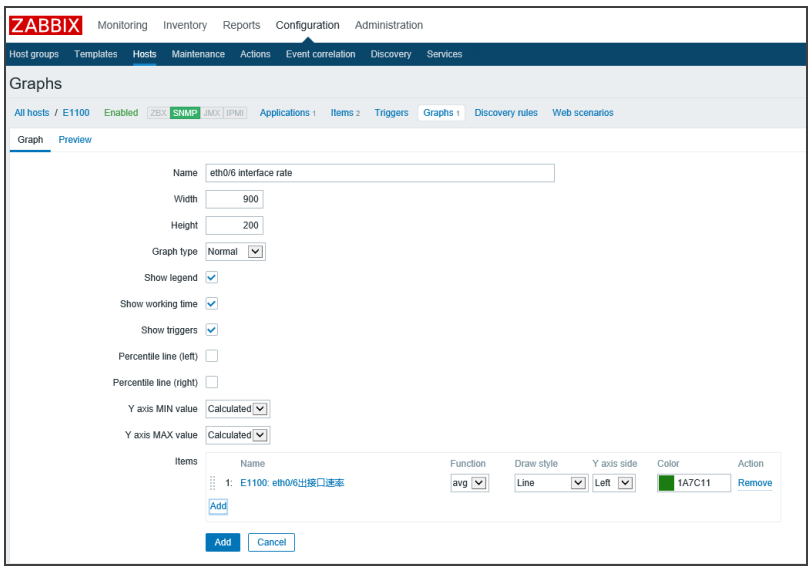
- Host name： E1100
- Click icon to add **Hillstone_FW** to **In groups** list.
- In **SNMP interfaces** area, click **Add** and type the ip address of StoneOS 192.168.1.1, Port 161.



Step6: Configuring Graph

Select **Configuration > Hosts**. Click **E1100 > Graphs** and click **Create graph**.

- Name: eth0/6 interface rate
- Click **Add** in the **Items** area. Select **eth0/6 Egress interface rate**.

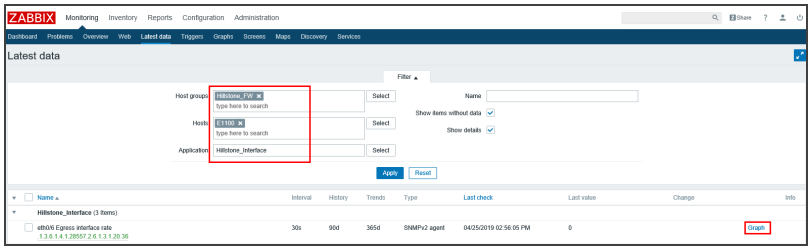


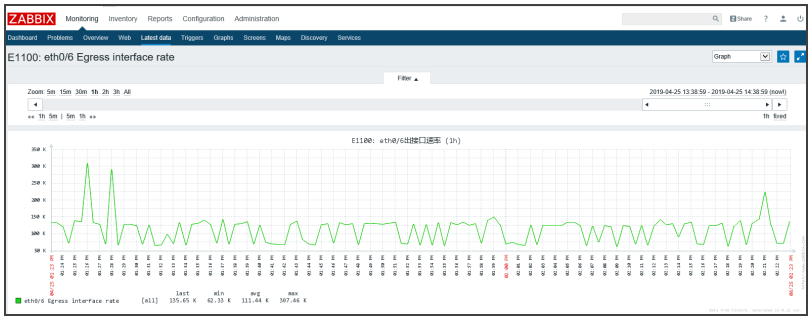
Step7: Results

After configuration, select **Monitoring >Latest data** to view the monitoring data.

- Host groups: Select **Hillstone_FW**
- Hosts: Select **E1100**
- Application: Select **Hillstone_Interface**

Click **Graph** to view the monitoring graph.



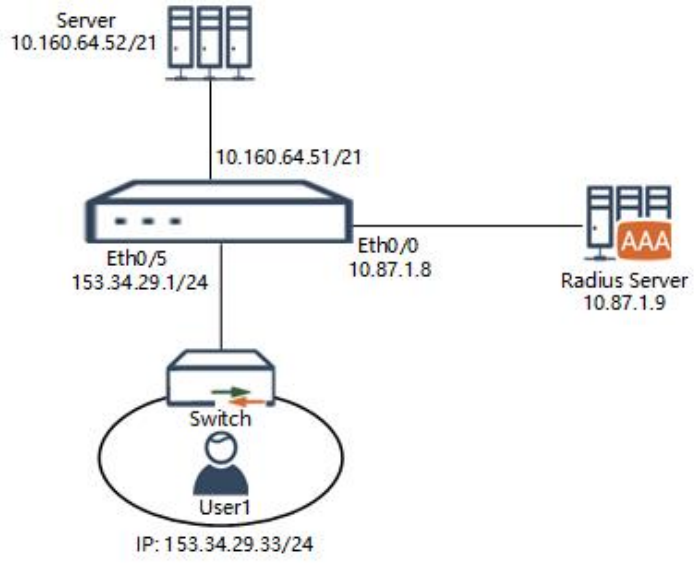


Dynamically Manage Access Authority Via Radius Dynamic Authorization

This example introduces how to dynamically manage access authority via radius dynamic authorization.

Scenario

As shown in the topology, one enterprise can configure Radius server authentication and enable authorization policy to dynamically manage the access authority of visitors. When the visitor logins the SSLVPN, the radius server issues authorization policy to the firewall allowing the visitor to visit the network segment 10.160.64.0/21. When the visitor successfully logins, the administrator can use CoA messages to modify the issued authorization policy, adding new network segment 10.160.32.0/21 that the visitor is allowed to visit. When the visitor logs out, the firewall will automatically delete the responding authorization policy.

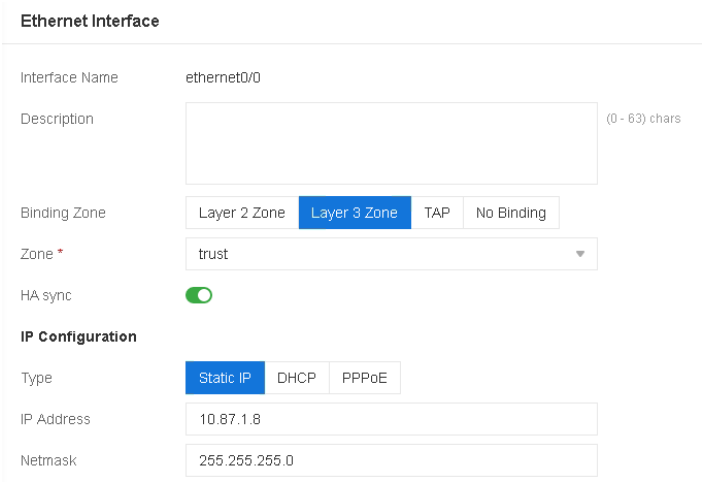


Configuration Steps

Step 1: Configure the Interface to Link Radius Server.

Select **Network>Interface**, and double click **ethernet0/0**.

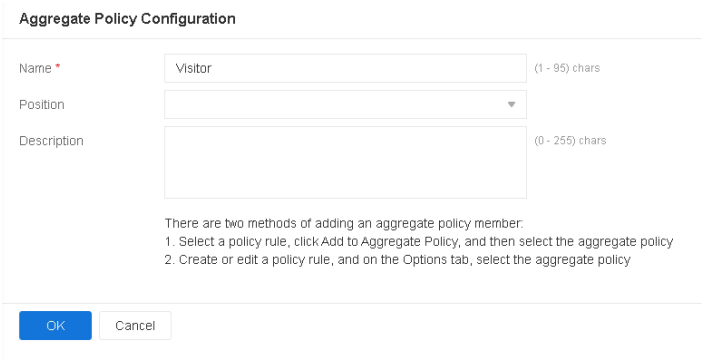
- Binding zone: Layer 3 zone
- Zone: trust
- Type: Static IP
- IP Address: 10.87.1.8
- Netmask: 255.255.255.0



Step 2: Create New Aggregate Policy.

Select **Policy>Security Policy>Policy**, and click **New>Aggregate Policy**.

- Name: Visitor



Step 3: Configure Radius Server, and Enable Authorization Policy and Accounting.

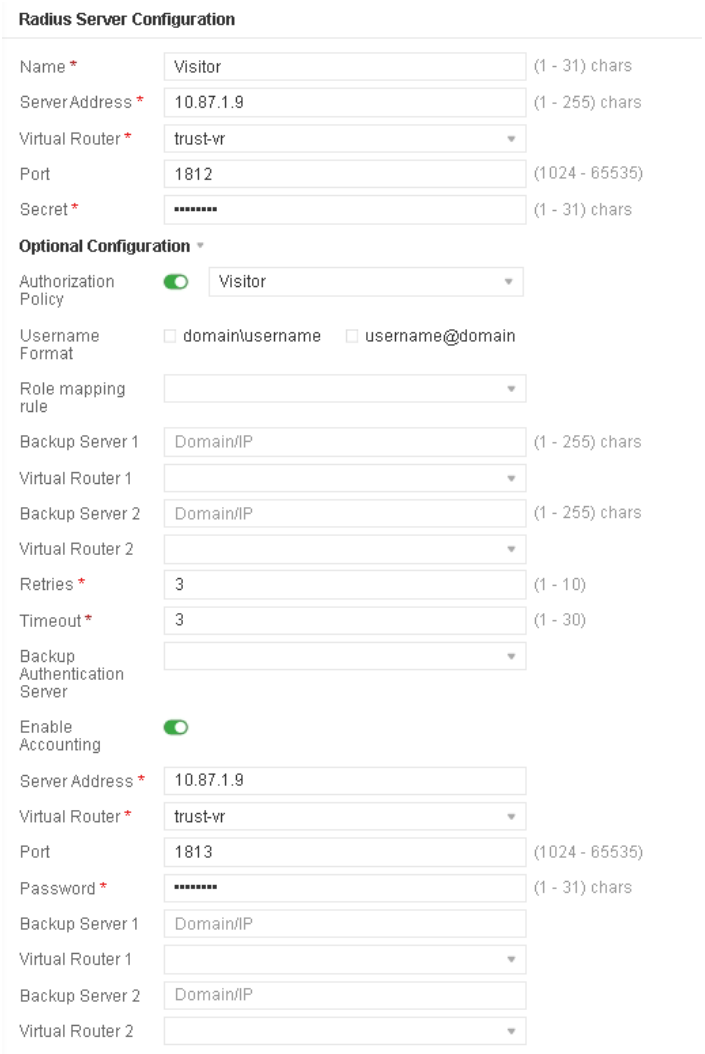
1. Select **Object>AAA Server**, and click **New>Radius Server**.

- Name: Visitor
- Server Address: 10.87.1.9
- Virtual Router: trust-vr
- Port: 1812
- Secret: 12345678

2. Click the **Enable** button of Authorization, and select **Visitor** from the drop-down menu.

3. Click the **Enable** button of Accounting.

- Server Address: 10.87.1.9
- Virtual Router: trust-vr
- Port: 1813
- Password: 12345678



Step 3: Configure Radius Server, and Enable Authorization Policy and Accounting.

4. Create a new user account.

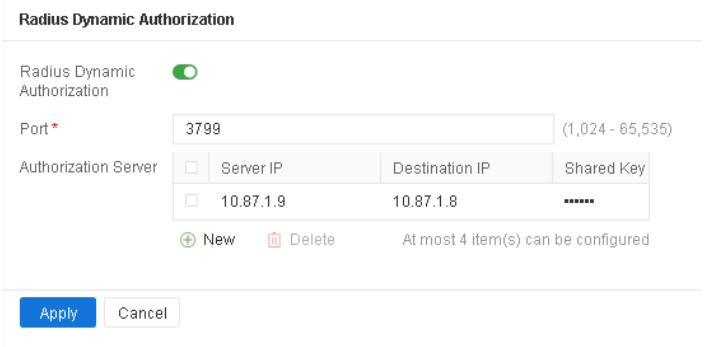
Client needs to created a new user account on Radius server.

- Username: user1
- Password: 123456
- Authorized network segment: 10.160.64.0/21

Step 4: Enable Radius Dynamic Authorization.

Click Object>Radius Dynamic Authorization, and click the Enable button of Radius Dynamic Authorization.

- Port: 3799
- Server IP: 10.87.1.9
- Destination IP: 10.87.1.8
- Shared Key: 12345678

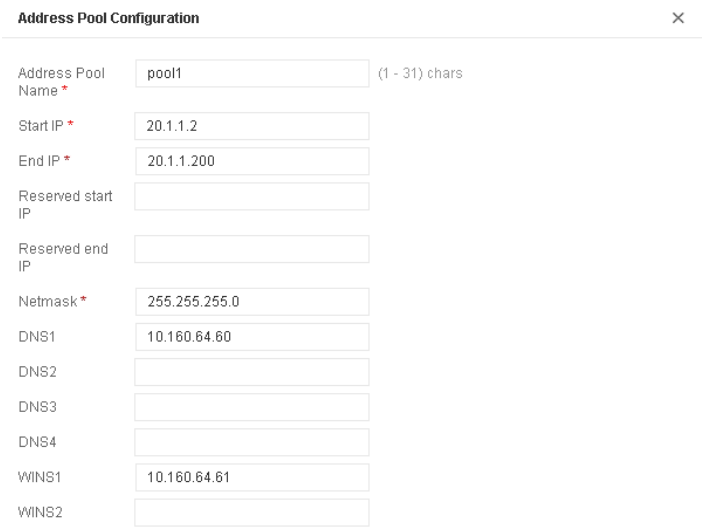


Step 5: Configure SSLVPN on StoneOS.

1. Configure SSLVPN address pool.

Select **Network>SSL VPN**, click **Configuration>Address Pool**, and click **New**.

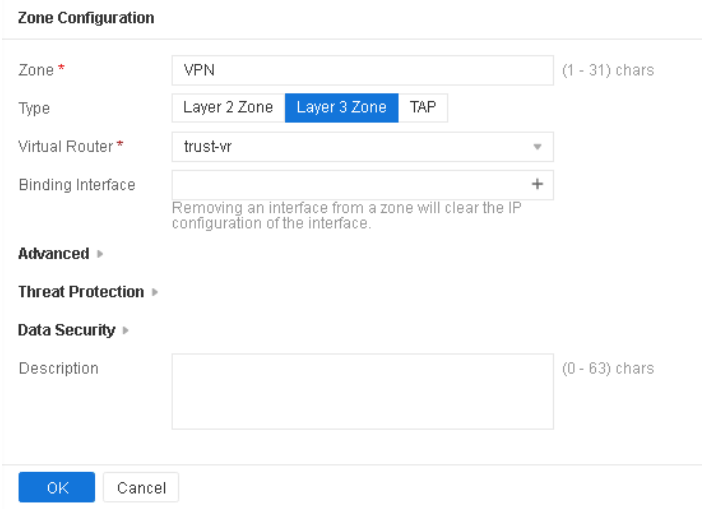
- Address Pool: pool1
- Start IP: 20.1.1.2
- End IP: 20.1.1.200
- Netmast: 255.255.255.0
- DNS1: 10.160.64.60
- WINS1: 10.160.64.61



2. Create new zone.

Select **Network>Zone**, and click **New**.

- Zone: VPN
- Type: Layer 3 Zone
- Virtual Router: trust-vr

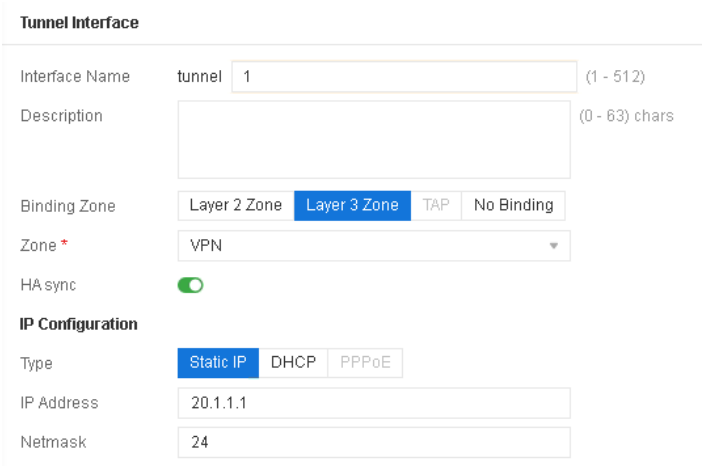


Step 5: Configure SSLVPN on StoneOS.

3. Create new tunnel interface.

Select **Network>Interface**, and click **New>Tunnel Interface**.

- Interface Name: tunnel 1
- Binding Zone: Layer 3 Zone
- Zone: VPN
- Type: Static IP
- IP Address: 20.1.1.1
- Netmask: 24



Step 5: Configure SSLVPN on StoneOS.

4. Configure SSLVPN.

Select **Network>SSL VPN**, and click **New**.

In the Name/Access User tab, configure as below.

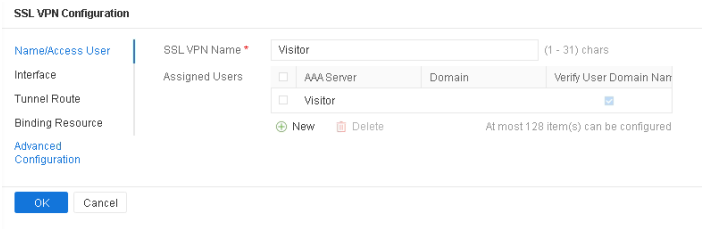
- SSL VPN Name: Visitor
- AAA Server: Visitor

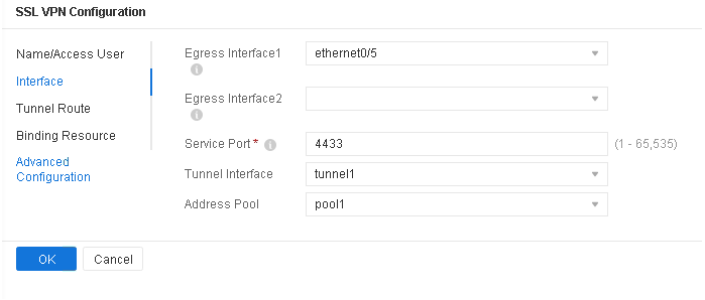
In the Interface tab, configure as below.

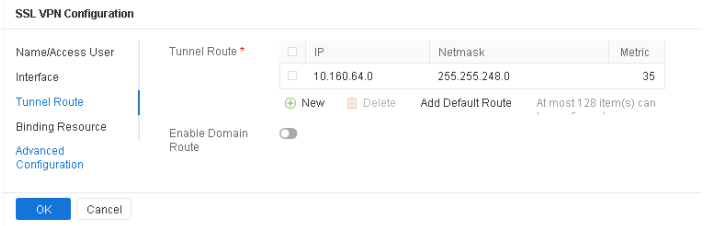
- Egress Interface 1： ethernet0/5
- Service Port： 443
- Tunnel Interface： tunnel1
- Address Pool： pool1

In the Tunnel Route tab, configure as below.

- IP： 10.160.64.0
- Netmask： 255.255.248.0



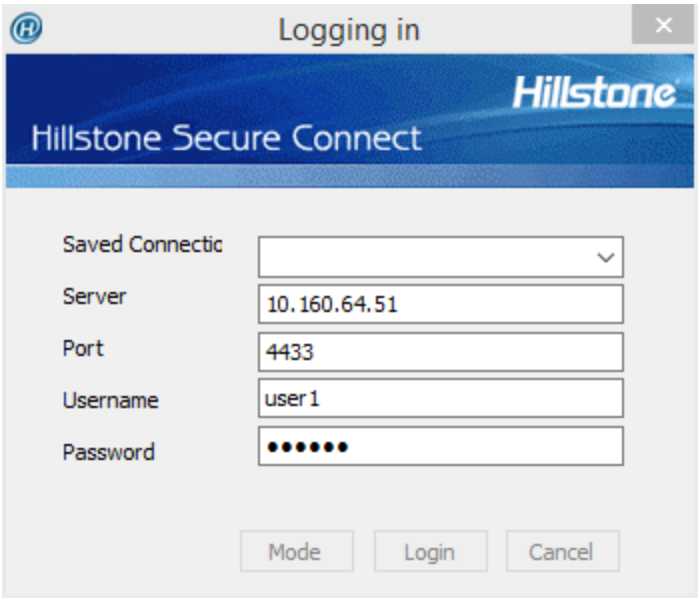




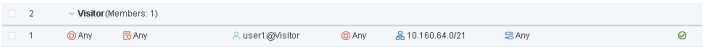
Step 6: Results.

1. User1 can access 10.160.64.52.

   - Server: 10.160.64.51
   - Port: 4433
   - Username: user1
   - Password: 123456



2. Corresponding policy is created on Firewall.

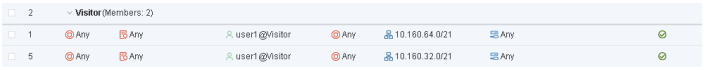


Step 7: Use CoA message to modify the access authority of the authorized user.

1. Use CoA message in CLI commands to modify the network segment that the authorized user has access to (If the radius server that the client uses is customized, the client can operate directly on radius server rather than use CLI commands).

   - Create a new txt file named coa-auth of which the content is as below:
     User-Name： user1
     Framed-IP-Address=20.1.1.3
     NAS-IP-Address=10.87.1.8
     Acct-Seesion-Id= “1”
     Hillstone-User-Data-Filter= “rule 1 permit dst 10.160.64.0/21”
     Hillstone-User-Data-Filter= “rule2 permit dst 10.160.32.0/21”
     Calling-Station-Id="00-1c-54-ff-08-05"
   - Use the blow CLI command to send the instruction (take freeradius for example):
     root@hillstone-HVM-domU:/etc/-freeradius# radclient 10.87.1.8:3799 coa 12345678 -f coa-auth.txt -x

2. Policies are updated on Firewall.

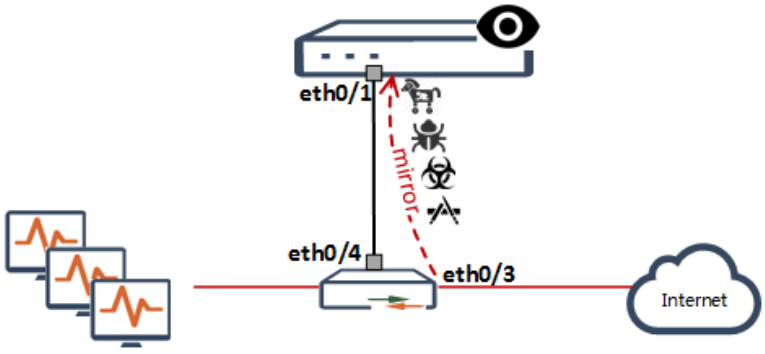


Step 8: User1 logs out of SSLVPN.

User1 logs out of SSLVPN, and the corresponding policies are deleted from Firewall.

Deploying Tap Mode to Monitor Network Traffic

Inline mode places a device directly in the network path, while in tap mode, the device only connects to a mirrored interface of core network. Tap device monitors or sniffs the packet information mirrored from core network gateway. Tap products tend to be resilient and transparent so as to minimize or eliminate the effect they can have on production traffic. If you just want a sensor to monitor, analyze and log network traffic, not data forwarding, it is best to choose tap mode.



In this example, a Hillstone device (T-Series Intelligent Next Generation Firewall recommended) is a network tap. Its tap interface eth0/1 directly connects to mirror interface of inline network gateway. Hillstone T-Series threat detection features to analyze mirrored data packets in search for network threats.

We present 4 threat detecting functions in this example. All the functions require respective licenses installed before they take effect.

- **Intrusion Prevention System (IPS)**: Requires Threat Prevention (TP) or IPS license installed.
- **Application Identification**: Requires APP DB license installed. This license is issued with platform license for free. No need to purchase APP DB license individually.
- **Advanced Threat Detection (ATD)**: Requires StoneShield license installed.
- **Abnormal Behavior Detection (ABD)**: Requires StoneShield license installed.

Preparation

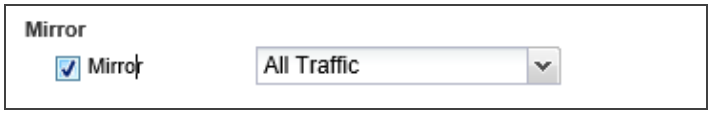
As shown in the topology above, you need use a RJ-45 cable to connect the mirror port eth0/4 and the tap interface eth0/1.

Configure port mirroring on gateway of core network. We take Hillstone gateway as example.

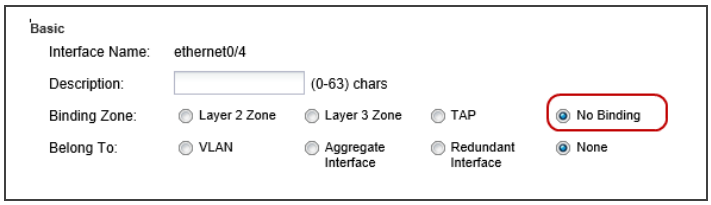
Configuring port mirroring

1. Select **Network > Interface**, and double-click **ethernet0/3**.

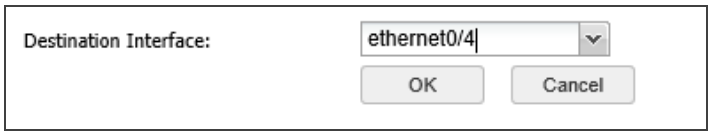
2. In the pop-up, click the **Properties** tab, under Mirror part, select the checkbox to enable traffic mirroring.



3. Return to interface list, make sure that the mirror port ethernet0/4 is not bound to any zone.



4. Select **Network > Port Mirroring**, select **ethernet0/4** from drop-down menu, and click **OK**.



Configuring Tap Mode and Threat Detection

Configure all the following settings on tap device.

Step 1: Creating a tap mode

1. Select **Network > Zone**, click **New**.

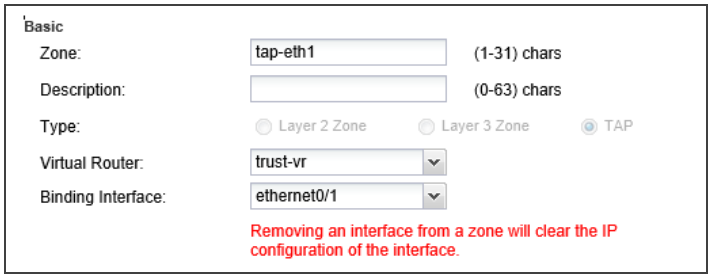
2. In the Zone Configuration dialog, configure the following:

   Zone: tap-eth1

   Type: TAP

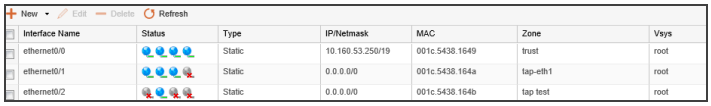
   Virtual Router: trust-vr

   Binding Interface: ethernet0/1



Step 1: Creating a tap mode

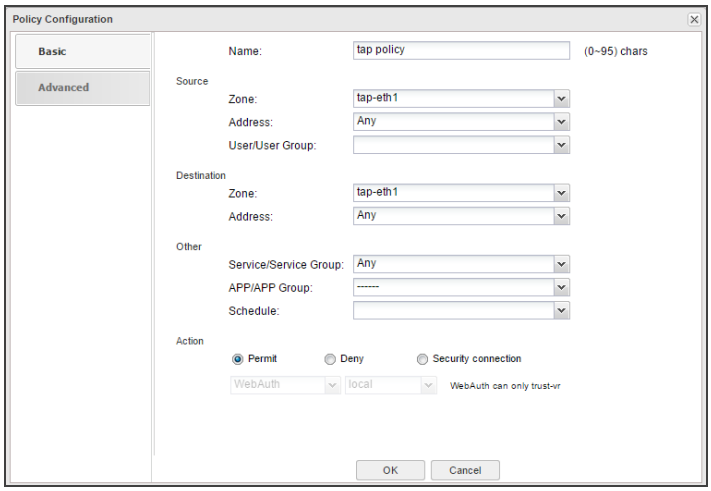
3. Return to **Network > Interface**, in the interface list, check that eth0/1 is in the "tap-eth1" zone.



Step 2: Creating a Policy

Creating a "permit" policy on the tap device so that it can establish sessions within itself.

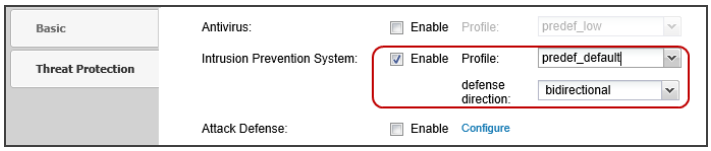
1. Select **Policy > Security Policy**, click **New**.
2. In the **Policy Configuration** dialog, make a "permit" rule from and to the same tap zone.



Step 3: Enabling IPS and viewing IPS attacks

Enabling IPS:

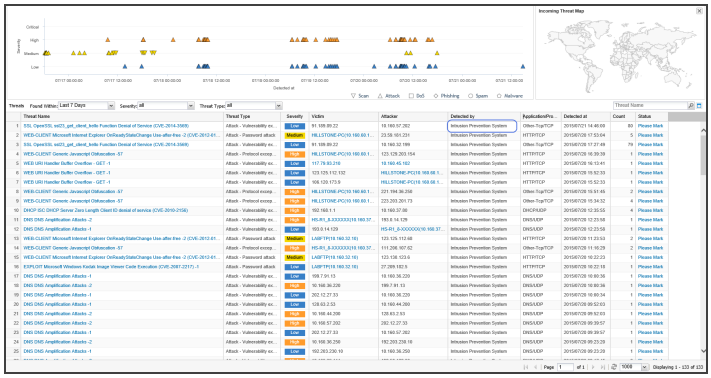
1. Select **Network > Zone**, double-click **tap-eth1**.
2. Under the Threat Prevention tab, select **Enable** check-box on the right of **Intrusion Prevention System**.
   Profile: predef_default
   Defense Direction: bidirectional



Step 3: Enabling IPS and viewing IPS attacks

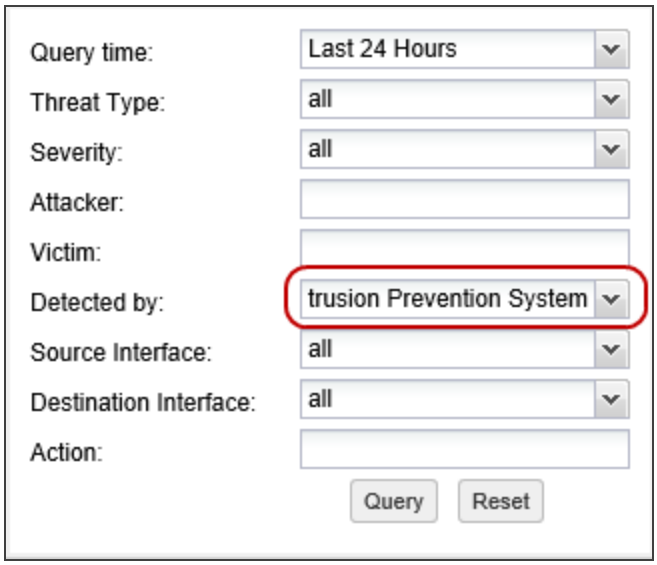
Checking detection results:

1. Select **iCenter > Threat**.
2. In the list, , items marked as "Intrusion Prevention System" under the **Detected by** column are IPS attacks detected by tap device.

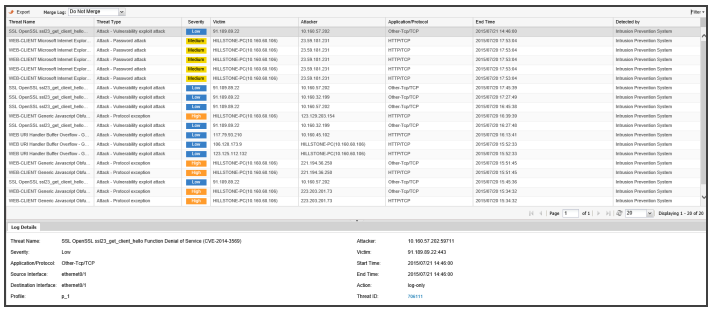


Viewing IPS logs:

1. Select **Monitor > Log > Threat**, click **Filter** on the top right corner.
   - **Detected by:** Intrusion Prevention System



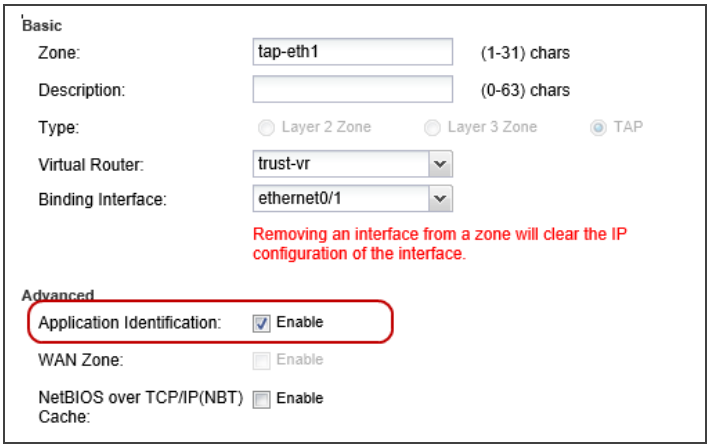
2. Click **Query**, and the page will show IPS logs.



Step 4: Enabling Application Identification and viewing APP usage statistics

Enabling APP Identification:

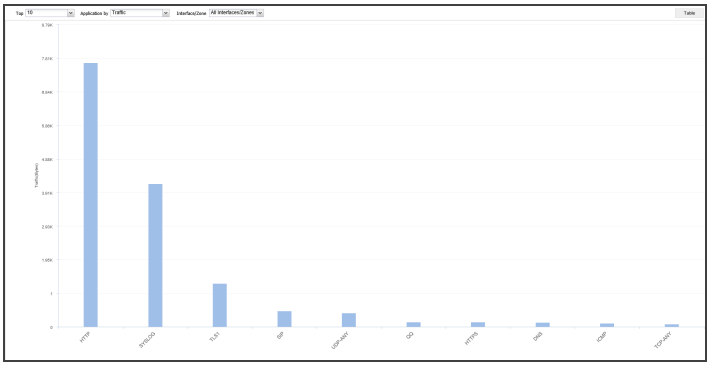
1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Basic** tab, select the **Enable** check-box after Application Identification.



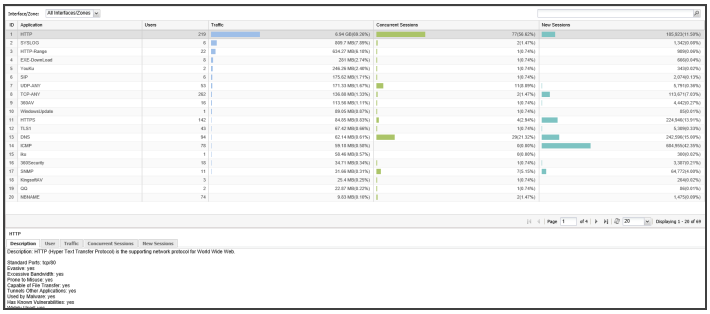
Viewing App monitor results:

Select **Monitor > Application**.

- **Summary**: Application usage statistics by user, traffic, new session or concurrent session.

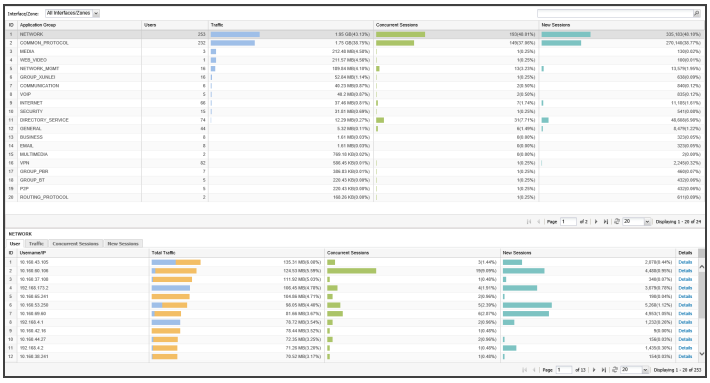


- **Application Details**: Details of every application.



Step 4: Enabling Application Identification and viewing APP usage statistics

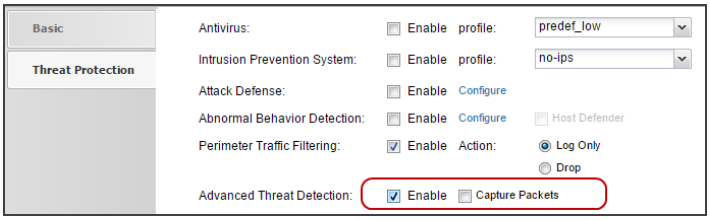
- **Group Details**: Application group usage details.



Step 5: Enabling Advanced Threat Detection (ATD) and viewing ATD attacks

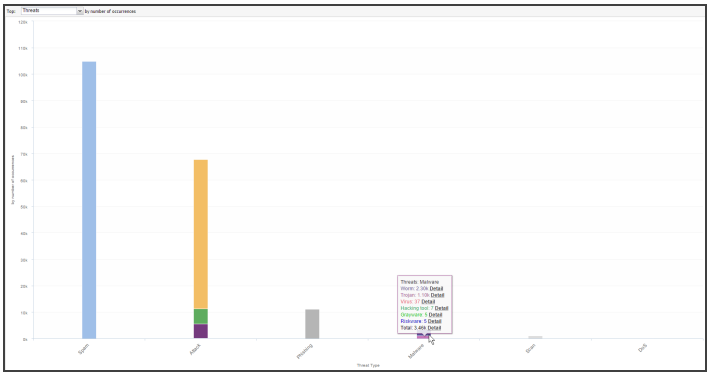
Enabling ATD:

1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Threat Prevention** tab, select the **Enable** check-box after **Advance Threat Detection**.



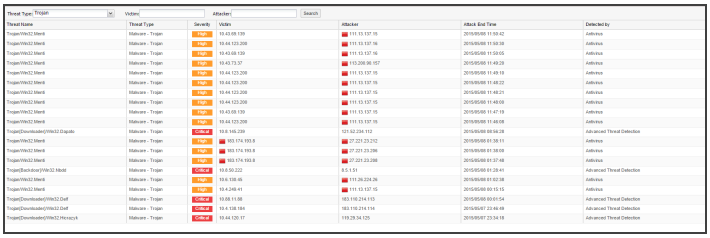
Viewing ATD monitor result:

1. Select **Monitor > Threat > Summary**, hover your cursor over **Malware** bar to show a balloon of malware attacks.



Step 5: Enabling Advanced Threat Detection (ATD) and viewing ATD attacks

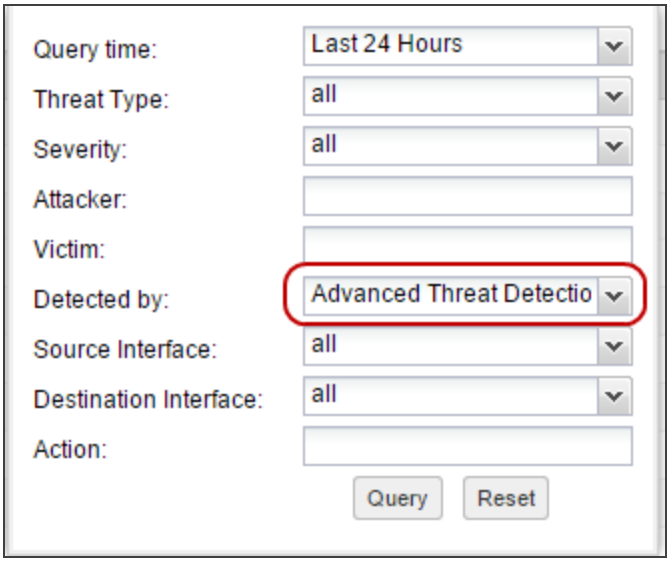
2. Click **Details** after **Trojan** in the balloon, you can see details of this attack.



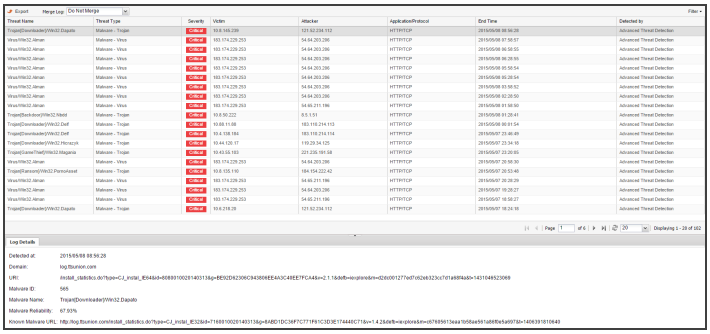
Viewing ATD logs

1. Select **Monitor > Log > Threat**, and click **Filter** on the top right corner.

   - **Detected by**: Advanced Threat Detection



2. Click **Query**, the page will show ATD logs.

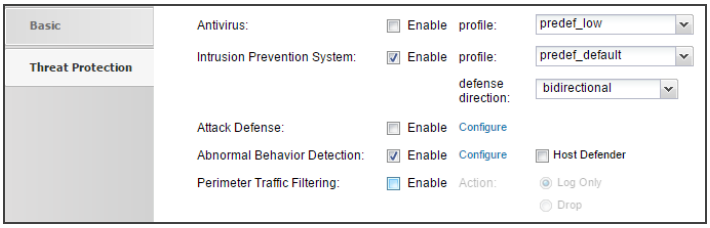


To know more about ATD, you may refer to another case in this cookbook Finding Malware Attacks via Advanced Threat Detection.

Step 6: Enabling Abnormal Behavior Detection and viewing abnormal behaviors

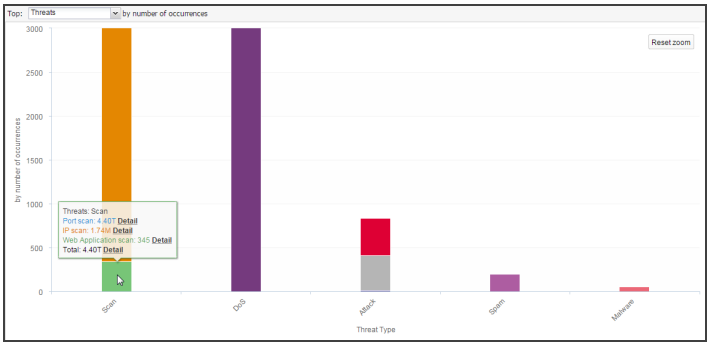
Enabling ABD:

1. Select **Network > Zone**, double-click the **tap-eth1** zone.
2. Under the **Threat Prevention** tab, select the **Enable** check-box after **Abnormal Behavior Detection**.



Viewing monitor results:

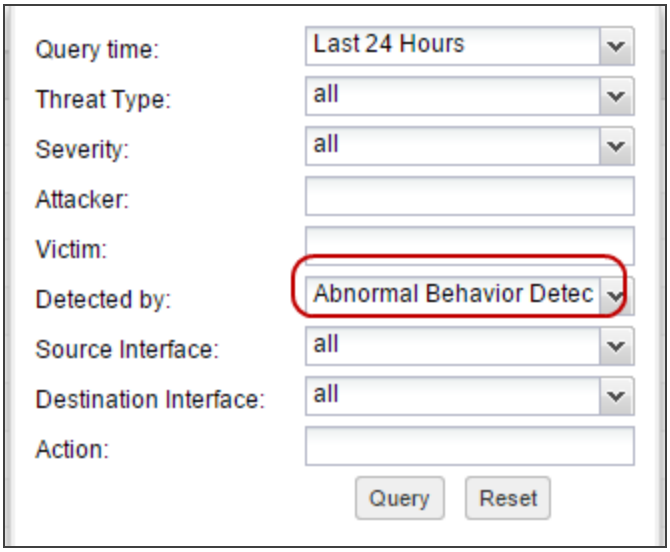
1. Select **Monitor > Threat > Summary**.
2. Hover you cursor over **Scan** or **DoS** bar, a balloon will show up to indicate number of **Scan** and **DoS** attacks.



Viewing ABD logs

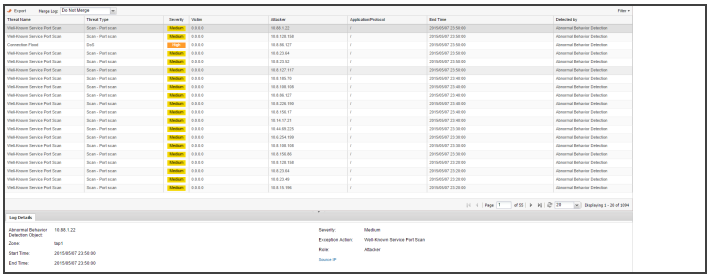
1. Select **Monitor > Log > Threat**, and click **Filter** on the top right corner.

- **Detected by:** Abnormal Behavior Detection



Step 6: Enabling Abnormal Behavior Detection and viewing abnormal behaviors

2. Click Query, ABD logs will show.



To know more about ABD, you may refer to another case in cookbook "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 390.

DNS Proxy

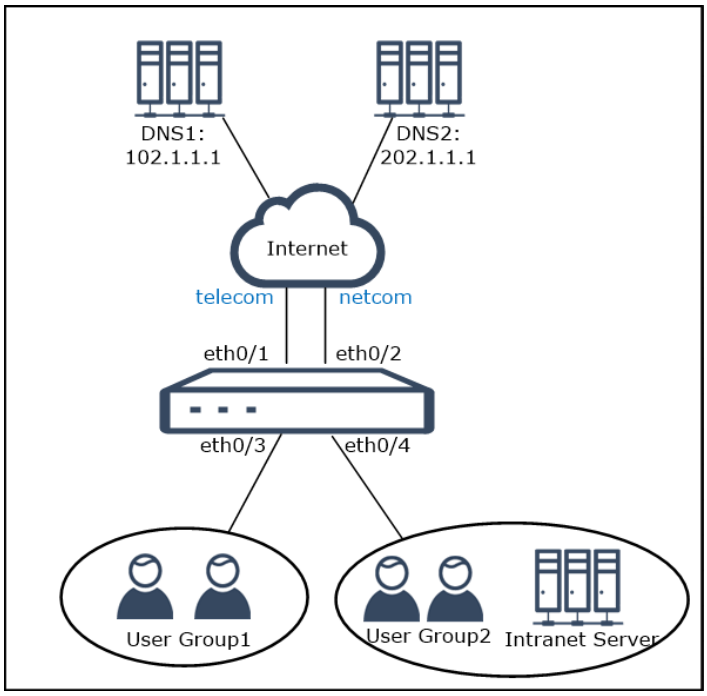
This example shows how to configure the DNS proxy function. By configuring flexible DNS proxy rules, users from different segments are assigned to different DNS servers for domain name resolution.

Scenario

A secondary ISP rents the bandwidth of telecom, netcom and other ISP to different users for Internet access. The telecom and netcom ISP have their own DNS servers. So the secondary ISP want to assign users of different network segments to the DNS servers of corresponding ISP for domain name resolution through DNS proxy devices.

This example simulates the export scenario of the above secondary ISP through the following configuration. Use eth0/1 (IP:101.0.0.1) of the device to connect to the telecom special line to access the Internet, and use eth0/2 (IP: 201.1.1.1) to connect to the netcom special line to access the Internet. In the public network, the DNS server of telecom is DNS1:102.1.1.1, and that of netcom is DNS2:202.1.1.1. Also, eth0/3, eth0/4 connect to the Intranet user groups. The administrator now has the following requirements:

1. The DNS request of user group 1 (network segment: 192.168.10.1 / 28) is uniformly proxy to dns1 for domain name resolution;
2. The DNS request of user group 2 (network segment: 172.168.10.1 / 24) is uniformly proxy to dns2 for domain name resolution;
3. The DNS request of intranet server (172.168.10.88) is not restricted and bypassed directly.



Preparation

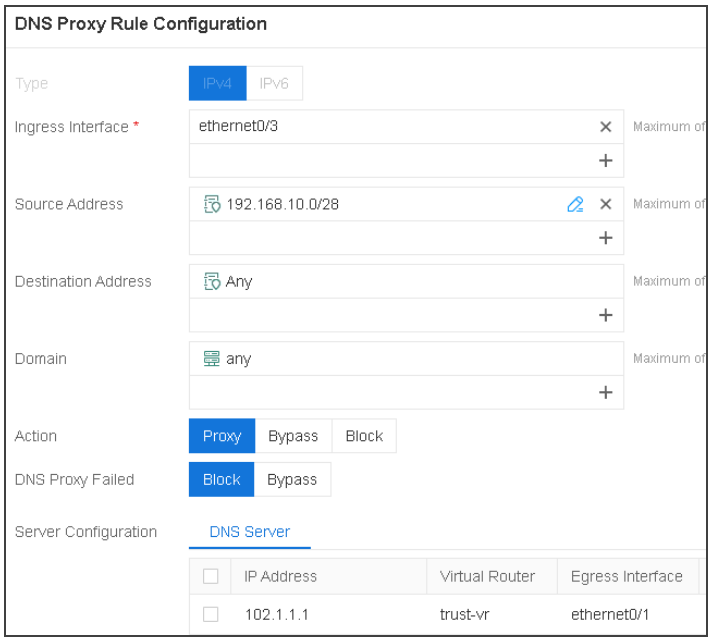
The basic interface and route configuration have been completed, and users can access the Internet normally.

Configuration Steps

Step 1： Configure a DNS proxy rules to proxy DNS requests of user group 1 to DNS1 for domain name resolution;

Login WebUI and select **Network > DNS >DNS Proxy**, and click **New**.

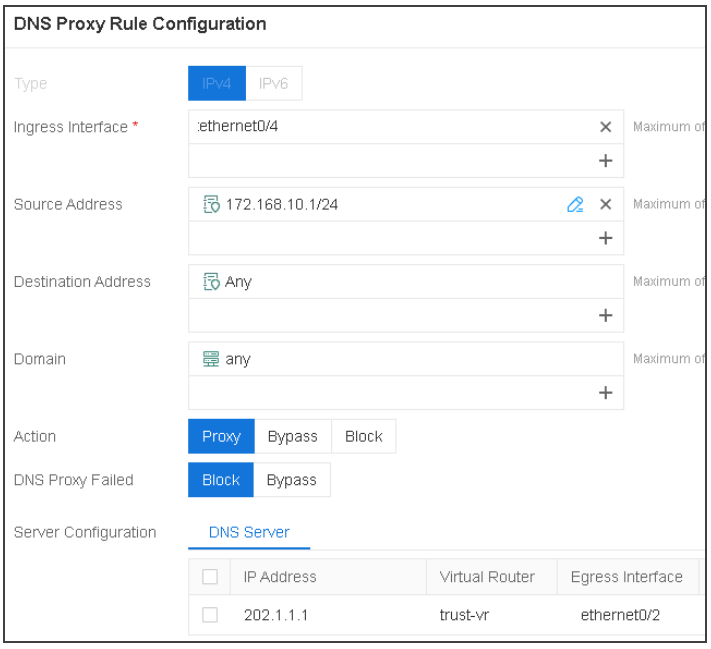
- Ingress Interface: ethernet0/3;
- Source Address: Configure a new address book 192.168.10.1/28
- Destination Address: Any
- Domain: any
- Action: Proxy
- DNS Proxy Failed: Block
- DNS Server：
  - IP Address: 102.1.1.1
  - Virtual Router: trust-vr
  - Egress Interface： etherent0/1



Step 2: Configure another DNS proxy rule to uniformly proxy DNS requests of user group 2 to DNS2 for domain name resolution.

Continue to configure another rule. Select **Network > DNS >DNS Proxy**, and click **New**.

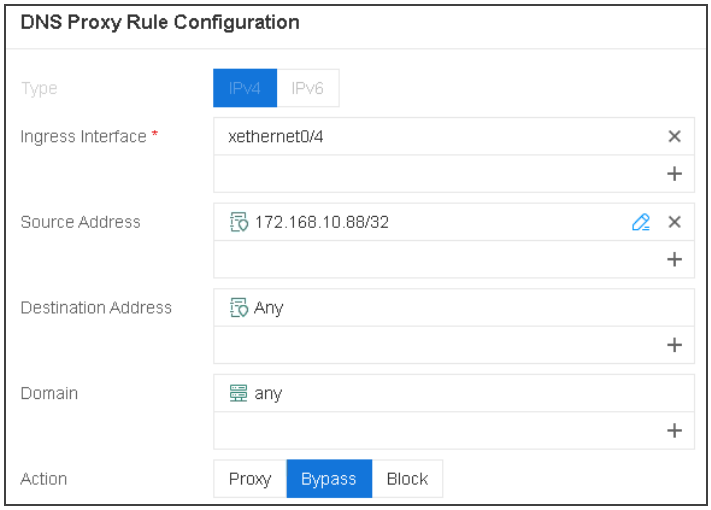
- Ingress Interface: ethernet0/4;
- Source Address: Configure a new address book 172.168.10.1/24
- Destination Address: Any
- Domain: any
- Action: Proxy
- DNS Proxy Failed: Block
- DNS Server：
  - IP Address: 202.1.1.1
  - Virtual Router: trust-vr
  - Egress Interface： etherent0/2



Step 3: Configure one more DNS proxy rule to release DNS requests from the Intranet server (172.168.10.88) directly.

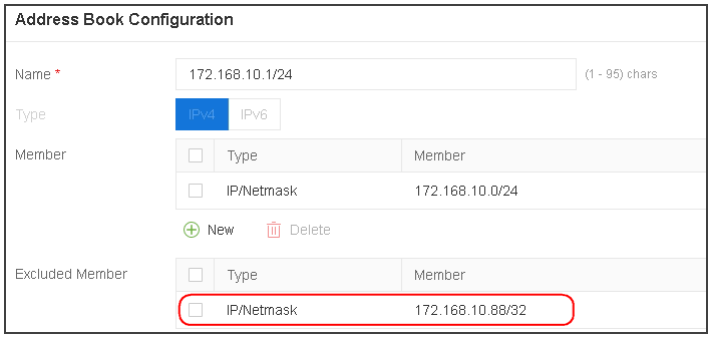
Continue to configure one more rule. Select **Network > DNS >DNS Proxy**, and click **New**.

- Ingress Interface: ethernet0/4;
- Source Address: Configure a new address book 172.168.10.88/32
- Destination Address: Any
- Domain: any
- Action: Bypass



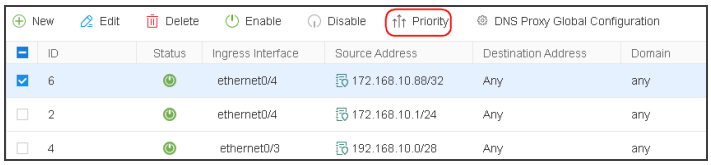
(Optional) In addition to creating a new address rule, the following methods can also be used to bypass the DNS requests from intranet servers. Select **Object > Address Book**,and select the "172.168.10.1/24" item, and click **Edit** to add the IP address of intranet server to the **Exclude Member**.

- Exclude Member: 172.168.10.88



Step 4: Adjust the priority of DNS proxy rules.

After the above steps, you will get three DNS proxy rules. Because the DNS proxy rules match from top to bottom, so the DNS rules for releasing the Intranet server should be placed on top of the other two. When configuring, select the corresponding rule item and click **Priority**to adjust.



Step 5: Results

After configuration, capture packets on eth0 / 1 and eth0 / 2 interfaces. The results are as follows:

- The users of 192.168.10.1/28 network segment in user group 1 can still access the Internet normally, and their DNS requests will be sent to the DNS1 server of Telecom for domain name resolution through the device.
- The uesrs of 172.168.10.1/24 network segment in user group 2 can still access the Internet normally, and DNS requests will be sent to the DNS2 server of Netcom for domain name resolution.
- The DNS request of the internal server 172.168.10.88 will not be proxy through the device, but will be resolved according to the DNS server set by itself.

Q&A

- Q: What is the order and manner of matching multiple DNS proxy rules?

  A: The device will query for DNS proxy rules by turns from up to down. In each rule, only if all matching conditions are met can the matching be successful.

- Q: When multiple DNS servers are configured in a DNS proxy rule, what is the priority of preferred and bound out interface properties?

  A: 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.

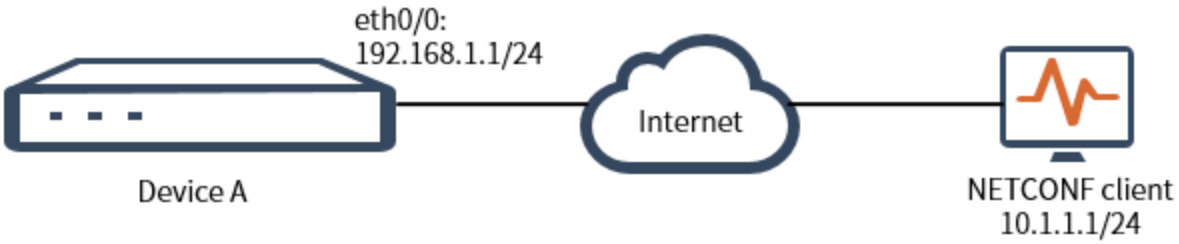
- Q: Can DNS proxy for specific domain names?

  A: Yes, you can configure a specific domain name in the option "**Domain Name**", and then configure the proxy action and the corresponding DNS server when creating a new rule.

Adding an SNAT Rule to StoneOS through 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. This example shows how to add an SNAT rule to the device through the NETCONF client.

The topology is shown as below. Device A connects to the NETCONF client. It is required to add an SNAT rule to device A using NETCONF.



Preparation

Before configuring the NETCONF function, prepare the following first:

1. The NETCONF client software has been correctly installed on the client PC, and the client environment has been configured. This case takes the client software *netopeer2-cli* as an example.
2. Device A is connected to the NETCONF client, and messages can be sent between them.

Configuration Steps

Device A

Step 1: Configuring the management method of the interface as NETCONF.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# manage netconf
hostname(config-if-eth0/0)# exit
hostname(config)#
```

Step 2: Configuring the access of the administrator as NETCONF (Take the administrator hillstone as an example).

```
hostname(config)# admin user hillstone
hostname(config-admin)# access netconf
hostname(config-admin)# exit
hostname(config)#
```

Step 3: Configuring the login type of the trusted host as NETCONF.

```
hostname(config)# admin host any netconf
hostname(config)#
```

Step 4: Enabling the NETCONF agent and the NETCONF candidate functions.

```
hostname(config)# netconf-manager enable
hostname(config)# netconf-manager candidate
hostname(config)#
```

NETCONF Client

Step 1: Connecting to the Device.

Running the client software *netopeer2-cli* in Linux and connecting to the device:

[root@linux1~]# netopeer2-cli

> connect --ssh --host 192.168.1.1 --port 830 --login hillstone

hillstone@192.168.1.1 password:

cmd_connect: Already connected to 192.168.1.1.

In the above command:

- --host: specifies the IP address of the device.
- --login: specifies the login user name which must be the same as the device administrator name.

After the above command is executed, a prompt for password will appear. Enter the password of the administrator hillstone and press Enter.

Step 2: Getting the Yang model of the device.

> get-schema --model configuration

Executing the above command to get the Yang model of the device.

Step 3: Editing the XML file which will be used to add an SNAT rule to the device.

Editing the XML file according to the Yang model obtained in step 2 and saving it as snat.xml. The contents of the XML file are as follows:

```
-<vr xmlns="https://hillstone.com/yang/SG6000-K-2-5.5R9-v6-r1208/hc" >
<!--The namespace "https://hillstone.com/yang/SG6000-K-2-5.5R9-v6-r1208/hc" in the XML file must be consistent with the namespace of the device Yang model-->
  -<vrouter>
    <vr_name>trust-vr</vr_name>
    -<snat_rule>
      <rule_id>1</rule_id>
      <group_id>0</group_id>
      <from>192.168.2.2</from>
      <from_is_ip>1</from_is_ip>
      <to>Any</to>
      <to_is_ip>0</to_is_ip>
      <service>Any</service>
      <trans_to>192.168.1.10</trans_to>
      <trans_to_is_ip>1</trans_to_is_ip>
      <flag>1</flag>
      <log>0</log>
      <enable>0</enable>
      <trans_type>1</trans_type>
    </snat_rule>
  </vrouter>
</vr>
```

Step 4: Adding the SNAT rule to the device.

> edit-config --target running --config=snat.xml

In the above command:

- --target: "running" means that the distributed configuration will immediately change the running configuration of the device, which will have an impact on the current business. If you select the parameter "candidate", the distributed configuration will remain in the configuration repository and will not have any impact on the current business. If you want to use the candidate configuration to replace the running configuration of the device, you can first execute the "validate-- source candidate" command to check whether the candidate configuration is valid, and then execute the "commit" command.
- --config: specifies the path and file name of the xml file. If you do not specify this parameter, the system automatically opens an empty XML file after the command is executed, and you can edit the content in this empty document.

Viewing the results

After configuring the above steps, you can see that the SNAT rule has been added to the device using the Show command.

```
hostname(config)# show configuration vrouter trust-vr
ip vrouter "trust-vr"
snatrule id 1 from ip 192.168.2.2 to address-book "Any" service "Any" trans-to ip 192.168.1.10 mode static disable
exit
hostname(config)#
```

Binding the Log Processing Process and Database Storage Process to Core MAX

This example introduces how to bind the log processing process and database storage process to Core MAX. 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. The example including the following two scenarios:

- Scenario 1: A Hillstone security device is deployed on an enterprise network. Operation and maintenance personnel periodically check the session logs and NAT logs stored in the database. 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.
- Scenario 2: A Hillstone security device is deployed on an enterprise network. Operation and maintenance personnel need to periodically check traffic and session monitoring statistics. The device supports the storage of statistics on device traffic and sessions over the last 180 days to the device disk. The system's database storage process (MYSQLD) work on Core0 of the CPU. Core0 can be overloaded with a large amount of high speed traffic and session data storage operations, potentially affecting the normal operation of other functional modules.

Based on the above scenarios, 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.

Configuration Roadmap

1. Use the command **`flow-core-num`** *`number`* 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.
2. Bind the log processing process and database storage process to Core MAX.
3. Restart the device to make the configurations in Step 1 and Step 2 take effect.
4. For scenario 1, you can increase the the speed at which logs are sent to the log processing process.

Before binding the log processing process and database storage process to Core MAX, prepare the following first:

1. The NETCONF client software has been correctly installed on the client PC, and the client environment has been configured. This case takes the client software *netopeer2-cli* as an example.
2. Device A is connected to the NETCONF client, and messages can be sent between them.

- **Scenario 1**: The session logs and NAT logs have been stored in the device disk with the command.
- **Scenario 2**: The device has enabled the Long-term Monitor function for traffic and sessions.
- 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. SG-6000-A3000 with a hard disk is used as an example to describe the configuration.

Configuration Steps

Step 1: Specifying the number of CPU cores occupied by the system data.

```
hostname(config)# flow-core-num 3
hostname(config)# exit
```

Step 2: Binding the log processing process and database storage process to Core MAX, and restarting the for the above configuration to take effect.

```
hostname(config)# cp-multi-cores logd
hostname(config)# exit
hostname# reboot
System reboot, are you sure? [y]/n: y
```

Step 3: For scenario 1, adjusting the speed at which logs are sent to log processing process. The default sending speed of SG-6000-A3000 is 2000 logs per second.

```
hostname(config)# logging speed-limit to local 3000
hostname(config)# show logging speed-limit
Log speed limit:3000
```

Viewing the results

After configuring the above steps, you can see that the CPU utilization of Core 0 is decreasing and that of Core MAX is increasing by using the command **show cpu detail**.

```
hostname(config)# show cpu detail
```

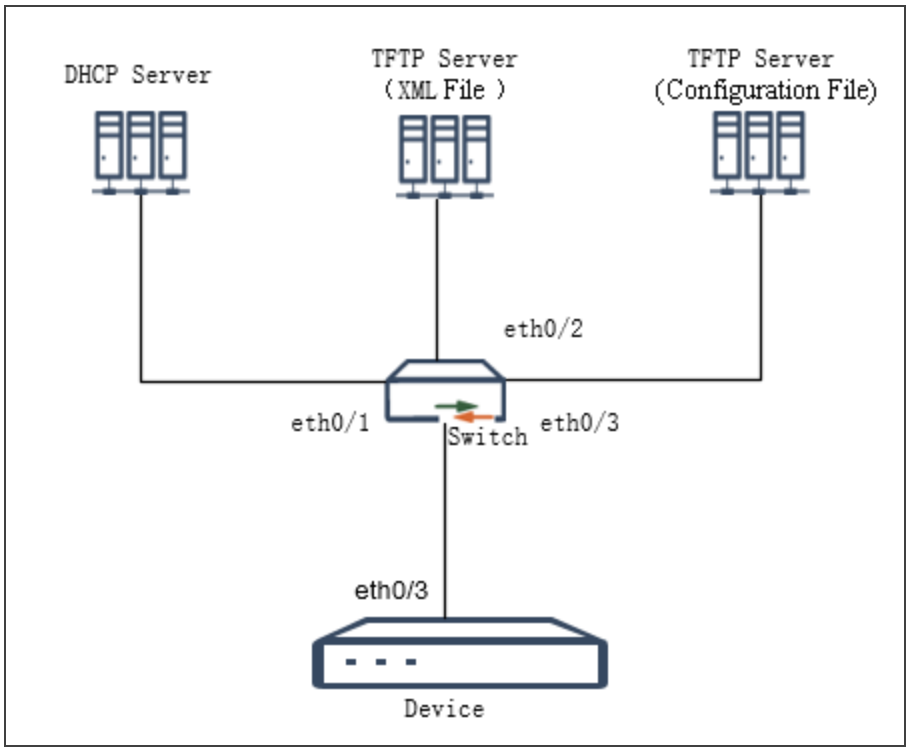
DHCP ZTP

This example introduces the DHCP zero touch provisioning (ZTP) process. As the DHCP client, the Hillstone security device automatically obtains a specified configuration file via DHCP and uses it as the startup configuration of the device, achieving ZTP of the device, thus enhancing deployment efficiency.

Networking Scenario

An enterprise purchases a batch of Hillstone A-series security devices and needs to deploy them in various regions. However, the O&M personnel cannot go to each location personally to make the new device come online. Therefore, they require devices that support ZTP. In addition, due to security protection requirements, the use of USB ports to achieve USB ZTP is not allowed. In this case, the plan is to use the Hillstone security device as the DHCP client to achieve DHCP ZTP.

The networking diagram is shown as follows.



Preparations

Before you configure the DHCP service for ZTP setup, prepare the following first:

- The DHCP client, DHCP server, TFTP server have been networked based on the actual scenario.
- The DHCP server has been configured with the address of the TFTP server where the XML file is located and with the path to the XML file, corresponding to the Option 66 and Option 67 fields in the DHCP message respectively.
- DHCP ZTP is supported only by A-series devices and certain K-series devices from the factory or with empty configuration (only system default configuration, no custom configuration). The ethernet0/3 interface of the device automatically obtains an address via the DHCP protocol by factory default. Please use the ethernet0/3 interface for DHCP ZTP.
- The servers where the XML file and the configuration file are located need to be TFTP servers, and they can be the same TFTP server.
- The configuration file on the TFTP server needs to be named after the device SN number with a .cfg suffix.

Procedure

Step 1: The StoneOS system determines whether the device is from the factory or is with empty configuration.

After the device from the factory or with empty configuration is powered on and started, it will automatically enter the DHCP ZTP procedure.

Step 2: Obtain DHCP information.

The device sends a request message to the DHCP server, and the DHCP server returns a response message to the device. The device obtains the DHCP client address, default gateway and other information by parsing the response message.

Step 3: Parse the response message and download the XML file.

The device parses the response message from the DHCP server to obtain the address of the TFTP server where the XML file is located and the path to download the XML file, and then downloads the XML file from the corresponding TFTP server.

Step 4: Parse the XML file and download the configuration file.

The device parses the downloaded XML file, obtains the address of the TFTP server where the configuration file is located and the path to download the configuration file, and then downloads the configuration file named with the device SN number, such as "5931844225000750.cfg", from the corresponding TFTP server.

Step 5: Restart the device automatically.

After the configuration file is downloaded, the system will use it as the startup configuration file when the device starts, and the configuration file will be loaded when the device restarts automatically, and the initiation can be completed after the restart is finished. If you log into the device successfully, the initiation is successful.

[Optional] Step 6: Compare whether the configuration files in the device and on the TFTP server are consistent.

Due to the skipping of loading for incorrectly formatted configurations during the configuration file loading process, the initialization may be successful but some services fail to start. You can run the **save** command to save the current running configuration to the startup configuration file. Then, export the startup file from the device and compare it with the configuration file on the TFTP server to verify consistency. Any inconsistencies can be manually adjusted on the device by adding or modifying configurations, which is intended for subsequent initialization tasks on new devices.

Routing

This chapter introduces different routing configuration use cases.

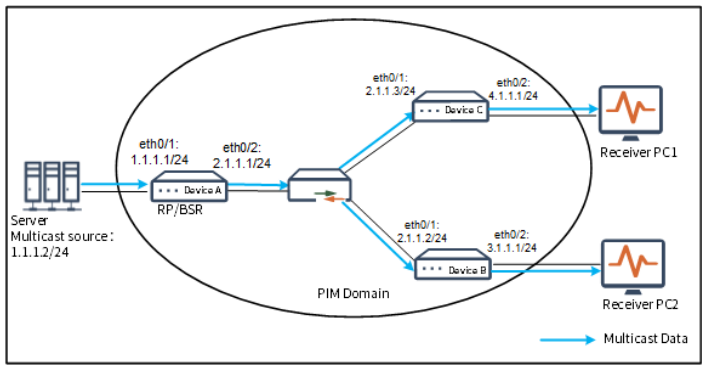
This chapter contains the following recipes:

- "Realizing Multicast Forwarding Through PIM-SM Multicast Protocol" on Page 75
- "Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol" on Page 84

Realizing Multicast Forwarding Through PIM-SM Multicast Protocol

This example introduces how to configure the basic functions of PIM-SM to realize multicast forwarding so that users can receive data from any multicast source.

In the topology below, the multicast source sends data to the multicast group, and the multicast address is 225.0.0.1. The receivers PC1 and PC2 send IGMPv2 Report to join the multicast group, and the PIM domain adopts the PIM-SM mode. Assume that Device A is the candidate RP and candidate BSR, the interface loopback1 is the interface for electing the RP, and the interface eth0/1 is the multicast data inbound interface. By configuring the PIM-SM function on each device in the PIM domain, multicast data can be forwarded to the recipient PC in a normal multicast manner.



Configuration Steps

Step 1: Configure the IP address and unicast routing protocol of each device interface (OSPF is used in this example).

Device A :

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# network 1.1.1.0/24 area 0
hostname(config-router)# network 2.1.1.0/24 area 0
```

Device B :

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)# **exit**

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/1)# **zone trust**

hostname(config-if-eth0/1)# **ip address 3.1.1.2/24**

hostname(config-if-eth0/1)# **exit**

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **router ospf**

hostname(config-router)# **router-id 2.2.2.2**

hostname(config-router)# **network 2.1.1.0/24 area 0**

hostname(config-router)# **network 3.1.1.0/24 area 0**

Device C:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.3/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 4.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 3.3.3.3
hostname(config-router)# network 2.1.1.0/24 area 0
hostname(config-router)# network 4.1.1.0/24 area 0
```

Step 2: Enable a multicast route.

Device A:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

Device B:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Device C:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Step 3: Enable and configure PIM-SM.

Device A:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Device B:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter))# router pim
hostname(config-vrouter)# pim-sm enable
hostname(config-vrouter))# exit
hostname(config)#interface ethernet0/1
hostname(config-if-eth0/1)# ip pim sparse-mode
hostname(config-if-eth0/1)# exit
hostname(config)#interface ethernet0/2
hostname(config-if-eth0/2)# ip pim sparse-mode
```

Device C:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter))# router pim
hostname(config-vrouter)# pim-sm enable
hostname(config-vrouter))# exit
hostname(config)#interface ethernet0/1
hostname(config-if-eth0/1)# ip pim sparse-mode
hostname(config-if-eth0/1)# exit
hostname(config)#interface ethernet0/2
hostname(config-if-eth0/2)# ip pim sparse-mode
```

Step 4: Configure RP and Candidate BSR.

Device A :

```
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)# ip vrouter trust-vr
hostname(config-vrouter)# rp-candidate loopback1
hostname(config-vrouter)# bsr-candidate loopback1
hostname(config-vrouter))# exit
hostname(config)#
```

Step 5: Verify result.

Device A :

hostname(config)# **show ip mroute**

U:interface up D:interface down

V:valid multicast entry I:invalid multicast entry Y:sync multicast entry

==========-

==========

source: 1.1.1.2 group : 225.0.0.1 vrouter: trust-vr

status: V update time: -

ingress interface: ethernet0/1(U)

egress interface : ethernet0/2(U)

==========-

==========

hostname(config)# **show ip pim rp**

PIM Rendezvous Point for Virtual Router <trust-vr>

==========-

==========

Group: 225.0.0.1, RP:2.2.2.2, v2, via bootstrap, priority 0 holdtime 35.

==========-

==========

hostname(config)# **show ip pim bsr-router**

PIM Bootstrap Router for Virtual Router <trust-vr>

==========-

==========

PIMv2 Bootstrap information

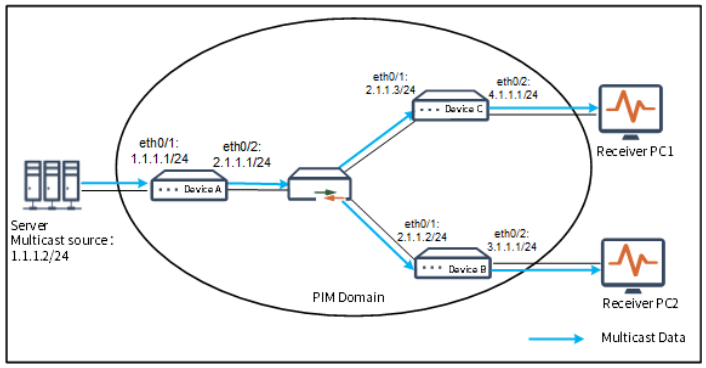
BSR address: 2.2.2.2

```
BSR Priority: 0
=============================================================-
======================
```

Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol

This example introduces how to configure the basic functions of PIM-SSM to realize multicast forwarding so that users can receive data from any multicast source.

In the topology below, the multicast source sends data to the multicast group, and the multicast address is 232.0.0.1. Receivers PC1 and PC2 send IGMPv3 Report to join the multicast group. The PIM domain adopts the PIM-SSM mode. The relationship between the host and the devices in the PIM domain is maintained through IGMPv3, so that the members of the multicast group can quickly join, directly at the multicast source SPT (Shortest Path Tree) is established with the recipient PC. Assume that the interface eth0/1 of Device A is used as the inbound interface for multicast data. By configuring the PIM-SSM function on each device in the PIM domain, multicast data can be multicast forwarded to the recipient PC normally.



Configuration Steps

Step 1: Configure the IP address and unicast routing protocol of each device interface (OSPF is used in this example).

Device A :

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 1.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.2/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 1.1.1.1
hostname(config-router)# network 1.1.1.0/24 area 0
hostname(config-router)# network 2.1.1.0/24 area 0
```

Device B :

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)# **exit**

hostname(config)# **interface ethernet0/2**

hostname(config-if-eth0/1)# **zone trust**

hostname(config-if-eth0/1)# **ip address 3.1.1.2/24**

hostname(config-if-eth0/1)# **exit**

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **router ospf**

hostname(config-router)# **router-id 2.2.2.2**

hostname(config-router)# **network 2.1.1.0/24 area 0**

hostname(config-router)# **network 3.1.1.0/24 area 0**

Device C:

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 2.1.1.3/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 4.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# router-id 3.3.3.3
hostname(config-router)# network 2.1.1.0/24 area 0
hostname(config-router)# network 4.1.1.0/24 area 0
```

Step 2: Enable a multicast route.

Device A:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

Device B:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Device C:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter)# **ip multicast-routing**

hostname(config-vrouter)# **exit**

hostname(config)#

Step 3: Configure PIM-SSM.

Device A:

hostname(config)# **ip vrouter trust-vr**

hostname(config-vrouter))# **router pim**

hostname(config-vrouter)# **pim-sm enable**

hostname(config-vrouter)# **pim-ssm default**

hostname(config-vrouter))# **exit**

hostname(config)#**interface ethernet0/1**

hostname(config-if-eth0/1)# **ip pim sparse-mode**

hostname(config-if-eth0/1)# **exit**

hostname(config)#**interface ethernet0/2**

hostname(config-if-eth0/2)# **ip pim sparse-mode**

Device B:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter))# router pim
hostname(config-vrouter)# pim-sm enable
hostname(config-vrouter)# pim-ssm default
hostname(config-vrouter))# exit
hostname(config)#interface ethernet0/1
hostname(config-if-eth0/1)# ip pim sparse-mode
hostname(config-if-eth0/1)# exit
hostname(config)#interface ethernet0/2
hostname(config-if-eth0/2)# ip pim sparse-mode
```

Device C:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter))# router pim
hostname(config-vrouter)# pim-sm enable
hostname(config-vrouter)# pim-ssm default
hostname(config-vrouter))# exit
hostname(config)#interface ethernet0/1
hostname(config-if-eth0/1)# ip pim sparse-mode
hostname(config-if-eth0/1)# exit
hostname(config)#interface ethernet0/2
hostname(config-if-eth0/2)# ip pim sparse-mode
```

Step 4: Verify result.

Device A :

hostname(config)# **show ip mroute**

U:interface up D:interface down

V:valid multicast entry I:invalid multicast entry Y:sync multicast entry

==========-

==========

source: 1.1.1.2 group : 232.0.0.1 vrouter: trust-vr

status: V update time: -

ingress interface: ethernet0/1(U)

egress interface : ethernet0/2(U)

==========-

==========

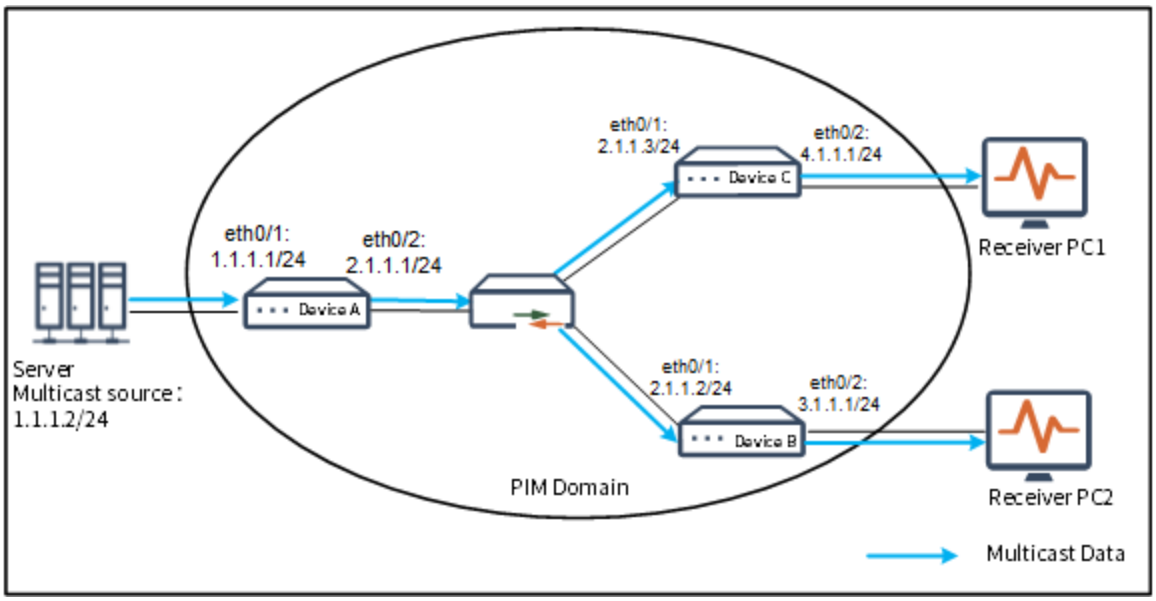
Deploying HA Scenario for Multicast Forwarding Through PIM-SM

This example introduces how to deploy the HA AP (Active-Passive) mode in the pim-ssm multicast environment to ensure that each router device in the PIM domain can transmit multicast data with high reliability.

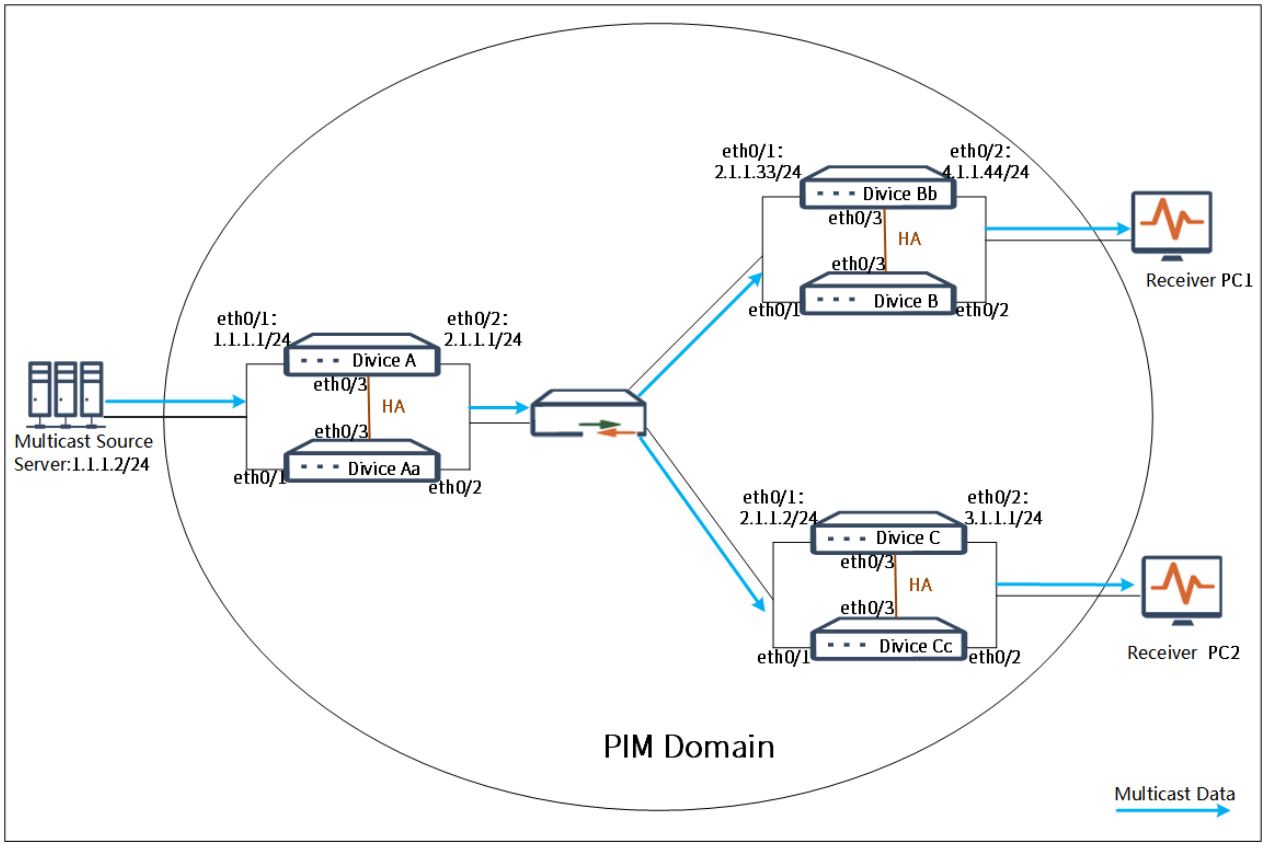
In the initial network as topology below, the multicast source sends data to the multicast group, and the multicast address is 232.0.0.1. Receivers PC1 and PC2 send IGMPv3 Report to join the multicast group. The PIM domain adopts the PIM-SSM mode. The relationship between the host and the devices in the PIM domain is maintained through IGMPv3, so that the members of the multicast group can quickly join, directly at the multicast source SPT (Shortest Path Tree) is established with the recipient PC. Assume that the interface eth0/1 of Device A is used as the inbound interface for multicast data. By configuring the PIM-SSM function on each device in the PIM domain, multicast data can be multicast forwarded to the recipient PC normally. For details, see Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol .

In this example, Device A , Device B and Device C in the PIM domain are deployed in HA AP mode. After deployment, Device A , Device B and Device C are elected as as the master devices, and Device Aa , Device Bb and Device Cc are elected as backup devices. Meanwhile, the multicast route generated in the master device Device A(Device B or Device C) will be quickly synchronized to the backup device with a temporary status of Y; When the master device Device A (Device B or Device C) fails or cannot forward traffic normally, the backup device Device Aa (Device Bb or Device Cc) will switch as the master device. At this time, the multicast route in Y state will be based on to forward multicast traffic without affecting the original normal communication. AfterDevice Aa receives the IGMPv3 report messages, The status in the multicast routing table will be updated to the normal status V.

Original Multicast Network :



Multicast Network after HA-AP Deployment:



Configuration Steps

Step 1: Configure the PIM-SSM multicast protocol according to the example Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol .

Step 2: Configure the Device A and Device Aa as HA AP mode and HA negotiate successfully.

```
Device A

hostname(config)# track track1

hostname(config-trackip)# interface ethernet0/1 weight
255////Monitor the status of interface eth0/1 and eth0/2.

hostname(config-trackip)# interface ethernet0/2 weight 255

hostname(config-trackip)# exit

hostname(config)# ha group 0

hostname(config-ha-group)# priority 50

hostname(config-ha-group)# monitor track track1

hostname(config-ha-group)# exit

hostname(config)# ha link interface ethernet0/3

hostname(config)# ha link ip 100.1.1.1/24

hostname(config)# ha cluster 1
```

```
Device Aa

hostname(config)# ha group 0

hostname(config-ha-group)# priority 100

hostname(config-ha-group)# exit

hostname(config)#

hostname(config)# ha link interface ethernet0/3

hostname(config)# ha link ip 100.1.1.2/24

hostname(config)# ha cluster 1
```

Step 3: Configure management IP addresses for the two devices and monitor objects on the standby Device after HA negotiation between Device A and Device Aa is successful .

```
Device A:

hostname(config)# interface ethernet0/1

hostname(config-if-eth0/1)# zone trust

hostname(config-if-eth0/1)# manage ip 1.1.1.253

Device Aa:

hostname(config)# interface ethernet0/1

hostname(config-if-eth0/1)# zone trust

hostname(config-if-eth0/1)# manage ip 1.1.1.254

hostname(config-if-eth0/1)# exit

hostname(config)# ha group 0

hostname(config-ha-group)# monitor track track1

hostname(config-ha-group)# exit

hostname(config)#
```

Step 4: Results

1. Configurations related to multicast have been synchronized on the standby device.

```
 Device Aa
hostname(B)#show configuration vrouter
ip vrouter "mgt-vr"
exit
ip vrouter "trust-vr"
ip multicast-routing
router-id 1.1.1.1
network 1.1.1.0/24 area 0
network 2.1.1.0/24 area 0
exit
router pim
pim-sm enable
pim-ssm default
exit
exit
```

2. The stutas of multicast routing table is V. On the back device, the multicast routing table is synchronized and its status is Y.

```
Device A:
hostname(M)# show ip mroute
U:interface up D:interface down
V:valid multicast entry I:invalid multicast entry Y:sync mul-
ticast entry
=================================================================-
==============
source: 1.1.1.2 group : 232.0.0.1 vrouter: trust-vr
status: V update time: -
ingress interface: ethernet0/1(U)
egress interface : ethernet0/2(U)
=================================================================-
==============
Device Aa:
hostname(B)# show ip mroute
U:interface up D:interface down
V:valid multicast entry I:invalid multicast entry Y:sync mul-
ticast entry
=================================================================-
==============
source: 1.1.1.2 group : 232.0.0.1 vrouter: trust-vr
status: Y update time: -
ingress interface: ethernet0/1(U)
egress interface : ethernet0/2(U)
=================================================================-
```

```
==============
```

3.Restart Device A (or change eth0 / 1 and eth0 / 2 of Device A to shutdown). At this time, the backup device Device Aa will quickly switch to the master device, and the multicast route in Y state can forward multicast traffic without affecting the original communication; After Device Aa receives the IGMPv3 report message, the status in the multicast routing table will be updated to V, and the multicast traffic will continue to be forwarded later. The status is shown as follows:

```
 Device Aa:
hostname(M)# show ip mroute
U:interface up D:interface down
V:valid multicast entry I:invalid multicast entry Y:sync mul-
ticast entry
================================================================-
==============
source: 1.1.1.2 group : 232.0.0.1 vrouter: trust-vr
status: V update time: -
ingress interface: ethernet0/1(U)
egress interface : ethernet0/2(U)
================================================================-
==============
```

Step 5: You can deploy device B and device C to the HA AP mode as required according to the above steps.

Authentication

Authentication is a method of verifying visitor's identity. When a visitor is confirmed as a valid user, he is allowed to use a certain network. The visitor can be a PC, a mobile phone or a tablet.

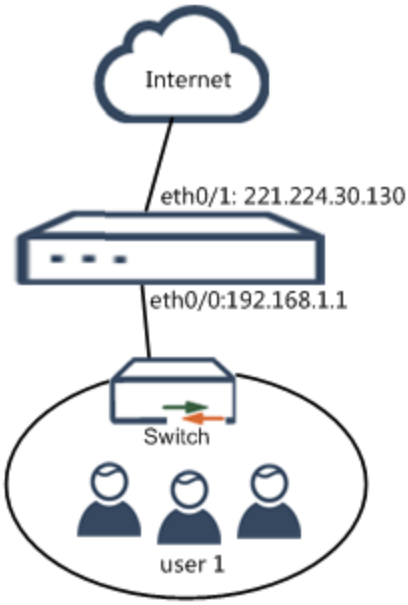
This chapter contains the following recipe:

- "Allowing the Internet Access via User Authentication" on Page 99
- " Using AD Polling for SSO" on Page 107
- " Allowing Internet Access via AD Polling" on Page 116
- " Allowing Internet Access via AD Agent" on Page 127
- " Allowing Internet Access via TS Agent" on Page 138

Allowing the Internet Access via User Authentication

This example shows how to use Web authentication (WebAuth). An AAA server is required in this example to confirm the identity of a user.

The topology describes the scenarios of the case. In this scenario, only user 1 passes the authentication, and then accesses the Internet; while other users fail to pass the authentication, and they are not allowed to access the Internet.



Configuration Steps

Step 1: Configuring the user and address book

Select **Object > User > Local User**. Under **Local Server**, click **New > User**.

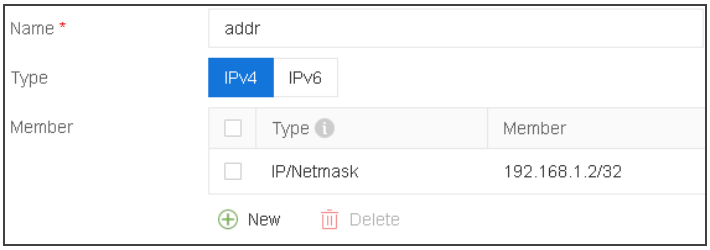


- Name: user1
- Password: 123456
- Confirm Password: 123456

Step 1: Configuring the user and address book

Select **Object > Address Book > New**.

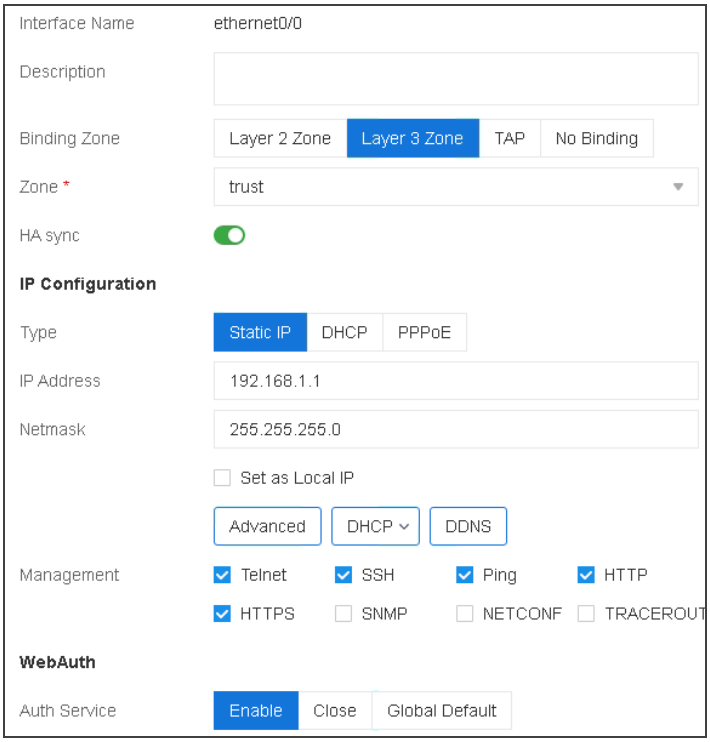
- Name: addr
- Type: IPv4
- Member: Click **New** , and select **IP/Netmask**, enter **192.168.1.2, 32**



Step 2: Configuring the interface and zone

Select **Network > Interface**, and double click **ethernet0/0**.

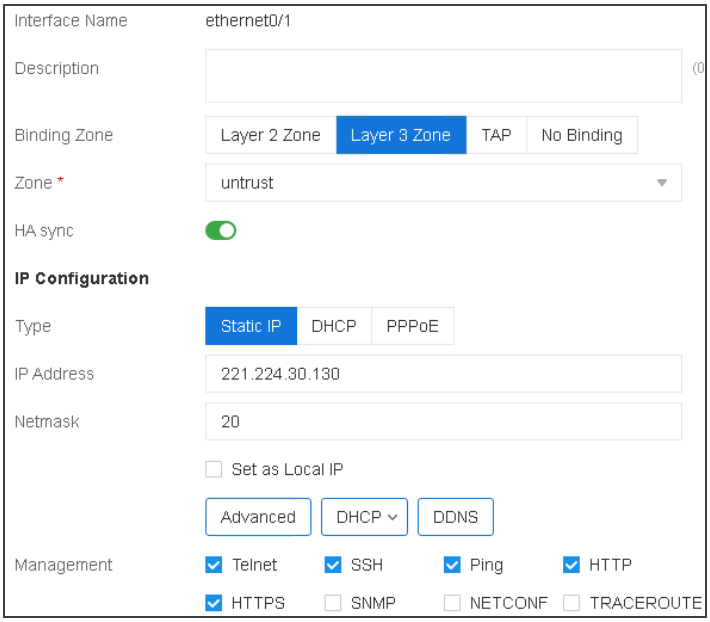
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Configuration
  - Type: Static IP
  - IP Address: 192.168.1.1
  - Netmask: 255.255.255.0
- WebAuth
  - Auth Service: Enable



Step 2: Configuring the interface and zone

Select **Network > Interface**, and double click **ethernet0/1**.

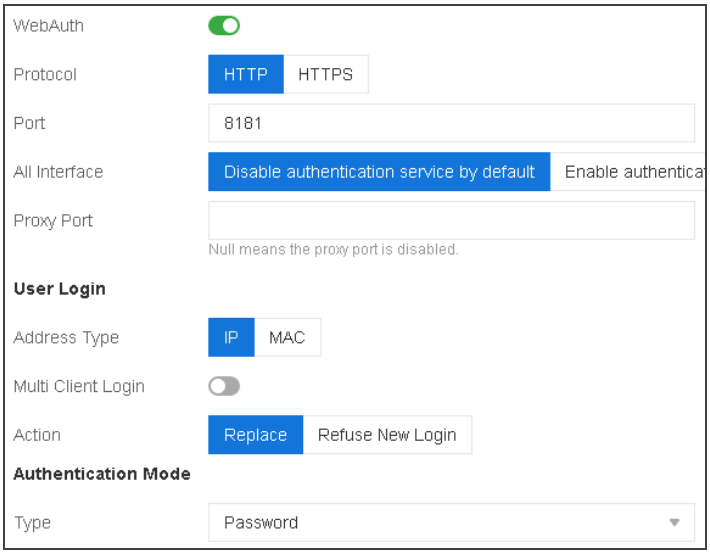
- Binding Zone: Layer 3 Zone
- Zone: untrust
- IP Configuration
  - Type: Static IP
  - IP Address: 221.224.30.130
  - Netmask: 20



Step 3: Configuring Web Authentication

Select **Network > WebAuth > WebAuth**, and configure the followings:

- WebAuth: Click the **Enable** button
- Protocol: HTTP
- Port: 8181
- Authentication Mode:
  - Type: Password



Step 3: Configuring Web Authentication

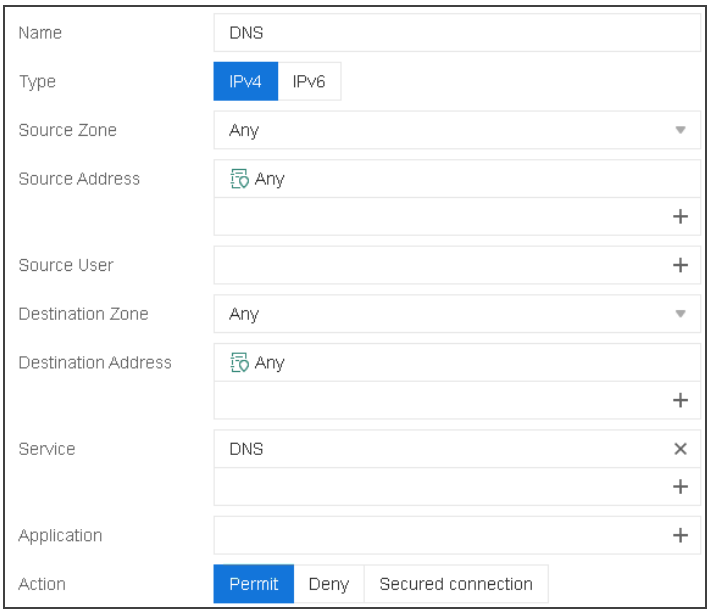
After the above configurations, continue to create policy rules in **Security Policy** to make WebAuth effective. Click **policy template** for reference.

Policy Template(Ensure DNS traffic is permitted and enable WebAuth)

Source Zone	Destination Zone	Source Address	Destination Address	User	Service	Action
Any	Any	Any	Any		DNS	Permit
Any	Any	Any	Any	unknown	Any	WebAuth

Step 4: Configuring Security Policy

Click the " policy page" quick link on the bottom of the Web authentication page or select **Policy > Security Policy > Policy**, and click **New > Policy**.

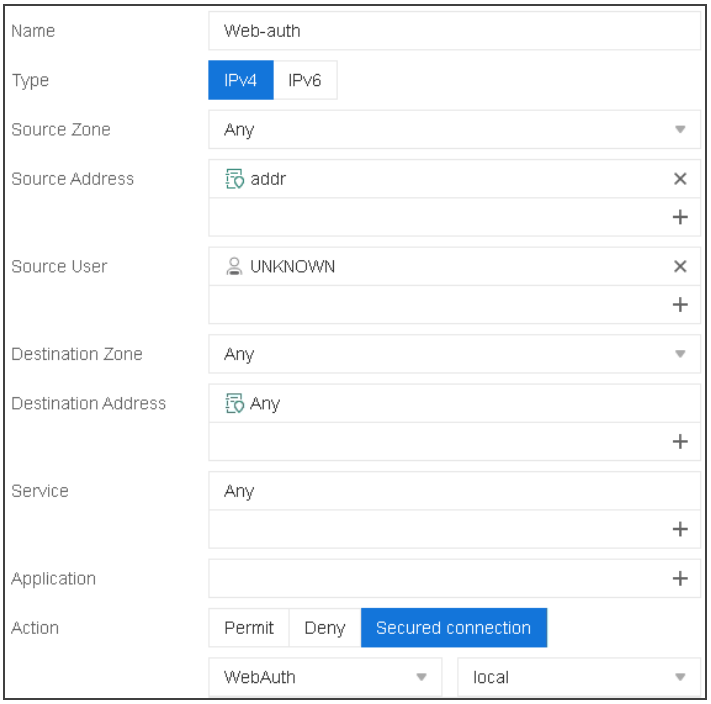


- Name: DNS
- Source Zone: Any
- Source Address: Any
- Destination Zone: Any
- Destination Address: Any
- Service: DNS
- Action: Permit

Step 4: Configuring Security Policy

Click **New**, and create the "Web-auth" policy.

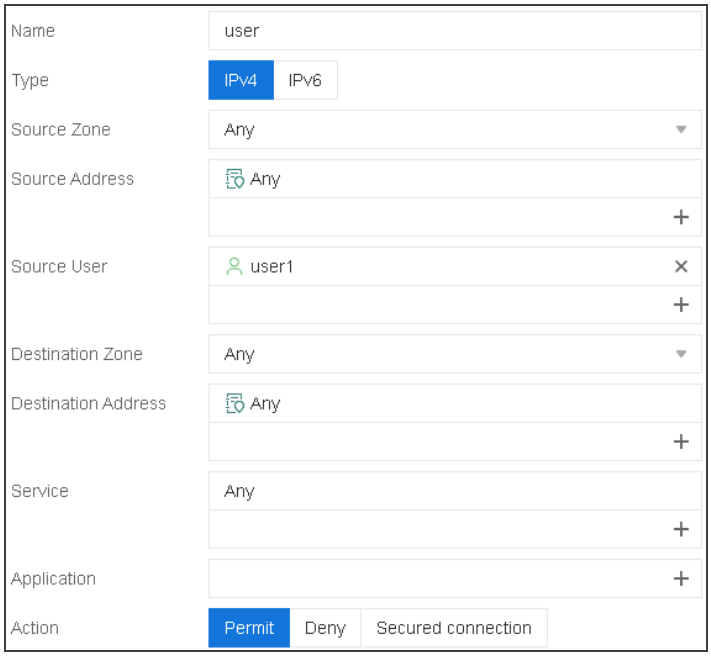
- Name: Web-auth
- Source Zone: Any
- Source Address: addr
- Source User: Click +, select "Role" from the **AAA Server/Role** drop-down list and select "UNKNOWN"
- Destination Zone: Any
- Destination Address: Any
- Action: Secured connection
  - WebAuth: local



Step 4: Configuring Security Policy

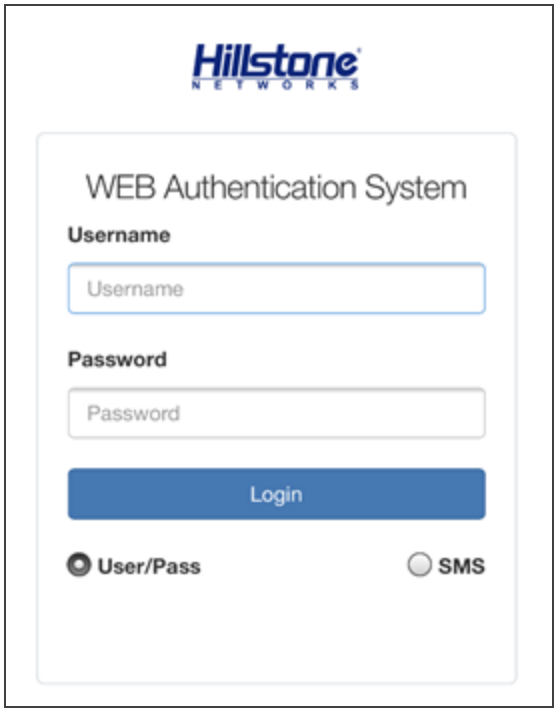
Click **New**, and create the "user" policy. Specify the source user who is allowed to access the Internet.

- Name: user
- Source Zone: Any
- Source Address: Any
- Source User: Click **+**, select "local" from the **AAA Server/Role** drop-down list and select "user1"
- Destination Zone: Any
- Destination Address: Any
- Action: Permit



Step 5: Triggering WebAuth through HTTP requests

After the above configurations, when there are HTTP requests sent from the interface 192.168.1.2/32, user1 will be prompted to authenticate by entering the username/password (user1/123456) before accessing the Internet.



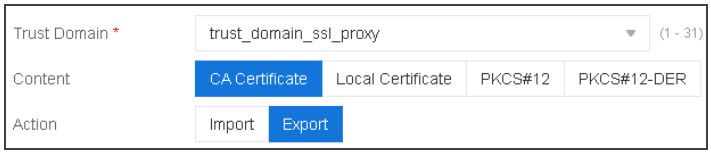
Step 6: Triggering WebAuth through HTTPS requests

Export the certificate from the device.

Select **System > PKI > Trust Domain Certificate**.

- Trust Domain: trust_domain_ssl_proxy
- Content: CA Certificate
- Action: Export

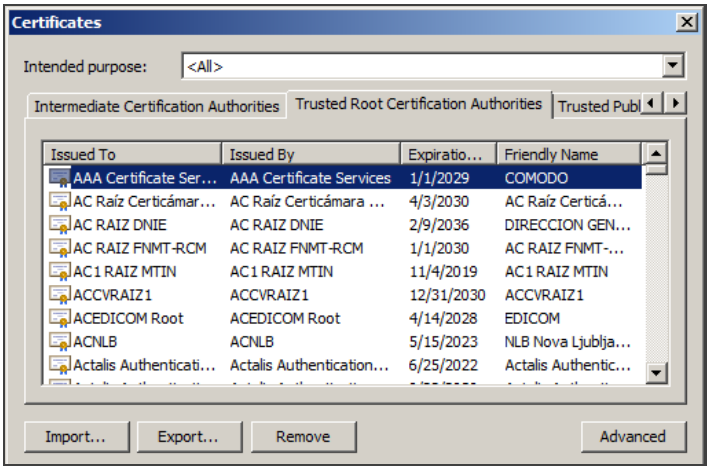
Click **OK** to export the certificate.



Step 6: Triggering WebAuth through HTTPS requests

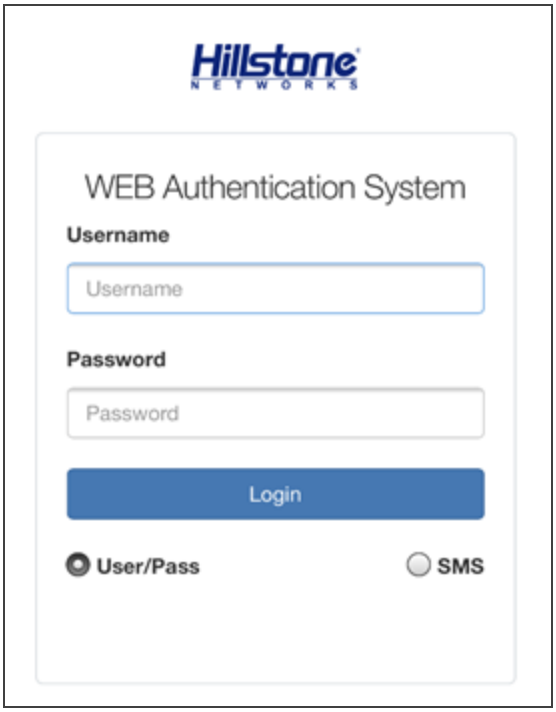
Import the certificate to client's Web browser.

1. In the Chrome Web browser, select **Settings > Show advanced settings**.
2. In the HTTPS/SSL section, select **Manage certificates**.
3. In the **Trusted Root Certification Authorities** tab, select **Import**.
4. Follow the wizard to import the certificate.



After the above configurations are finished, when there are HTTPS requests sent from the interface 192.168.1.2/32, user1 will be prompted to authenticate by entering the username/password (user1/123456) before accessing the Internet.

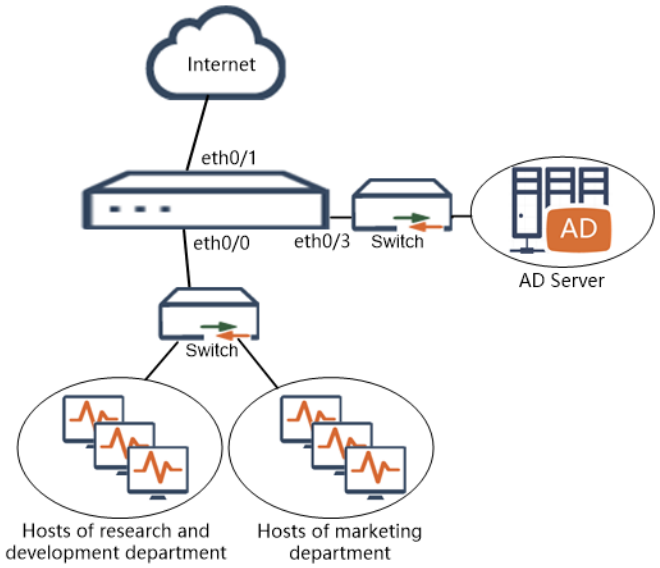
Note: Triggering WebAuth through HTTPS requests depends on the feature of SSL proxy . If the device does not support the SSL proxy. Triggering WebAuth through HTTPS requests will not work and you can then trigger WebAuth through HTTP requests.



Using AD Polling for SSO

This example introduces how the domain users access the Internet directly without Web authentication, after logging in the AD domain via configuring AD Polling.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Only the staffs in R&D department join in the AD domain (scep.pki.com), while the staffs in marketing department are excluded. The security device enables Web authentication. All the staffs of the enterprise are allowed to access the Internet only after they pass the authentication. After the AD Polling being configured, there will be login logs when staff in R&D department login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). The device can check the logs through AD Polling, as well as obtain authentication users information on the AD server. With this information, staff of R&D department can access the Internet directly without Web authentication.



Preparation

Before configuring the AD Polling function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote 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`**

- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security> Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it's necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 99.

Configuration Steps

Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

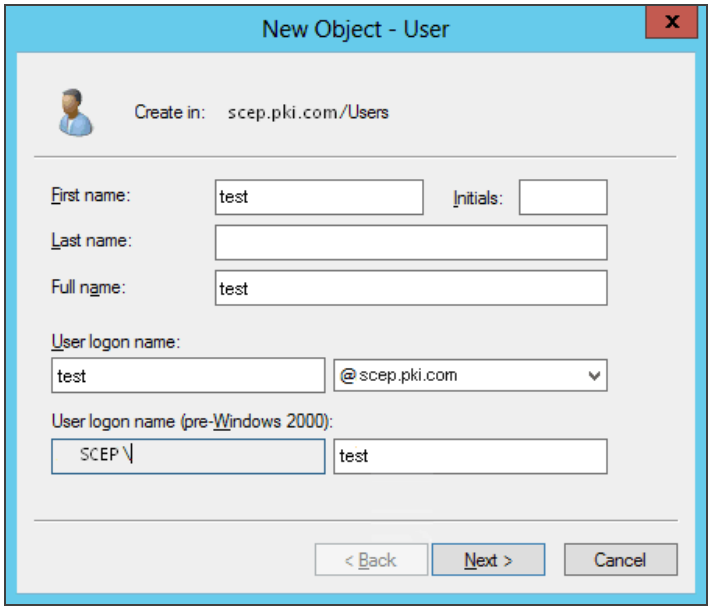
Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

Right-click **Users** and select **New Object > User**.

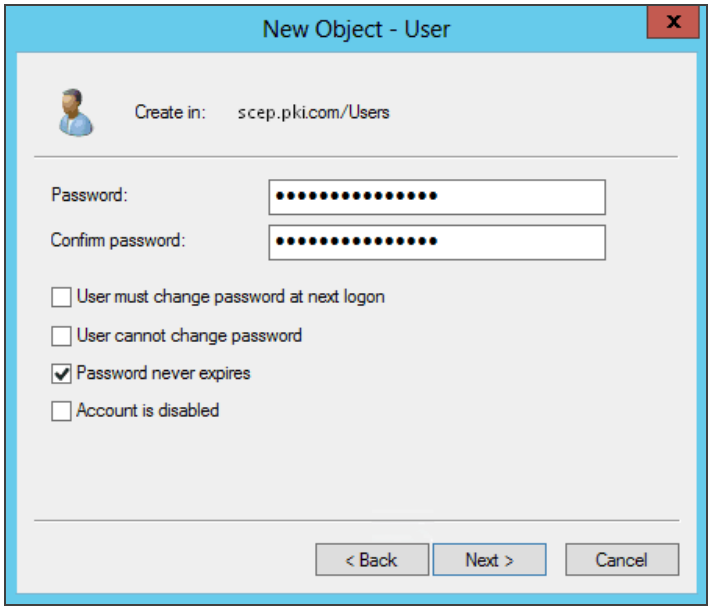
Click **Next**.

- First name: test
- User logon name: test@scep.pki.com



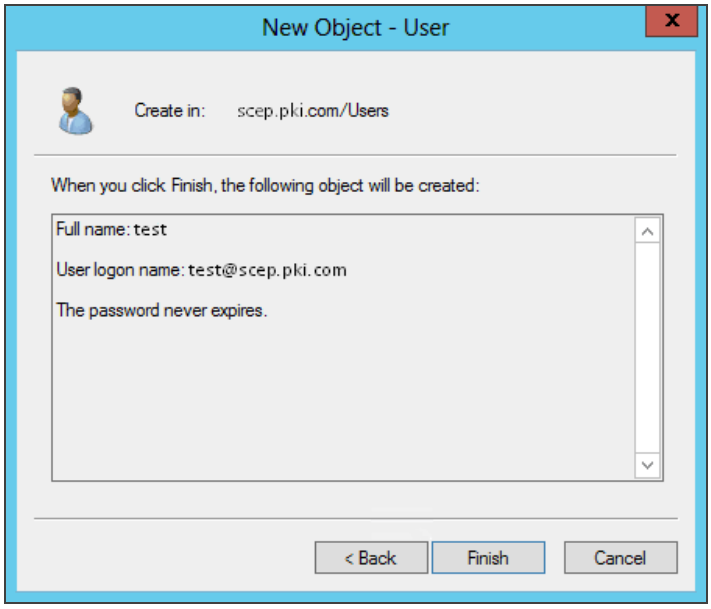
Configure a password on the **New Object- User** page, and click **Next**.

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



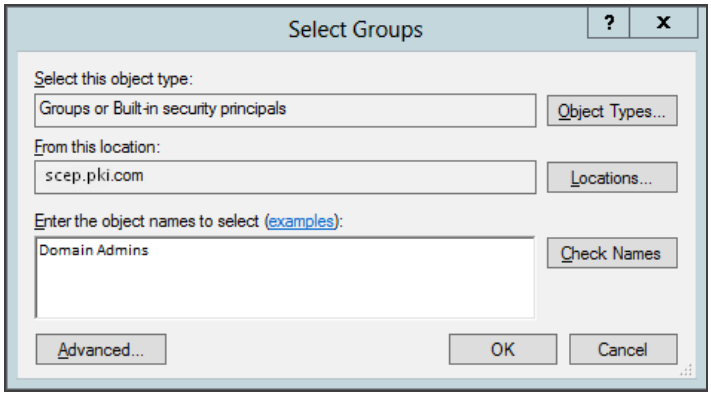
Step 1: Creating a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test**, and select **Add to group**. Click **OK**.

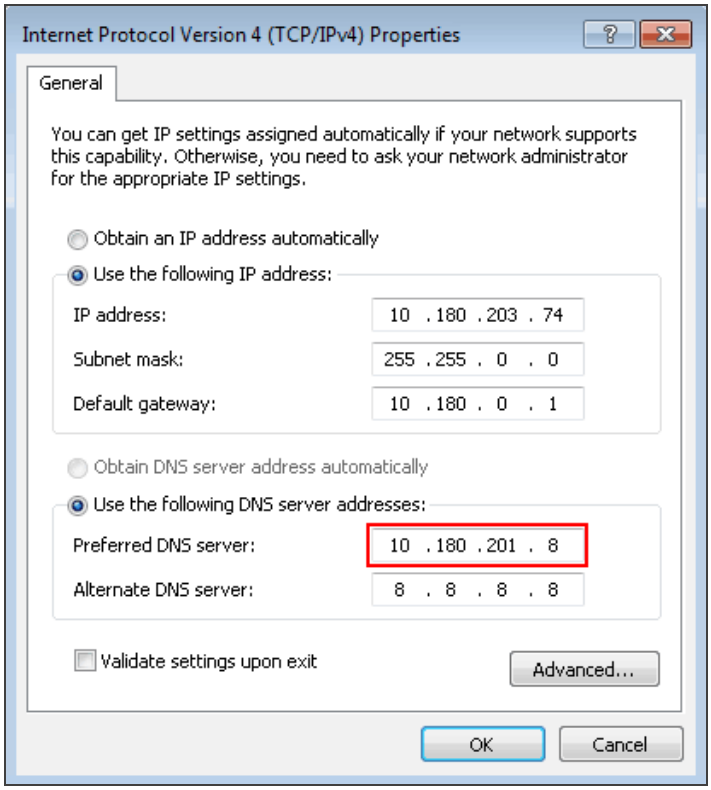
- Enter the object names to select: Domain Admins



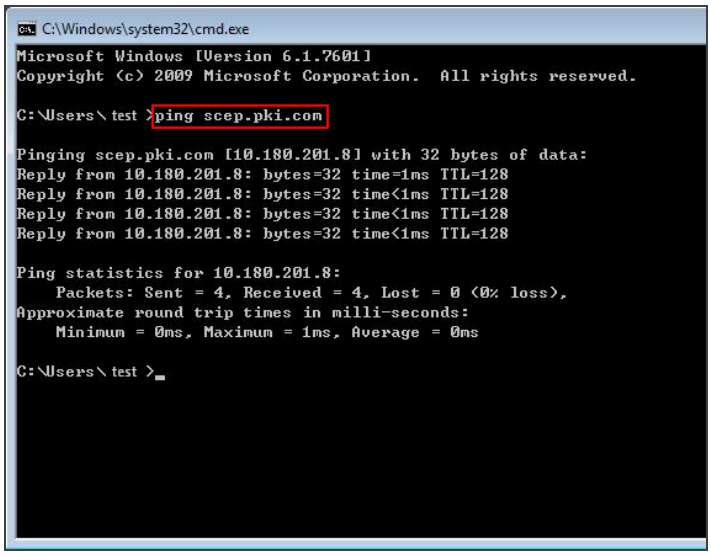
Step 2: Adding PCs of R&D staff into the AD domain (taking one PC as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



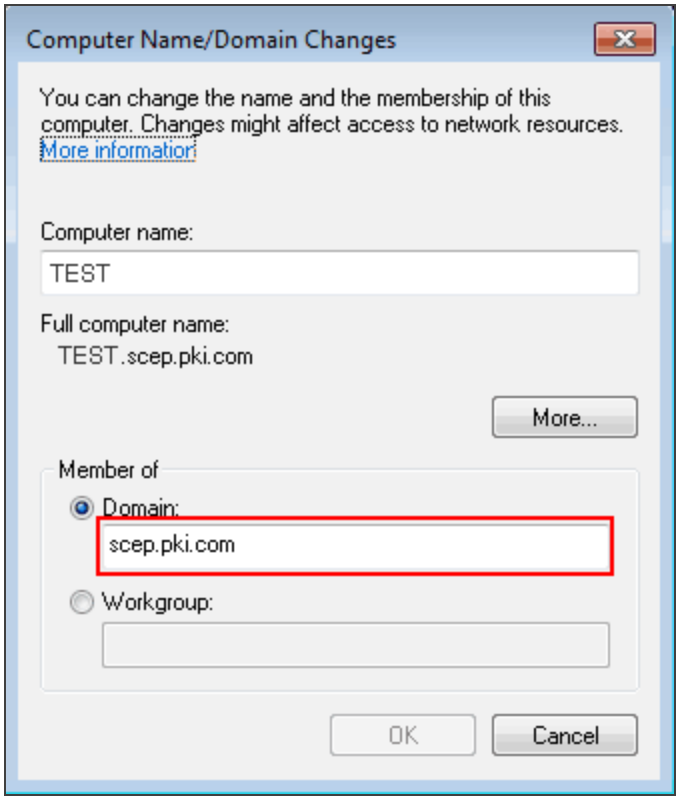
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller (scep.pki.com).



Step 2: Adding PCs of R&D staff into the AD domain (taking one PC as example).

Select **Control Panel > System and Security > System > Computer name, domain, and work-group settings > Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com



In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

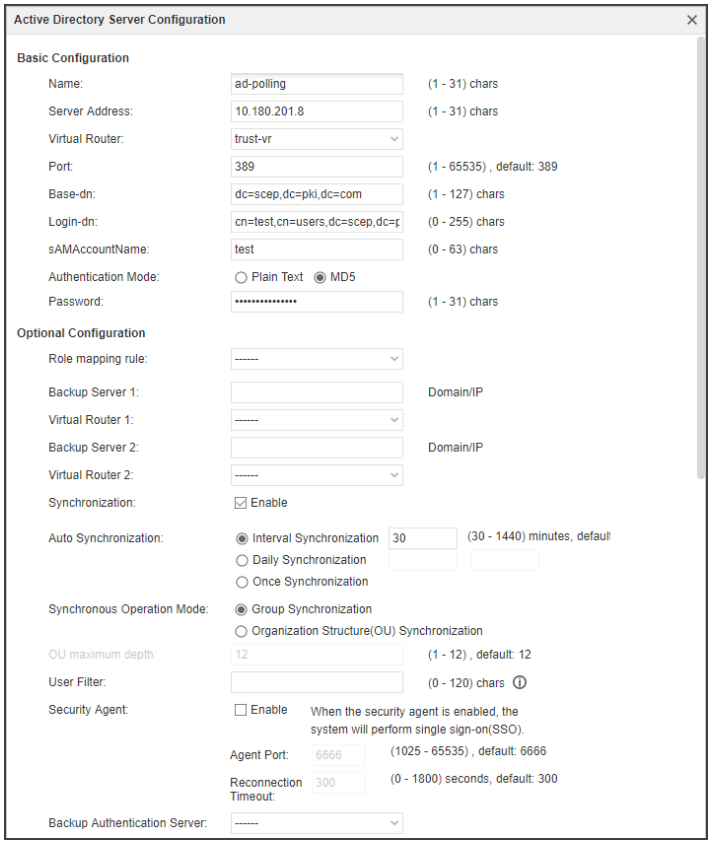
- Domain name\User name: scep\test
- Password: Hillstone123456

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Configuring AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.

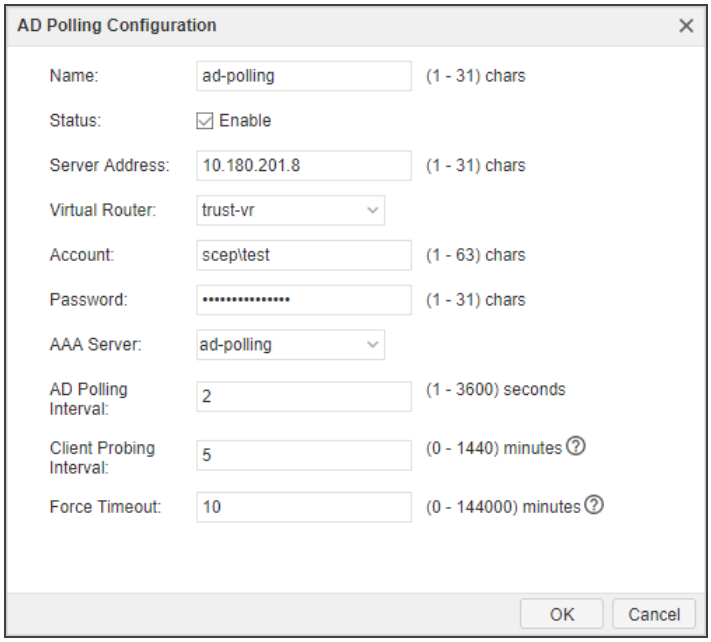
- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,c-cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456



Click **OK** and the AD server is created successfully.

Step 4: Configuring AD Polling in StoneOS

Select **Object > SSO Client > AD Polling**, click **Create** and enter AD Polling Configuration page.



- Name: ad-polling
- Status: click **Enable**
- Host: 10.180.201.8
- Virtual Router: trust-vr
- Account: scep\test
- Password: Hillstone123456
- AAA Server: select the AD server **ad-polling** created in step 3
- AD Polling Interval: 2 seconds
- Client Probing Interval: 5 minutes
- Force Timeout: 10 minutes

Click **OK** to finish AD Polling configuration.

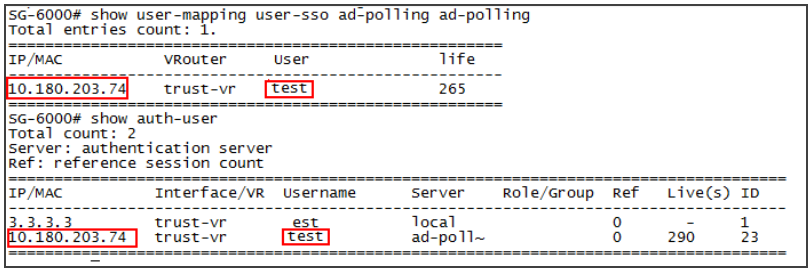
Step 5: Verifying result

After all the above configurations being finished, staff of R&D department (such as the user **test** added in AD domain in this example) can access the Internet without passing Web authentication. However, the staff of marketing department still needs to pass Web authentication before visiting the Internet.

Step 5: Verifying result

If user needs to check the mapping information between user and IP on the device via AD Polling, you're suggested to log in the StoneOS commands operation system and enter the command **show user-mapping user-sso ad-polling** or **show auth-user**.

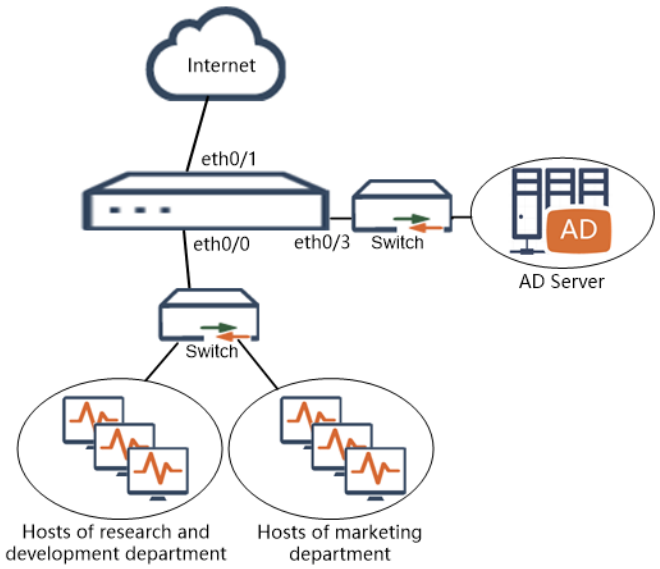
As shown in the figure, in the authentication user list obtained via AD Polling, the corresponding IP of the user **test** is **10.180.203.74**.



Allowing Internet Access via AD Polling

This example introduces how to configure AD polling to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. All the staff in R&D department and marketing department join in the AD domain (scep.pki.com). After the AD Polling being configured, there will be login logs when staffs login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). System can check the logs through AD Polling, as well as obtain authentication users information (user name and IP) on the AD server. With the user-based security policy, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the AD Polling function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote 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`**

- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security > Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it's necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 99.

Configuration Steps

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

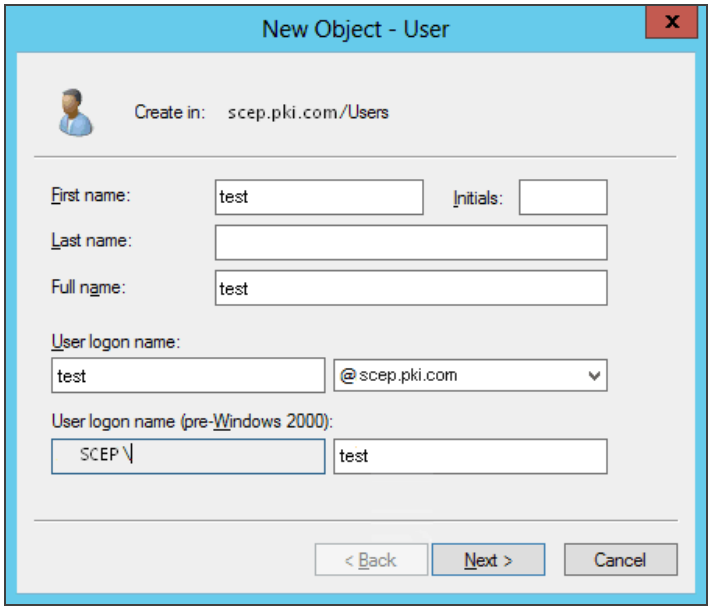
Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Right-click **Users** and select **New Object > User**.

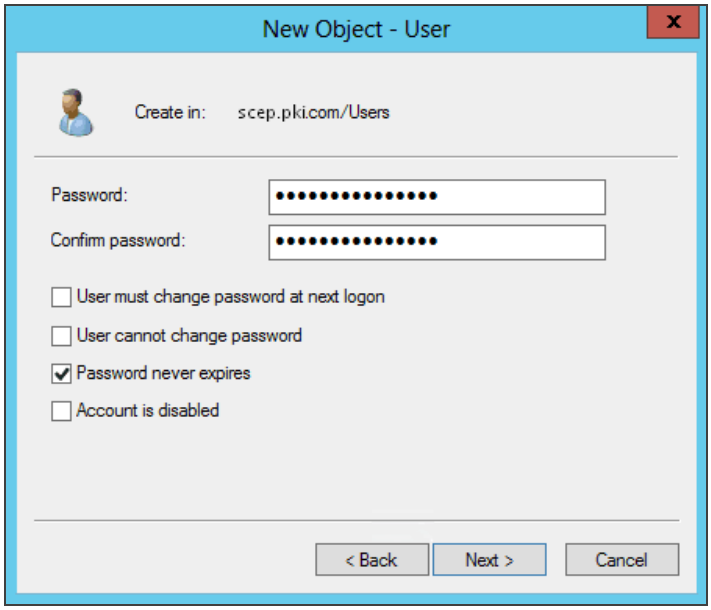
Click **Next**.

- First name: test
- User logon name: test@scep.pki.com



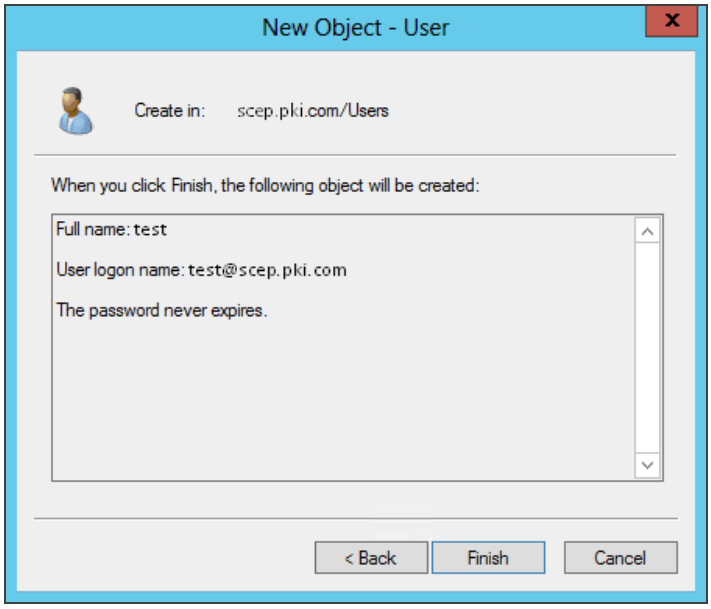
Configure a password on the **New Object- User** page, and click **Next**.

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



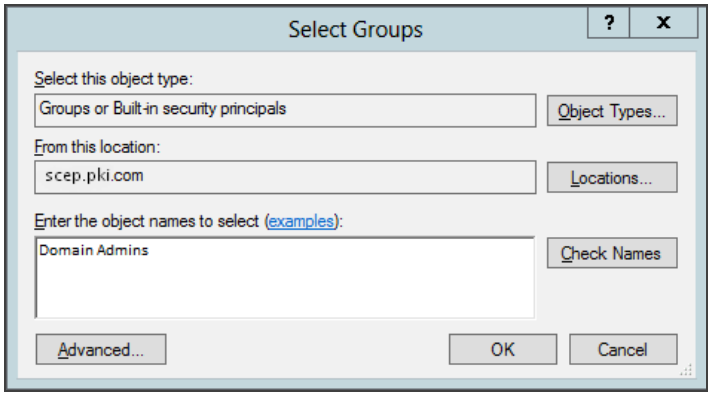
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test** and select **Add to group**. Click **OK**.

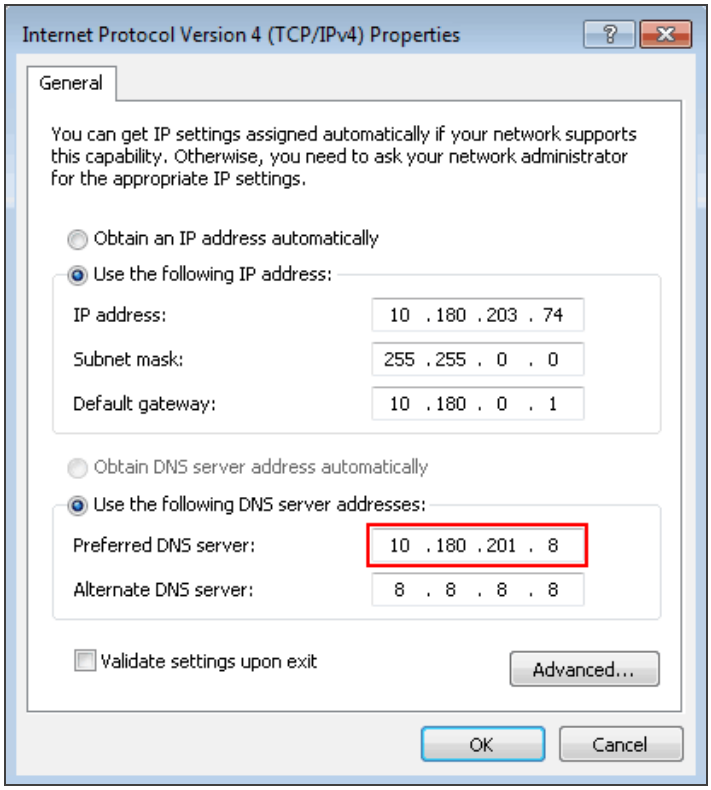
- Enter the object names to select: Domain Admins



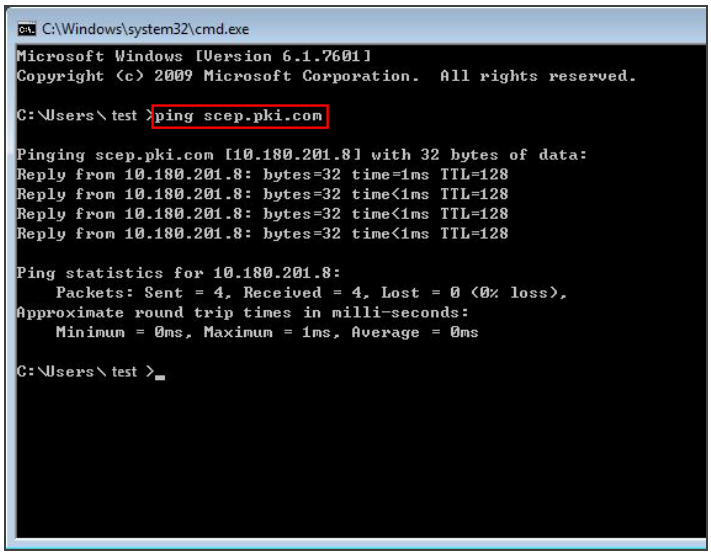
Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



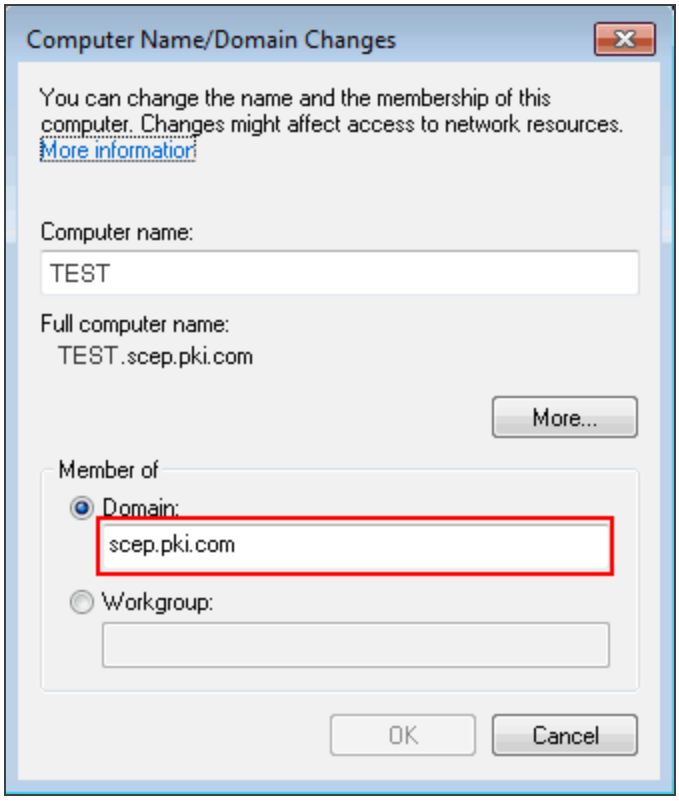
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller (scep.pki.com).



Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > System and Security > System > Computer name, domain, and work-group settings > Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com



In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

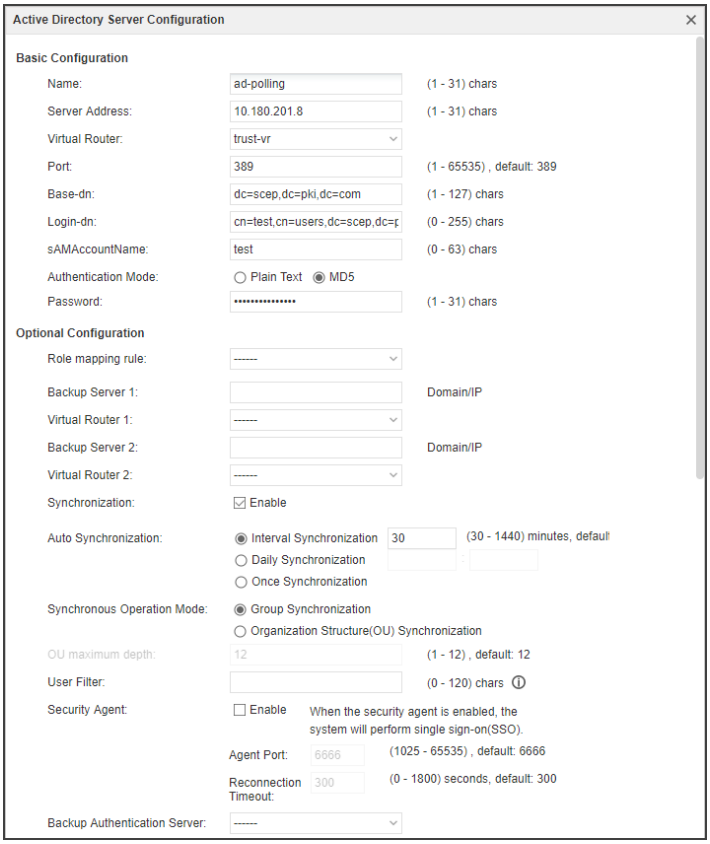
- Domain name\User name: scep\test
- Password: Hillstone123456

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Configure AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.

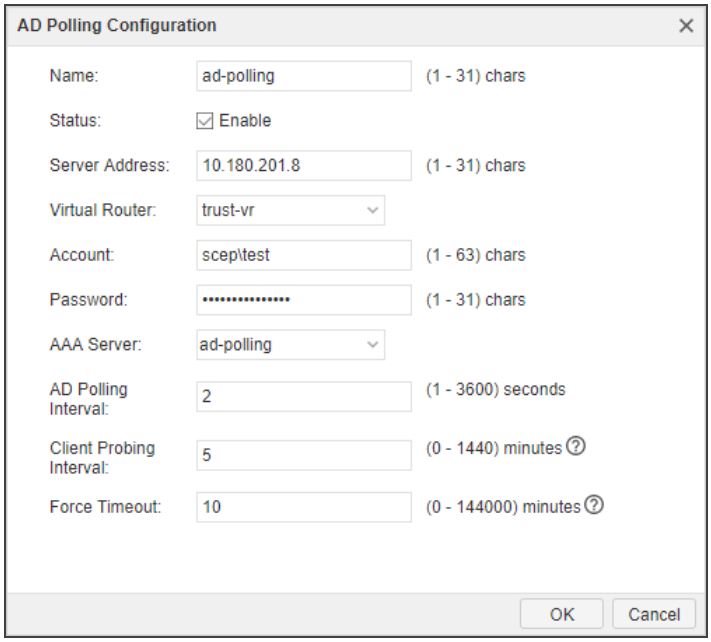
- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,c-cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456



Click **OK** and the AD server is created successfully.

Step 4: Configure AD Polling in StoneOS

Select **Object > SSO Client > AD Polling**, click **Create** and enter AD Polling Configuration page.



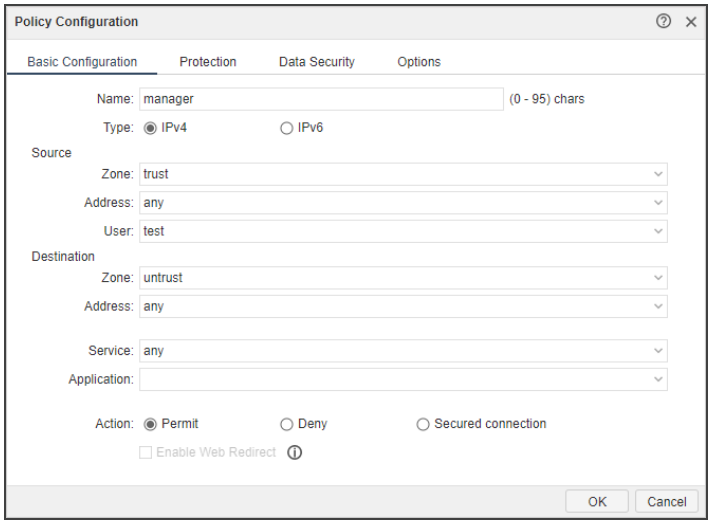
- Name: ad-polling
- Status: click **Enable**
- Host: 10.180.201.8
- Virtual Router: trust-vr
- Account: scep\test
- Password: Hillstone123456
- AAA Server: select the AD server **ad-polling** created in step 3
- AD Polling Interval: 2 seconds
- Client Probing Interval: 5 minutes
- Force Timeout: 10 minutes

Click **OK** to finish AD Polling configuration.

Step 5: Configure policies

Configuring a policy to allow the manager of R&D department to access the Internet

Select **Policy > Security Policy**, and click **New**.

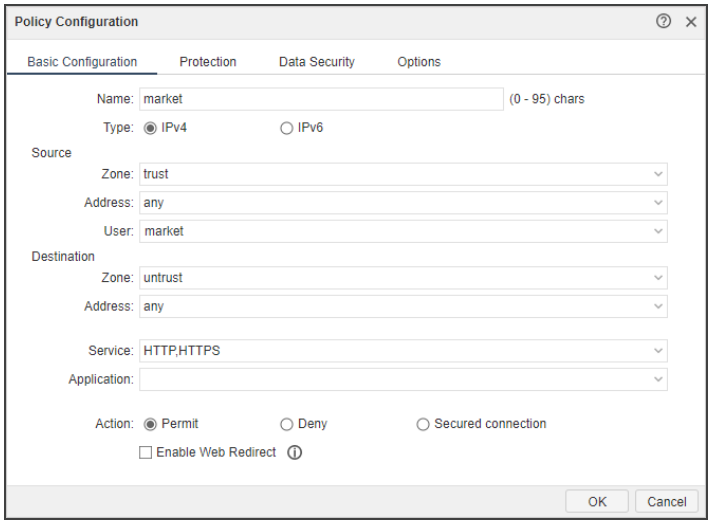


- Name: manager
- Source
  - Zone: trust
  - Address: any
  - User: Select the user name "test" of R&D manager
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Action: Permit

Step 5: Configure policies

Configuring a policy to allow the staff of the marketing department to access the Web service based on HTTP or HTTPS

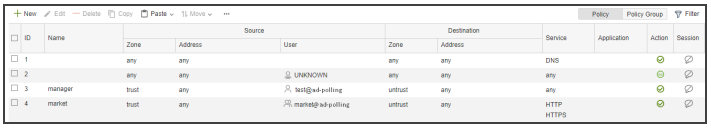
Select **Policy > Security Policy**, and click **New**.



- Name: market
- Source
  - Zone: trust
  - Address: any
  - User: Select the user group "market" of the marketing department
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Service: HTTP, HTTPS
  - Action: Permit

Step 5: Configure policies

Adjusting the priority of policies



1. Select **Policy > Security Policy** to enter the Security Policy page.
2. Select the check box of "manager" and "market" policies, and click **Move**.
3. Type the ID (2) of the second WebAuth policy into the **ToID** text, and click **After ID**.

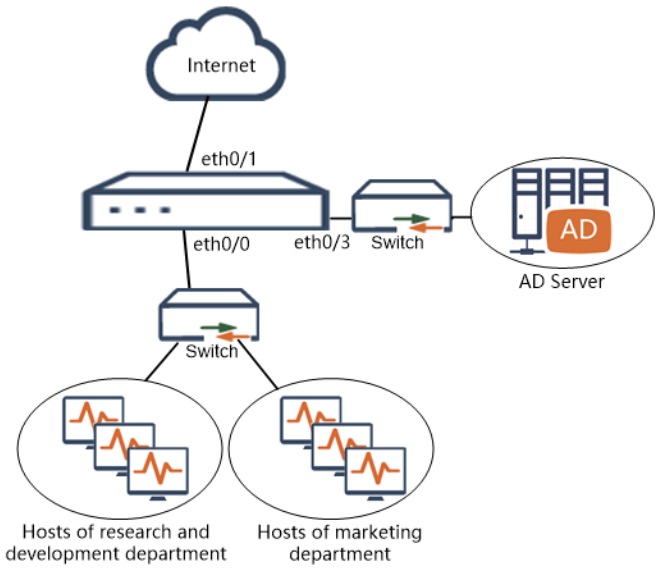
Step 6: Verify result

After all the above configurations, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.

Allowing Internet Access via AD Agent

This example introduces how to configure AD agent to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. All the staff in the R&D department and marketing department join in the AD domain (scep.pki.com). After the AD Agent being configured, there will be login information when staffs login though the AD server (Log in the PC which is added into the AD domain through domain user name and password). The AD Security Agent will send the authentication users information (user name and IP) to system. With the user-based security policy, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the AD Agent function, prepare the following first:

- The AD server has been set up according to the user network environment.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should open the RPC service and remote 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`**

- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security > Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- The security device should be configured with related policy to protect the AD server, which may result in the port used by WMI service (port 135 and random port) being restricted by policy. Therefore, it's necessary to configure another policy (the source IP is the IP address of ethernet0/3) allows all interface traffic to pass through.
- The rule has been configured on the security device that all the staff of the enterprise should pass the Web authentication before they access the Internet. For the detailed configuration method, please see "Allowing the Internet Access via User Authentication" on Page 99.

Configuration Steps

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

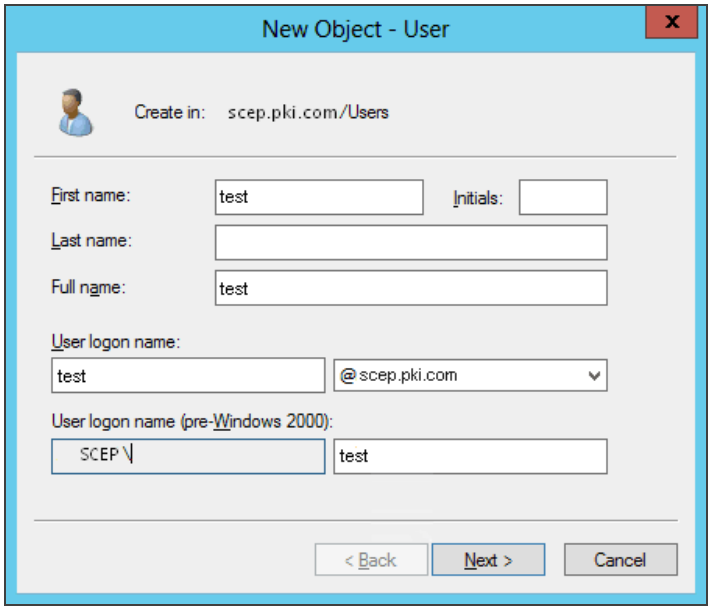
Access the PC with AD server, select **Start > Administrative Tools > Active Directory Users and Computers**, and enter the Active Directory Users and Computers page.

Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Right-click **Users** and select **New Object > User**.

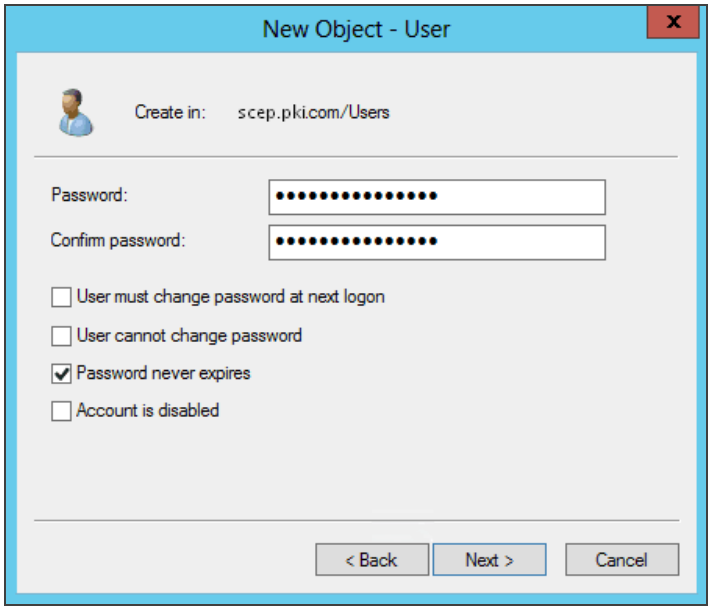
Click **Next**.

- First name: test
- User logon name: test@scep.pki.com



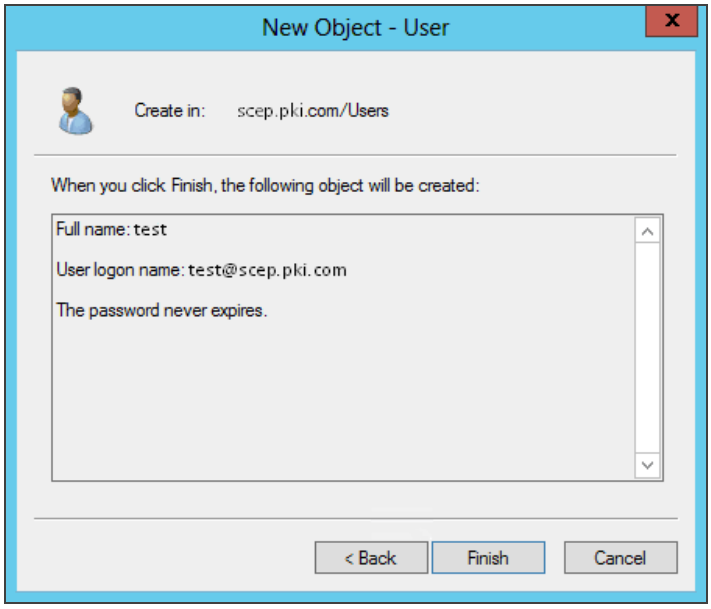
Configure a password on the **New Object- User** page, and click **Next**.

- Password: Hillstone123456
- Confirm password: Hillstone123456
- Password never expires: Select the check box



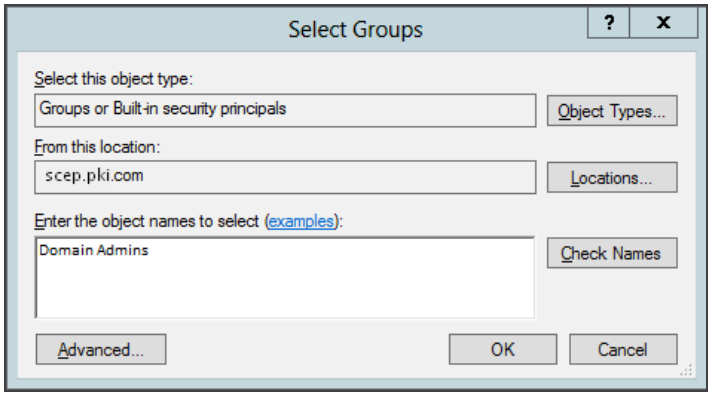
Step 1: Create a new domain user on the AD server and configuring the user as the Domain Admins group.

Click **Finish** to finish the creating of domain user **test**.



In the user list, right-click **test** and select **Add to group**. Click **OK**.

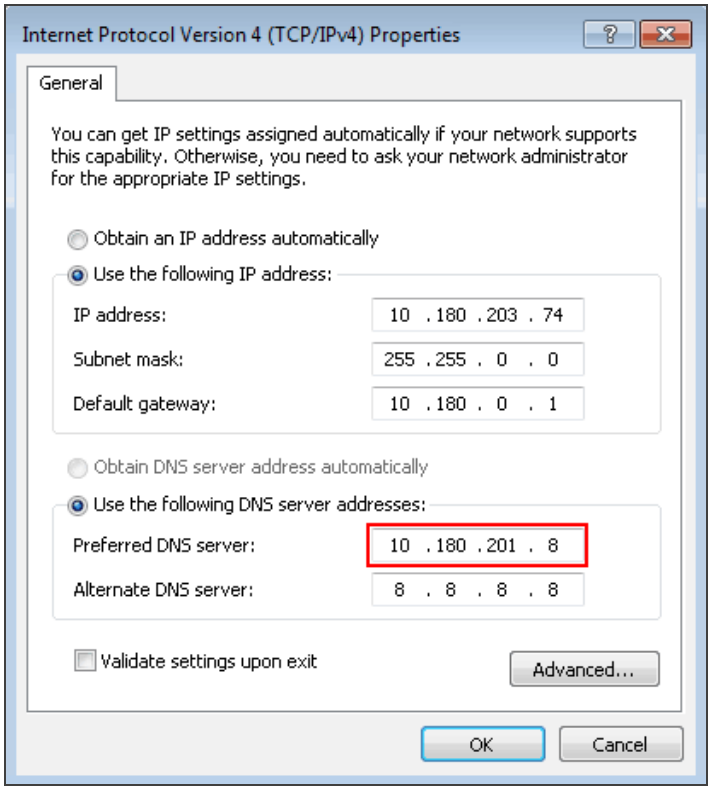
- Enter the object names to select: Domain Admins



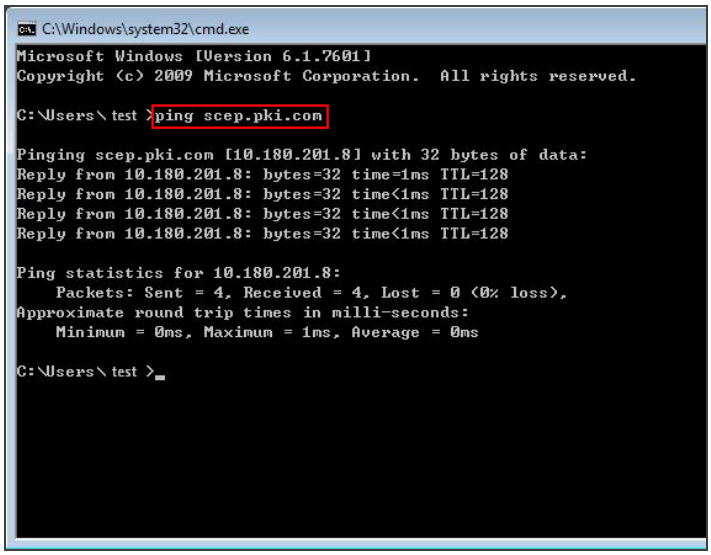
Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > Network and Internet > Network and Sharing Center** to check the attribute of network connection. Double-click **Internet Protocol Version 4 (TCP/IPv4)**, enter the Internet Protocol Version 4 (TCP/IPv4) Properties page and change the IP address of Preferred DNS server to the IP address of AD domain controller.

- Preferred DNS server: 10.180.201.8
- Alternate DNS server: 8.8.8.8



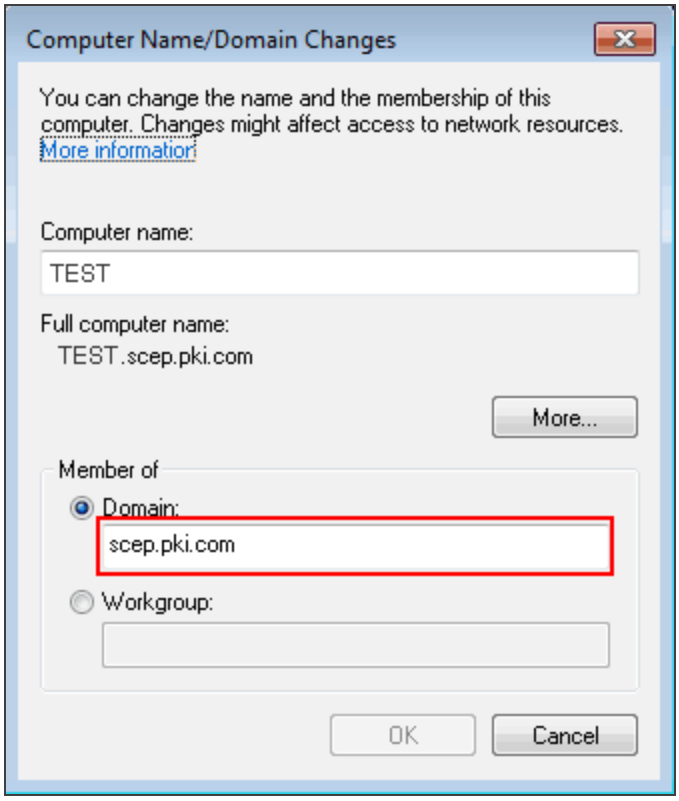
Search **cmd** in the Start menu and double-click to open the command prompt(cmd) application window, so as to make sure that the PC can be connected to the AD domain controller (scep.pki.com).



Step 2: Add PCs of R&D staff into the AD domain (taking the PC of R&D manager as example).

Select **Control Panel > System and Security > System > Computer name, domain, and work-group settings > Change settings**, and add the PC into the AD domain (scep.pki.com). Click **OK**.

- Domain: scep.pki.com

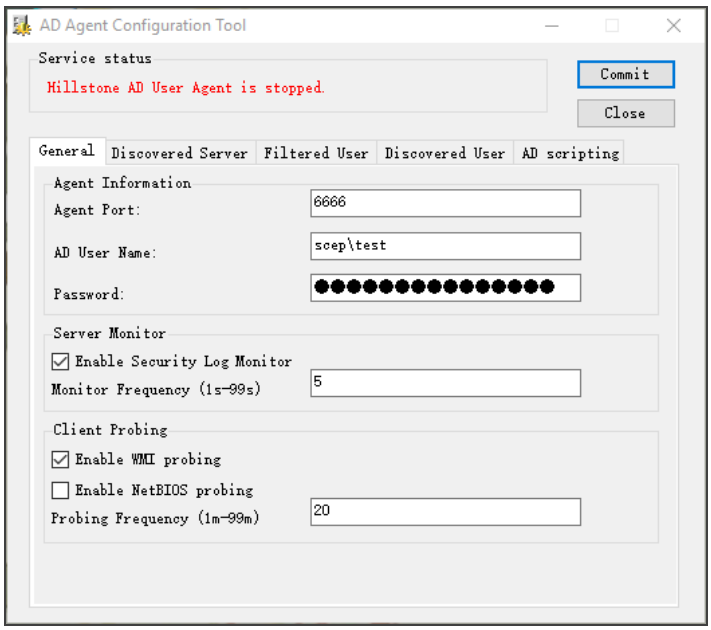


In the **Windows security** dialog box, enter Domain name\User name and Password. The user name should be the one in the Domain Admins group.

- Domain name\User name: scep\test
- Password: Hillstone123456

After the PC being added in the AD domain (scep.pki.com) successfully, restart the computer to make it take effect.

Step 3: Install and configure AD Security Agent in AD server.

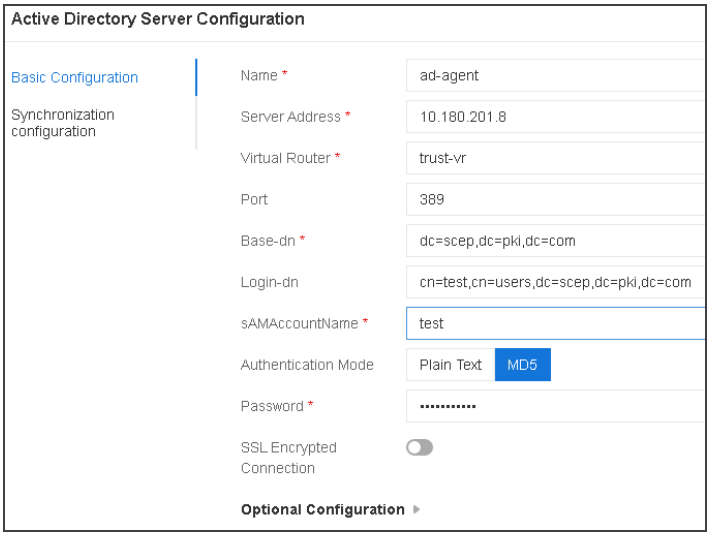


1. Click http://swup-date.hillstonenet.com:1337/sslvpn/download?os=windows-adagent to download an AD Security Agent installation program, and copy it to the AD server.
2. Double-click `ADAgentSetup.exe` to open it and follow the installation wizard to install it.
3. Double-click the `AD Agent Configuration Tool` shortcut, and the **AD Agent Configuration Tool** dialog pops up.
4. Click the **General** tab.
   - Agent Port: 6666
   - AD User Name: scep\test
   - Password: Hillstone123456
   - Server Monitor: Select the **Enable Security Log Monitor** check box, and configure the Monitor Frequency as 5 seconds
   - Client Probing: Select the **Enable WMI probing** check box, and configure the Probing Frequency as 20 minutes

Click **Commit** to commit the above configurations and start the AD Agent service.

Step 4: Configure AD server parameters in StoneOS.

Select **Object > AAA server**, and select **Active Directory Server** from the newly created drop-down list.



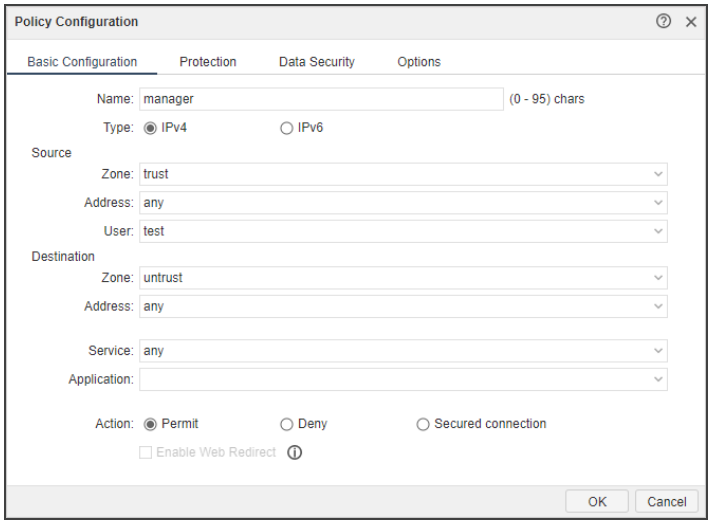
- Server Name: ad-polling
- Server Address: 10.180.201.8
- Base-dn: dc=scep,dc=pki,dc=com
- Login-dn: cn=test,c-cn=users,dc=scep,dc=pki,dc=com
- sAMAccountName: test
- Authentication Mode: MD5
- Password: Hillstone123456
- Security Agent: Select the check box, and configure the Agent Port as 6666

Click **OK** to finish AD server configuration.

Step 5: Configure policies

Configuring a policy to allow the manager of R&D department to access the Internet

Select **Policy > Security Policy**, and click **New**.

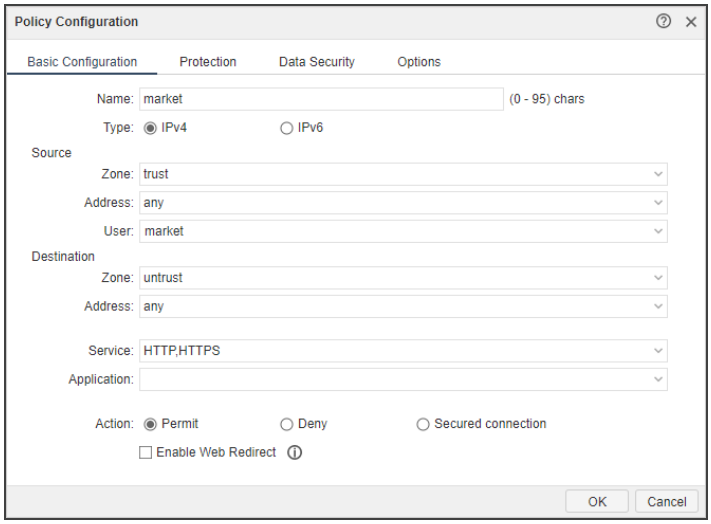


- Name: manager
- Source
  - Zone: trust
  - Address: any
  - User: Select the user name "test" of R&D manager
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Action: Permit

Step 5: Configure policies

Configuring a policy to allow the staff of the marketing department to access the Web service based on HTTP or HTTPS

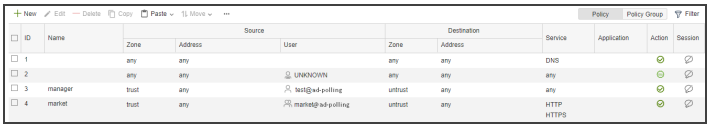
Select **Policy > Security Policy**, and click **New**.



- Name: market
- Source
  - Zone: trust
  - Address: any
  - User: Select the user group "market" of the marketing department
- Destination
  - Zone: untrust
  - Address: any
- Other Information
  - Service: HTTP, HTTPS
  - Action: Permit

Step 5: Configure policies

Adjusting the priority of policies



1. Select **Policy > Security Policy** to enter the Security Policy page.
2. Select the check box of "manager" and "market" policies, and click **Move**.
3. Type the ID (2) of the second WebAuth policy into the **ToID** text, and click **After ID**.

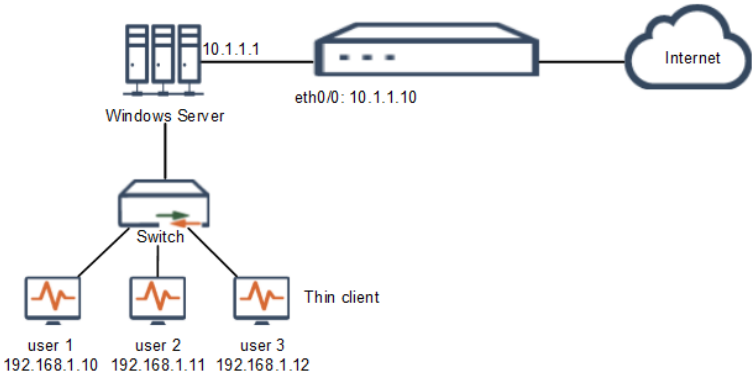
Step 6: Verify result

After all the above configurations being finished, only the R&D manager can access the Internet, while other staffs of the R&D department cannot access the Internet, and the staff of the marketing department can access the Web service based on HTTP or HTTPS.

Allowing Internet Access via TS Agent

This example introduces how to configure TS Agent to allow users to access the Internet.

The following shows a network environment. An enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Internal users connect to a Windows server through thin clients. 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. With the user-based security policy, only user 1 can access the Internet, while user 2 cannot access the Internet, and user 3 can access the Web service based on HTTP or HTTPS.



Preparation

Before configuring the TS Agent function, prepare the following first:

- The Windows server has been set up according to the user network environment. 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.
- The SNAT rule has been configured on the security device, and all the internal users can access the Internet. For the detailed configuration method, please see "Allowing Private Network to Access Internet Using SNAT" on Page 26.

Configuration Steps

Step 1: Installing and configuring 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.

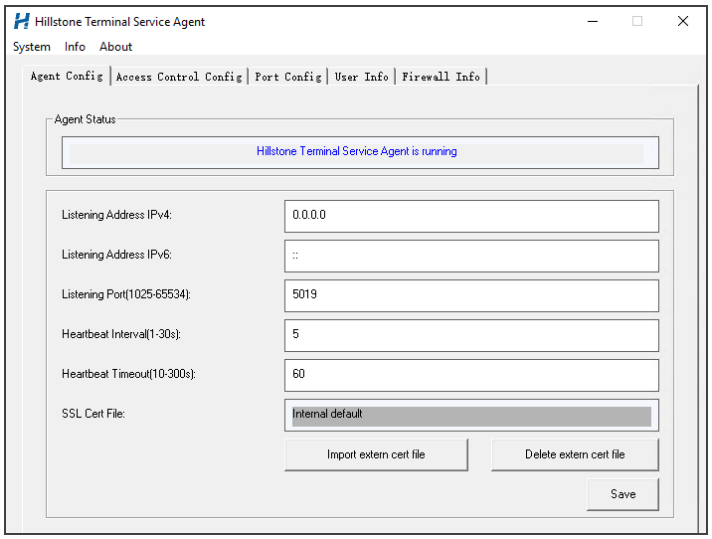
2. Double-click `HSTSAgent.exe` to open it and follow the installation wizard to install it.

3. Double-click the `Hillstone Terminal Service Agent` shortcut, and the **Hillstone Terminal Service Agent** dialog pops up.

4. Click the **Agent config** tab.

- 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.

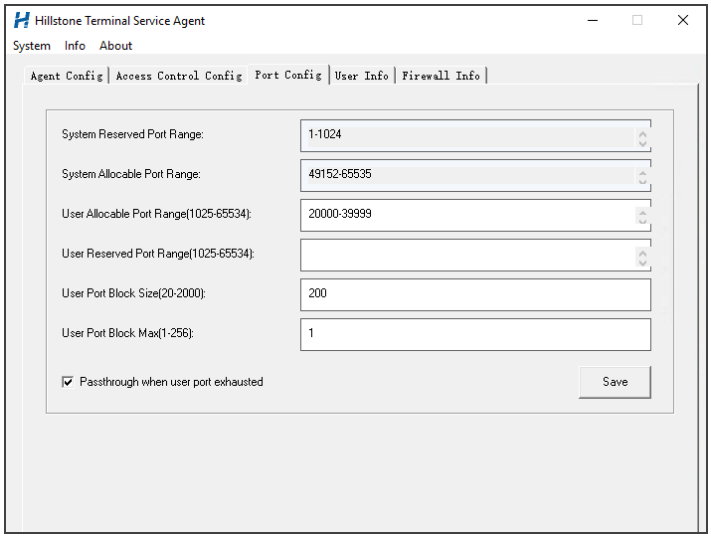


Step 1: Installing and configuring Hillstone Terminal Service Agent in Windows server.

5. Click the **Port config** tab.

- 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.

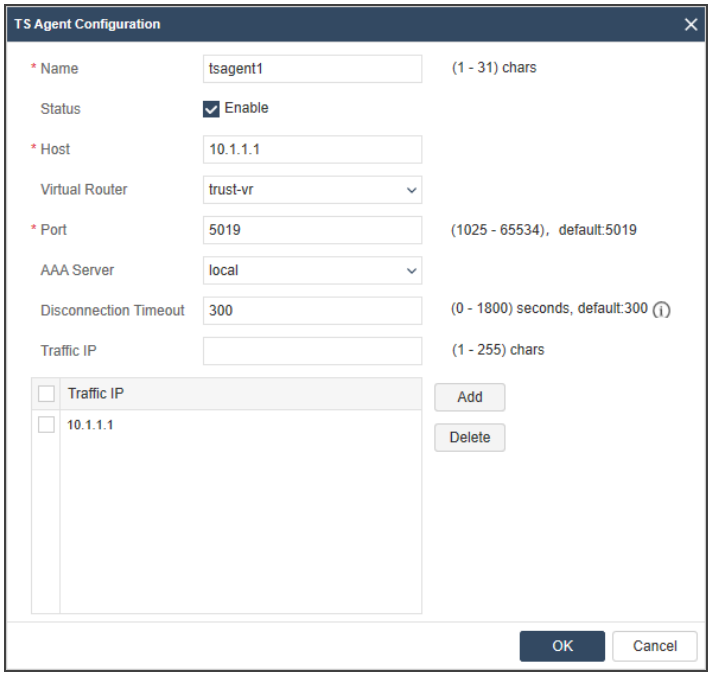


Step 2: Configuring TS Agent parameters in StoneOS via WebUI and CLI.

WebUI

Select **Object > SSO Client > TS Agent**, and click **New** .

- Name: tsagent1
- Status: Select the **Enable** check box
- HOST: 10.1.1.1
- Virtual Router: trust-vr
- Port: 5019
- AAA Server: local
- Disconnection Timeout: 300
- Traffic IP: Enter 10.1.1.1, and click **Add**



Step 2: Configuring TS Agent parameters in StoneOS via WebUI and CLI.

Click **OK** to save the configurations.

CLI

```
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
```

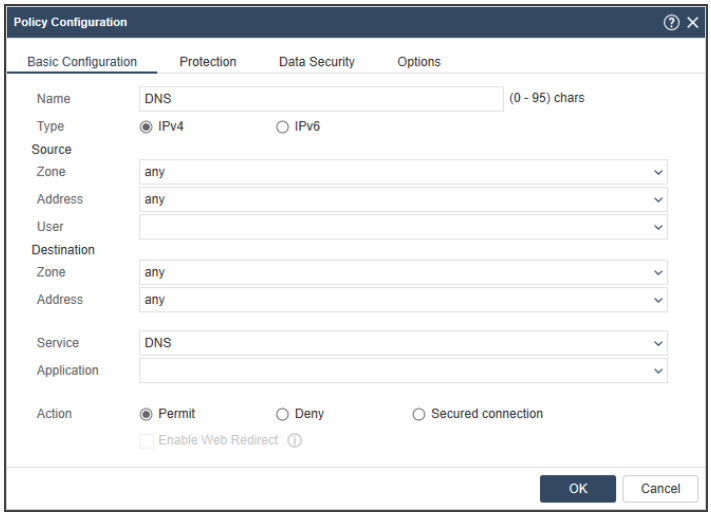
Step 3: Configuring policies in StoneOS via WebUI and CLI.

WebUI

Step 3: Configuring policies in StoneOS via WebUI and CLI.

Configuring a policy to allow all DNS traffic to get through.

Because DNS traffic is system traffic of the Windows Server, not the traffic of one specific user, configure a policy to allow all DNS traffic to get through first.



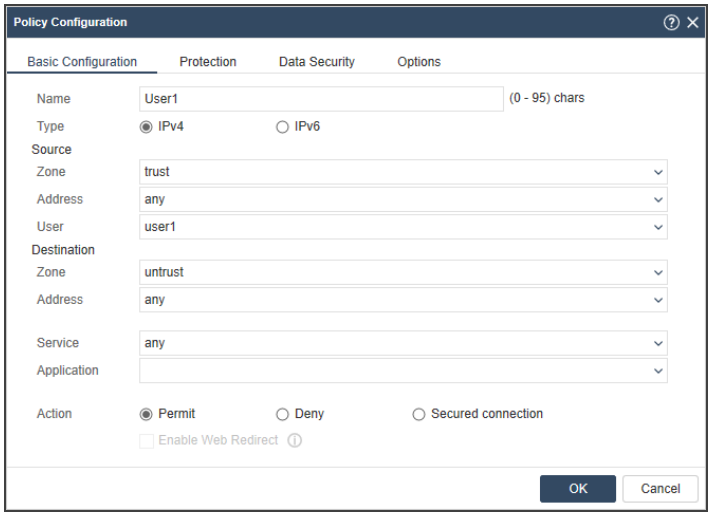
Select **Policy > Security Policy**, and click **New**.

- Name: DNS
- Source
  - Zone: any
  - Address: any
- Destination
  - Zone: any
  - Address: any
  - Service: DNS
  - Action: Permit

Step 3: Configuring policies in StoneOS via WebUI and CLI.

Configuring a policy to allow user 1 to access the Internet.

Select **Policy > Security Policy**, and click **New**.

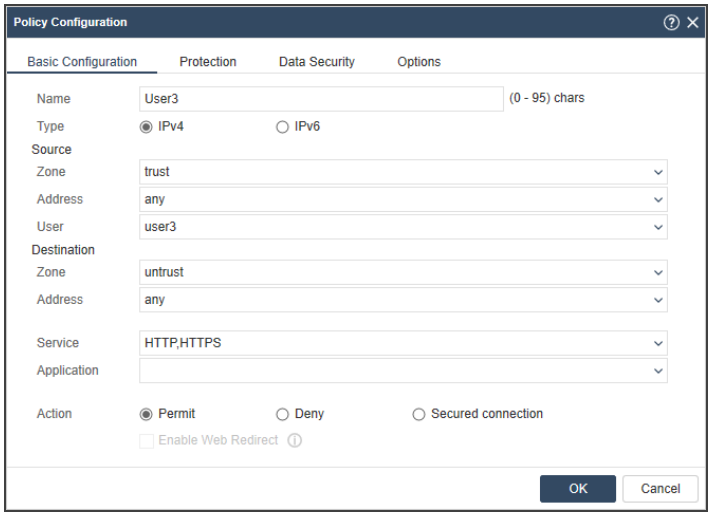


- Name: User1
- Source
  - Zone: trust
  - Address: any
  - User: user1
- Destination
  - Zone: untrust
  - Address: any
  - Action: Permit

Step 3: Configuring policies in StoneOS via WebUI and CLI.

Configuring a policy to allow user 3 to access the Web service based on HTTP or HTTPS

Select **Policy > Security Policy**, and click **New**.



- Name: User3
- Source
  - Zone: trust
  - Address: any
  - User: user3
- Destination
  - Zone: untrust
  - Address: any
  - Service: HTTP, HTTPS
  - Action: Permit

CLI

```
host-name(config)# rule name DNS from any to any service DNS permit

Rule id 2 is created.

host-name(config)# rule name User1 user local user1 from any to any from-
zone trust to-zone untrust permit

Rule id 3 is created.

host-name(config)# rule name User3 user local user3 from any to any from-
zone trust to-zone untrust service HTTP permit

Rule id 4 is created.

host-name(config)# rule id 4

host-name(config-policy-rule)# service HTTPS

host-name(config-policy-rule)# exit
```

Step 4: Verifying result

After all the above configurations are finished, only user 1 can access the Internet, while user 2 cannot access the Internet, and user 3 can access the Web service based on HTTP or HTTPS.

VPN

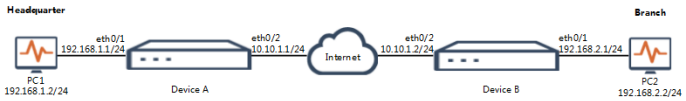
This chapter introduces virtual private network deployment.

This chapter contains the following recipes:

- IPSec VPN
  - "Connection between Two Private Networks Using IPSec VPN (IKEv1)" on Page 147
  - "Connection between Two Private Networks Using IPSec VPN (IKEv2)" on Page 160
  - "Connecting to Microsoft Azure Using Site-to-Site VPN" on Page 212
  - "Establishment of IPSec VPN Based on Certificate Authentication " on Page 173
  - "Realizing Dynamic Switch between IPSec Links Using IPSec VPN Smart Link" on Page 186
- SSL VPN
  - "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 199
  - "Using an iOS/Android Device to Remotely Access Intranet Services" on Page 223
- L2TP over IPSec VPN
  - "Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN" on Page 230
  - "Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN" on Page 249
- GRE over IPSec VPN
  - "Connection between Two Private Networks Using GRE over IPSec VPN" on Page 277
- VXLAN
  - " Configuring VXLAN Static Unicast Tunnel" on Page 293

Connection between Two Private Networks Using IPSec VPN (IKEv1)

This example tells how to create IPSec VPN (IKEv1)tunnels to encrypt and protect the communication between two private networks . Usually, IPSec VPN tunnel is to connect the Device A in a branch office and the Device B in the headquarters.



*** Note:** This topology uses laboratory environment. In this recipe, 10.10.1.0/24 represents public network.

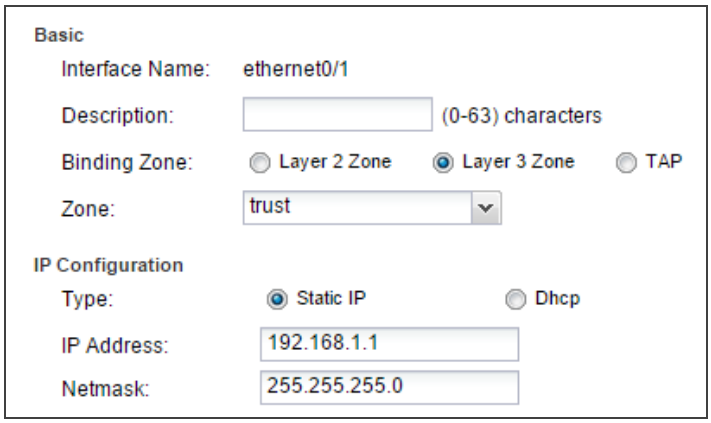
Configuration Steps

Device A

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.



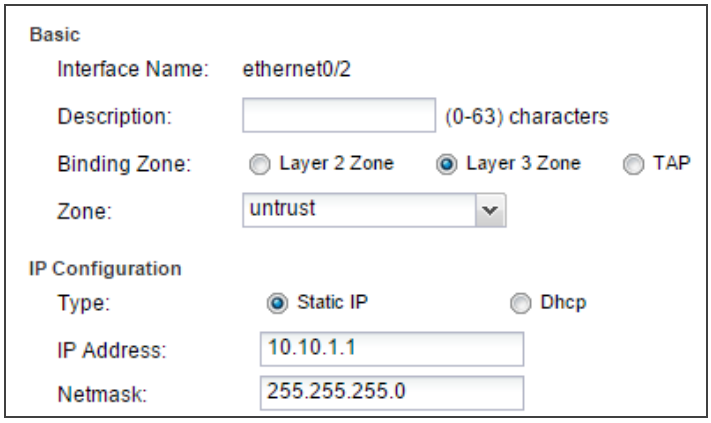
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0

Step 1: Configuring interface

2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.

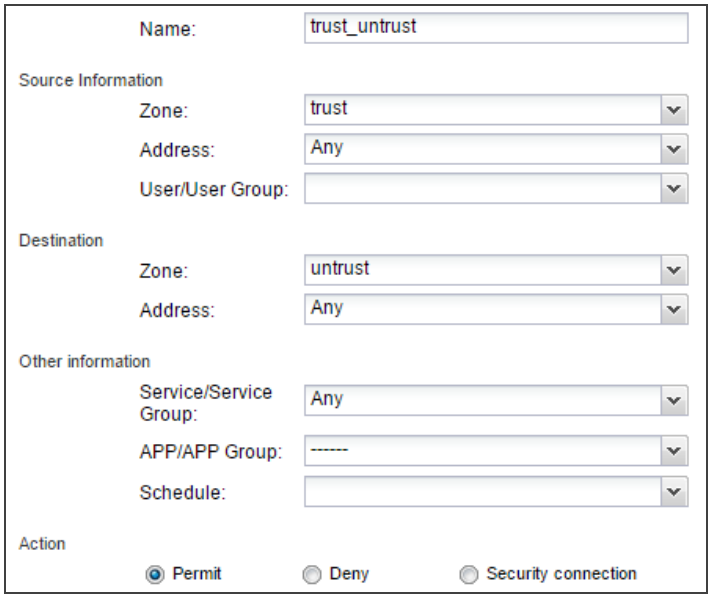
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0



Step 2: Configuring security policies

1. Creating a policy to allow private network to visit Internet

Select **Policy > Security Policy**, and click **New**.



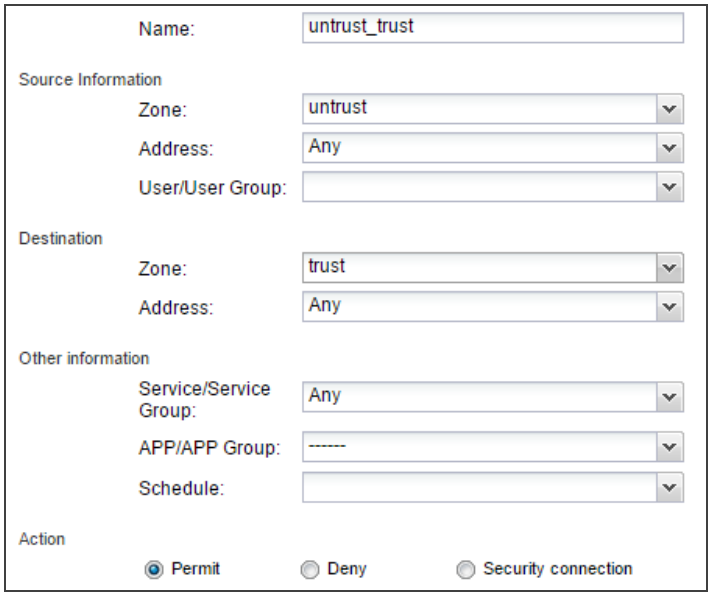
- Name: trust_untrust
- Source Information
  - Zone: trust
  - Address: Any
- Destination
  - Zone: untrust
  - Address: Any
- Other Information
  - Action: Permit

Step 2: Configuring security policies

2. Creating a security policy to allow Internet visit private network

Select **Policy > Security Policy**, and click **New**.

- Name: untrust_trust
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other Information
  - Action: Permit

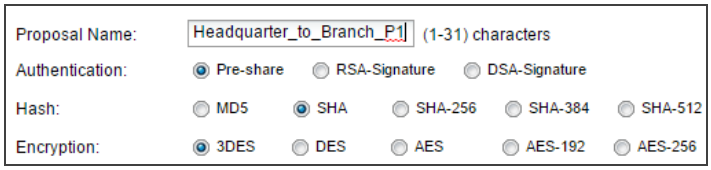


Step 3: Configuring IPSec VPN

1. Configuring P1 proposal for IKE SA

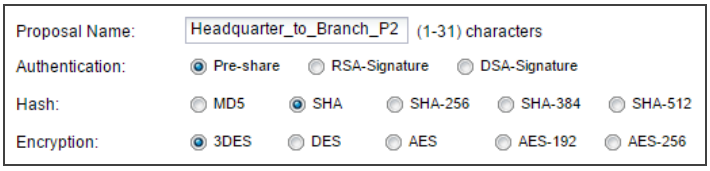
Select **Network > VPN > IPSec VPN**, under the P1 Proposal tab, click **New**.

- Proposal Name: Headquarter_to_Branch_P1
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES



Step 3: Configuring IPSec VPN

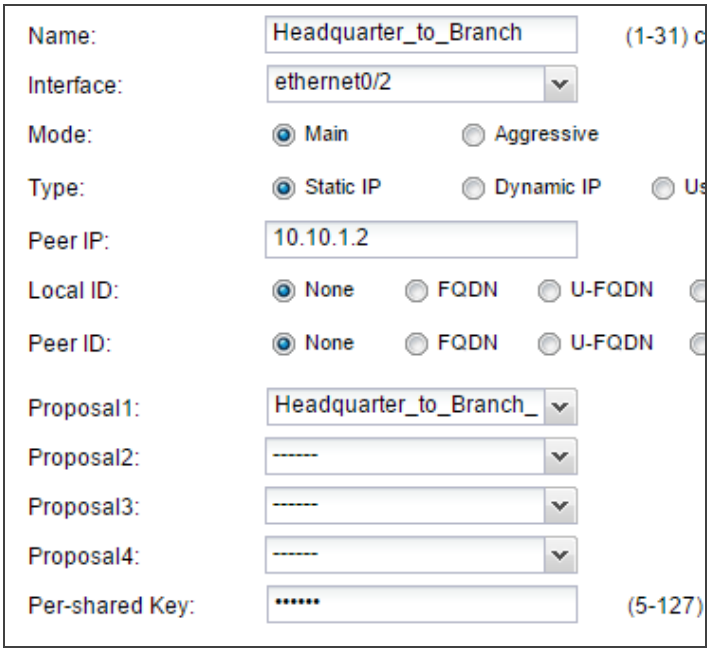
2. Configuring P2 proposal for IPSec SA



Select **Network > VPN > IPSec VPN**, under the P2 Proposal tab, click **New**.

- Proposal Name: Headquarter_to_Branch_P2
- Authentication: ESP
- Hash: SHA
- Encryption: 3DES

3. Configuring VPN peer



Select **Network > VPN > IPSec VPN**, under the VPN Peer List tab, click **New**.

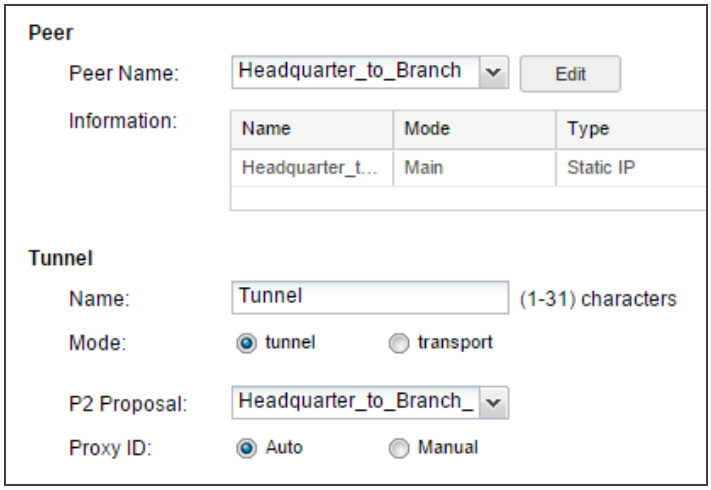
- Name: Headquarter_to_Branch
- Interface: ethernet0/2
- Mode: Main
- Type: Static IP
- Peer IP: 10.10.1.2
- Proposal 1: Headquarter_to_Branch_P1
- Pre-share Key: 123456

Step 3: Configuring IPSec VPN

4. Configuring IKE VPN

Select **Network > VPN > IPSec VPN**, under the IKE VPN List tab, click **New**.

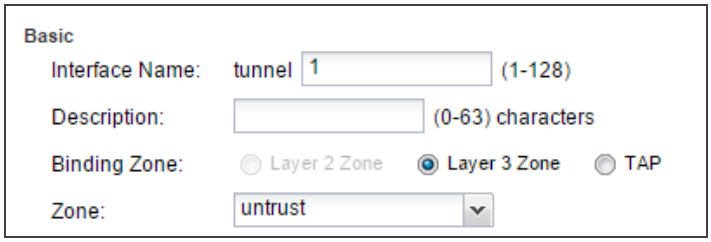
- Peer Name: Headquarter_to_Branch
- Tunnel Name: Tunnel
- Mode: tunnel
- P2 Proposal: Headquarter_to_Branch_P2

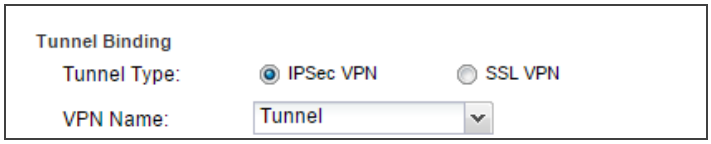


Step 4: Creating tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

- Basic
  - Name: 1
  - Zone: untrust
- Tunnel Binding
  - Tunnel Type: IPSec VPN
  - VPN Name: Tunnel

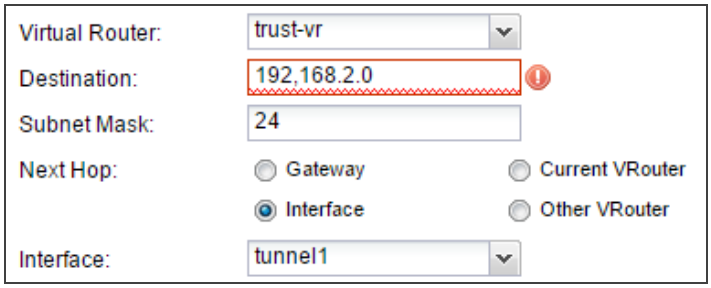




Step 5: Configuring route

Select **Network > Routing > Destination Routing**, and click **New**.

- Destination: 192.168.2.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel1



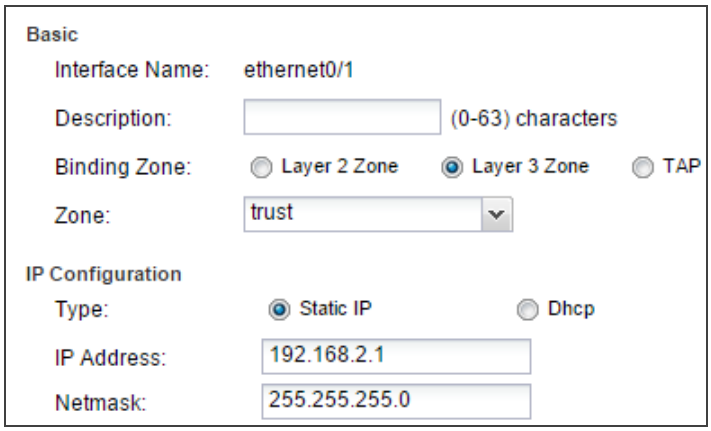
Device B

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

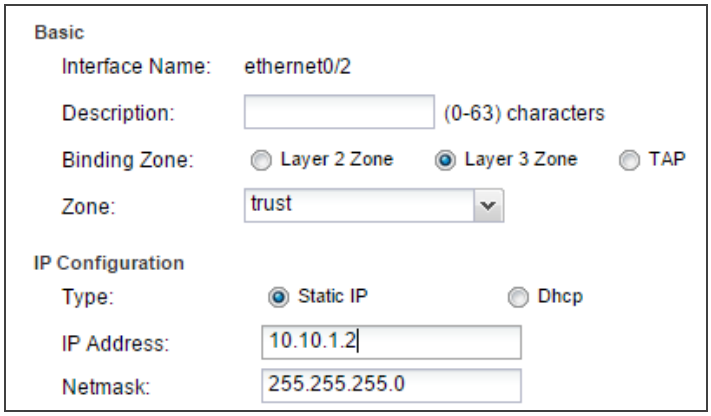
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.2.1
- Netmask: 255.255.255.0



Step 1: Configuring interface

2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.



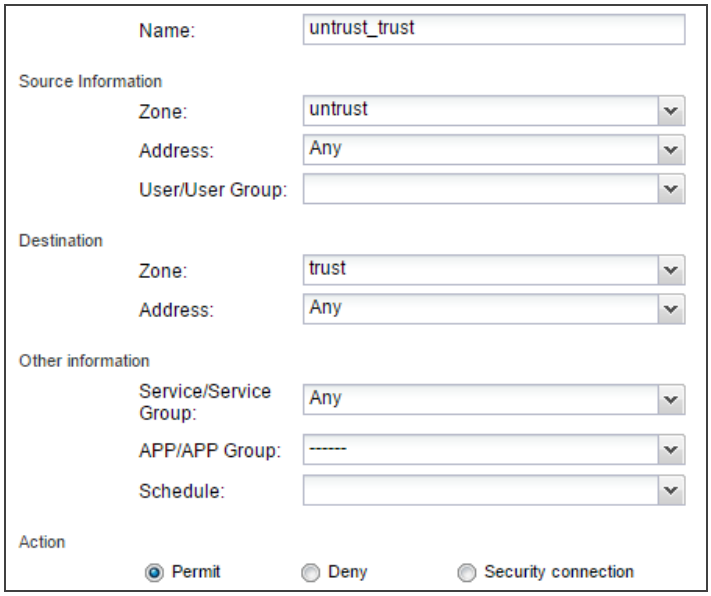
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.2
- Netmask: 255.255.255.0

Step 2: Configuring security policies

1. Creating a policy to allow private network to visit Internet

Select **Policy > Security Policy**, and click **New**.

- Name: trust_untrust
- Source Information
  - Zone: trust
  - Address: Any
- Destination
  - Zone: untrust
  - Address: Any
- Other Information
  - Action: Permit

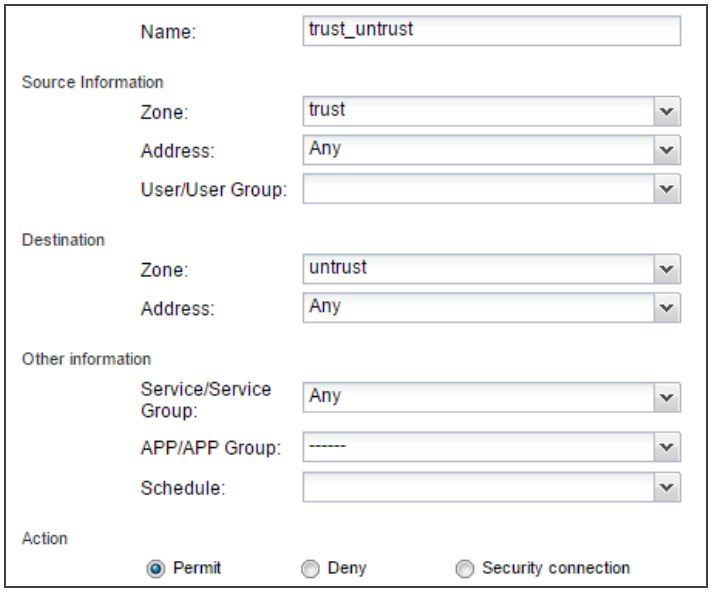


Step 2: Configuring security policies

2. Creating a security policy to allow Internet visit private network

Select **Policy > Security Policy**, and click **New**.

- Name: untrust_trust
- Source Information
  - Zone: untrust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other Information
  - Action: Permit

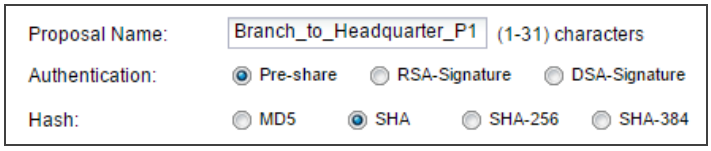


Step 3: Configuring IPSec VPN

1. Configuring P1 proposal for IKE SA

Select **Network > VPN > IPSec VPN**, under the P1 Proposal tab, click **New**.

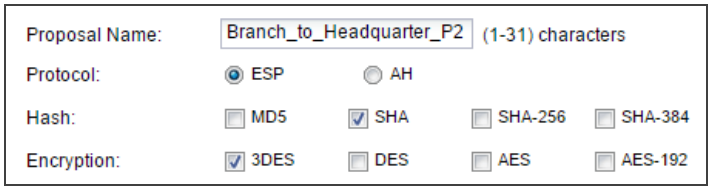
- Proposal Name: Branch_to_Headquarter_P1
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES



Step 3: Configuring IPSec VPN

2. Configuring P2 proposal for IPSec SA

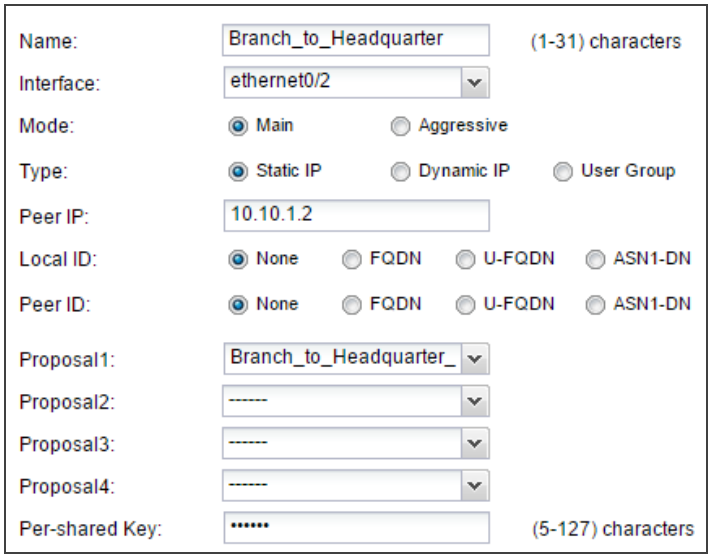
Select **Network > VPN > IPSec VPN**, under the P2 Proposal tab, click **New**.



- Proposal Name: Branch_to_Headquarter_P2
- Authentication: ESP
- Hash: SHA
- Encryption: 3DES

3. Configuring VPN peer

Select **Network > VPN > IPSec VPN**, under the VPN Peer List tab, click **New**.



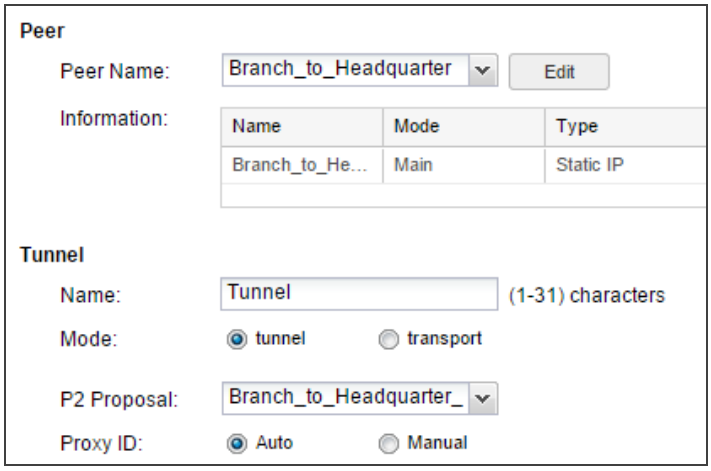
- Name: Branch_to_Headquarter
- Interface: ethernet0/2
- Mode: Main
- Type: Static IP
- Peer IP: 10.10.1.2
- Proposal 1:Branch_to_Headquarter_P1
- Pre-share Key: 123456

Step 3: Configuring IPSec VPN

4. Configuring IKE VPN

Select **Network > VPN > IPSec VPN**, under the IKE VPN List tab, click **New**.

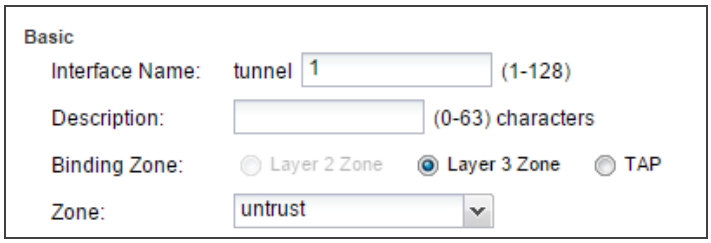
- Peer Name: Branch_to_Headquarter
- Tunnel Name: Tunnel
- Mode: tunnel
- P2 Proposal: Branch_to_Headquarter_P2

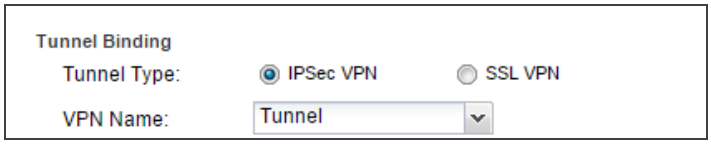


Step 4: Creating tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

- Basic
  - Name: 1
  - Zone: untrust
- Tunnel Binding
  - Tunnel Type: IPSec VPN
  - VPN Name: Tunnel

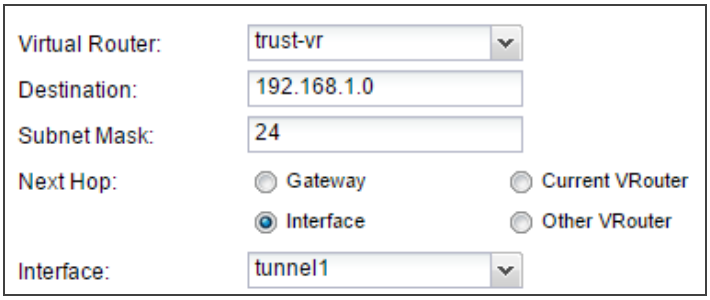




Step 5: Configuring route

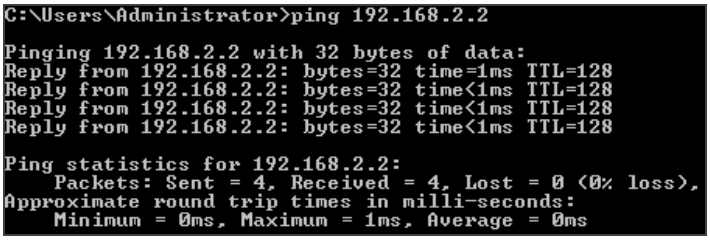
Select **Network > Routing > Destination Routing**, and click **New**.

- Destination: 192.168.1.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel1



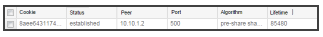
Step 6: Results

Use PC1 in the headquarters to ping PC2 in the branch. It works.



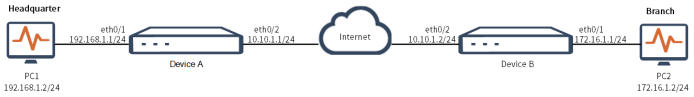
Step 7: Check if IPSec VPN tunnel has been established

Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <ISAKMP SA> tab and under the IPSec SA tab, you will see the status of the tunnel.



Connection between Two Private Networks Using IPSec VPN (IKEv2)

This example tells how to create IPSec VPN (IKEv2)tunnels to encrypt and protect the communication between two private networks . Usually, IPSec VPN tunnel is to connect the Device A in a branch office and the Device B in the headquarters.



*** Note:** This topology uses laboratory environment. In this recipe, 10.10.1.0/24 represents public network.

Configuration Steps

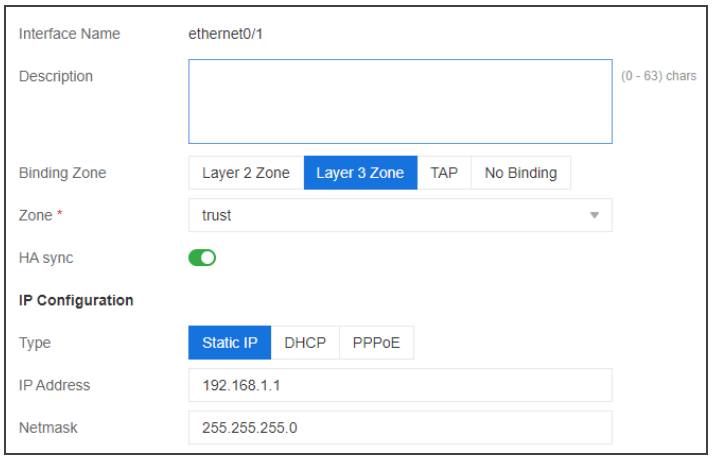
Device A

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

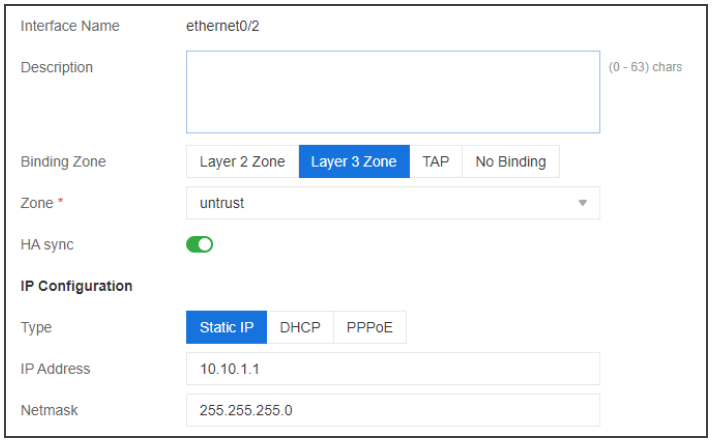
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0



Step 1: Configuring interface

2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.



- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0

Step 2: Configuring trust domain and import certificate

1. Creating a trust domain

Select **System > Trust Domain**, and click **New**.

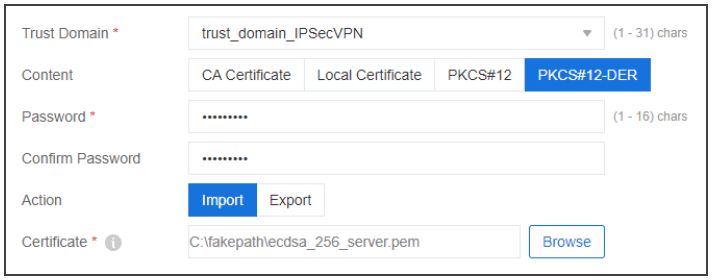


- Trust Domain: trust_domain_IPSecVPN
- Enrollment Type: Manual Input

Step 2: Configuring trust domain and import certificate

2. Importing a trust domain certificate

Select **System > Trust Domain Certificate**, and click **New**.

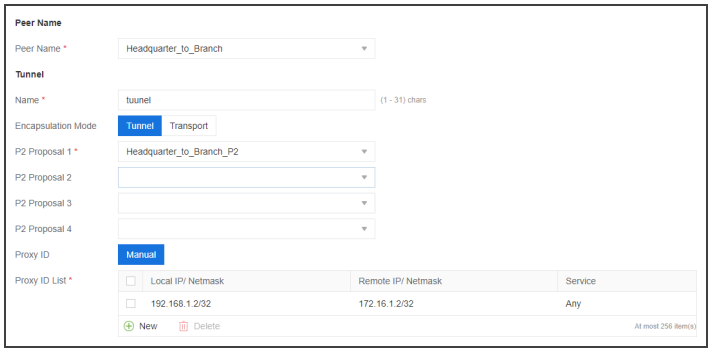


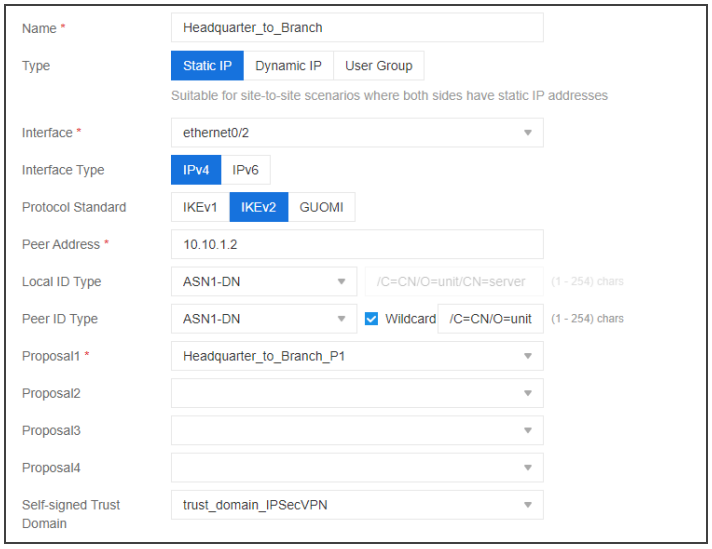
- Trust Domain: trust_domain_IPSecVPN
- Content: PKCS#12-DER
- Password: hillstone
- Confirm Password: hillstone
- Action: Import
- Certificate: Click **Browse** to select local certificate.

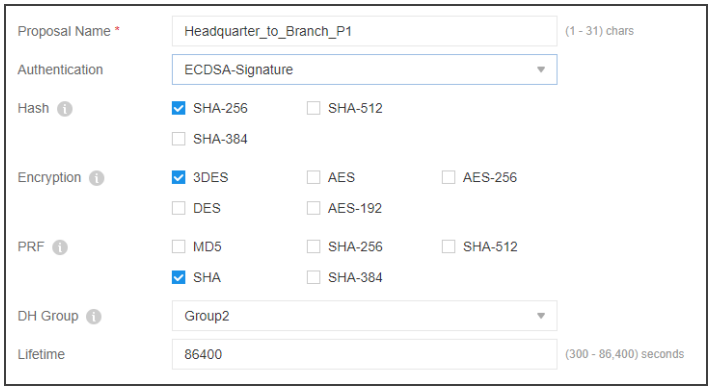
Step 3: Configuring IPSec VPN

Select **Network > VPN > IPSec VPN**, click **New**.

- Peer Name: click ⊕ button to configure VPN peer in the drop-down list.
  - Name: Headquarter_to_Branch
  - Type: Static IP
  - Interface: ethernet0/2
  - Protocol Standard: IKEv2
  - Peer Address: 10.10.1.2
  - Local ID Type: ASN1-DN
  - Peer ID Type: ASN1-DN, Wildcard: /C=CN/-/O=unit/CN=client
  - Proposal1: click ⊕ button to configure P1 proposal for IKE SA in the drop-down list.
    - Proposal Name: Headquarter_to_Branch_P1
    - Authentication: ECDSA-Signature
    - Hash: SHA-256
    - Encryption: 3DES
    - DH Group: Group2
  - Self-signed Trust Domain: trust_domain_IPSecVPN
- Name: tunnel

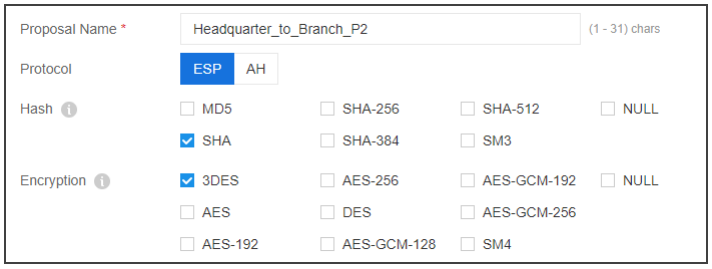






Step 3: Configuring IPSec VPN

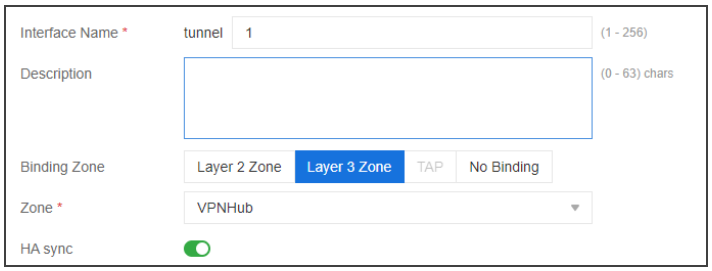
- Encapsulation Mode: Tunnel
- P2 Proposal: click ⊕ button to configure P2 proposal for IPSec SA in the drop-down list.
  - Proposal Name: Headquarter_to_Branch_P2
  - Protocol: ESP
  - Hash: SHA
  - Encryption: 3DES
- Proxy ID: Click **New** to configure proxy ID.
  - Local IP/Netmask: 192.168.1.2/32
  - Remote IP/Netmask: 172.16.1.2/32
  - Service: Any

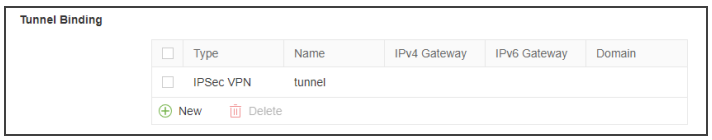


Step 4: Configuring tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

- Interface Name: 1
- Zone: VPNHub
- Tunnel Binding
  - Type: IPSec VPN
  - Name: tunnel

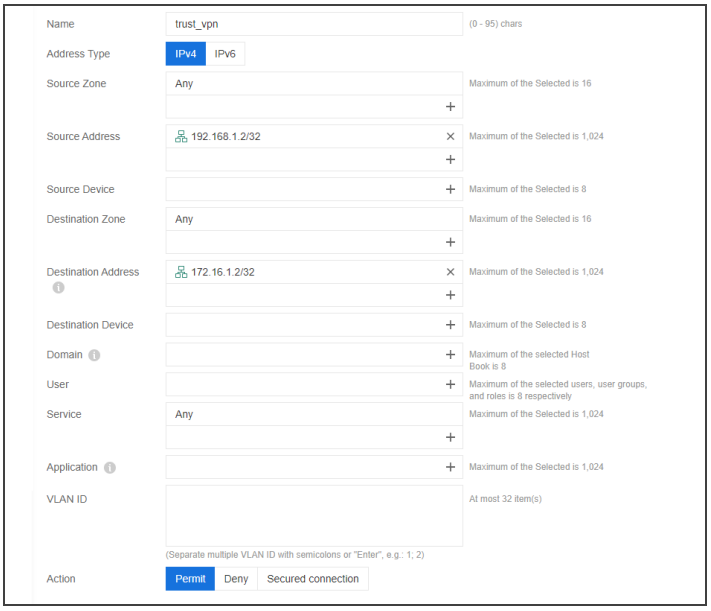




Step 5: Configuring security policies

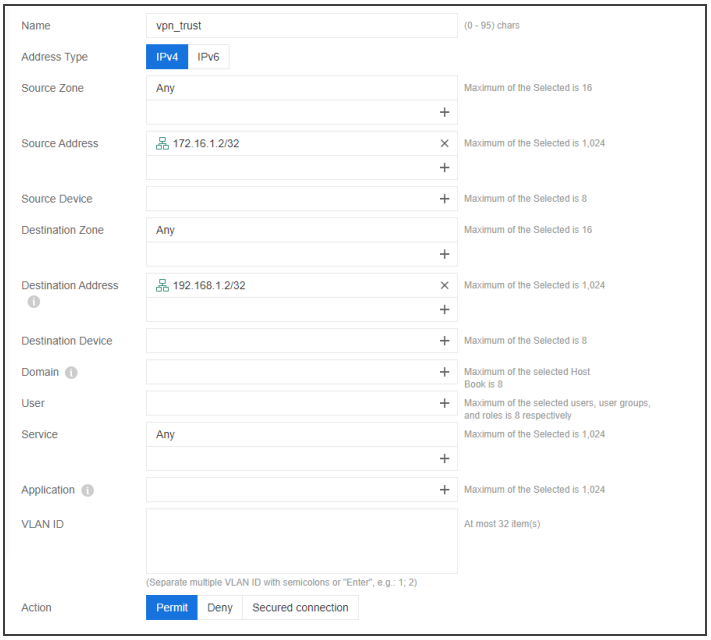
Select **Policy > Security Policy**, and click **New**.

- Name: trust_vpn
- Source Address: 192.168.1.2/32
- Destination Address: 172.16.1.2/32
- Action: Permit



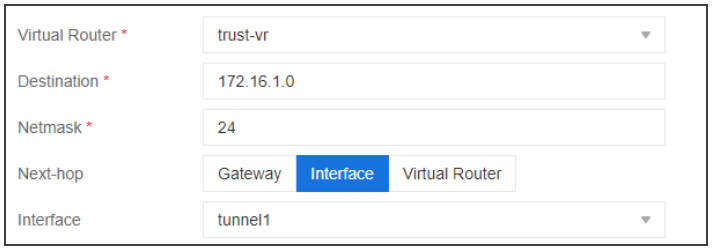
Select **Policy > Security Policy**, and click **New**.

- Name: vpn_trust
- Source Address: 172.16.1.2/32
- Destination Address: 192.168.1.2/32
- Action: Permit



Step6: Configuring route

Select **Network > Routing > Destination Routing**, and click **New**.



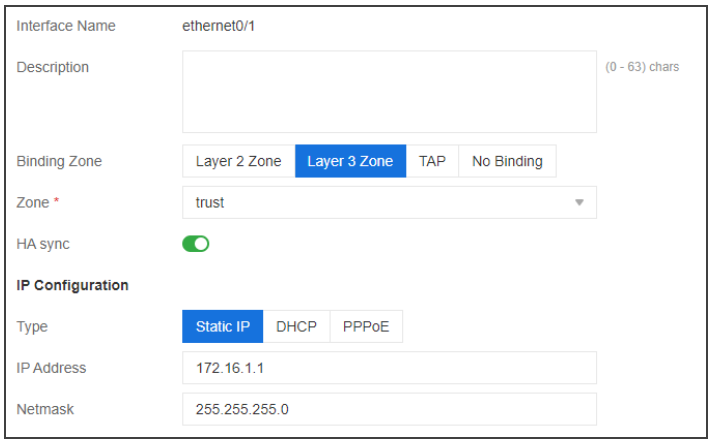
- Destination: 172.16.1.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel1

Device B

Step 1: Configuring interface

1. Configuring the interface connected to private network

Select **Network > Interface**, and double click ethernet0/1.

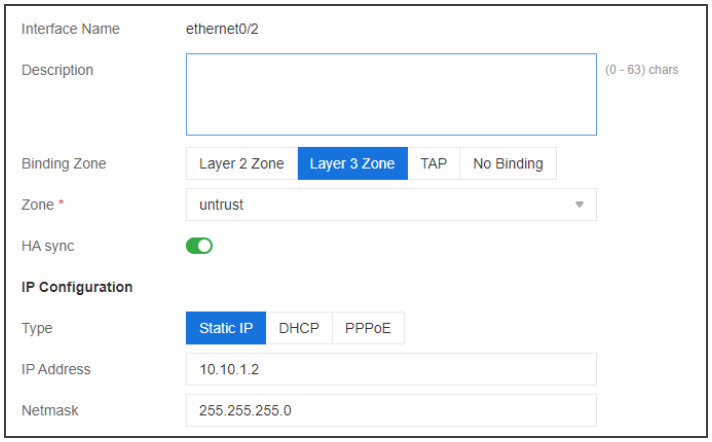


- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 172.16.1.1
- Netmask: 255.255.255.0

Step 1: Configuring interface

2. Configuring the interface connected to Internet

Select **Network > Interface**, and double click ethernet0/2.



- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.2
- Netmask: 255.255.255.0

Step 2: Configuring trust domain and import certificate

1. Creating a trust domain

Select **System > Trust Domain**, and click **New**.

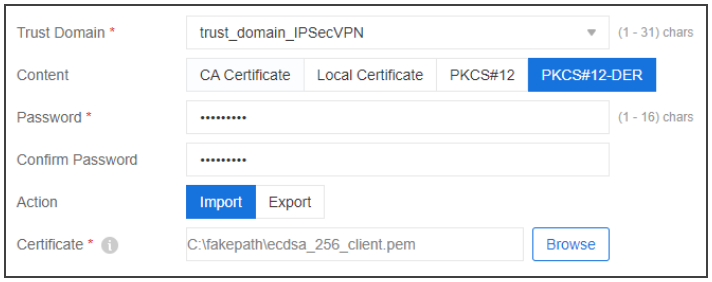


- Trust Domain: trust_domain_IPSecVPN
- Enrollment Type: Manual Input

Step 2: Configuring trust domain and import certificate

2. Importing a trust domain certificate

Select **System > Trust Domain Certificate**, and click **New**.

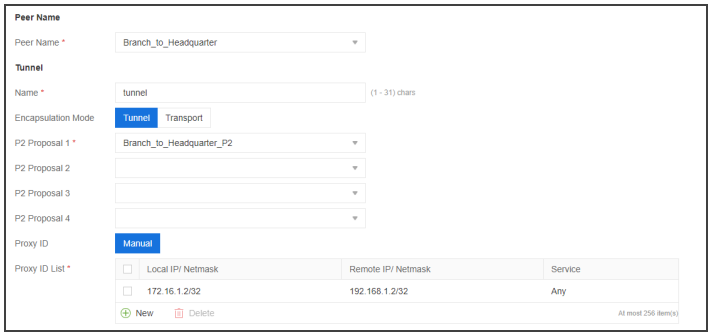


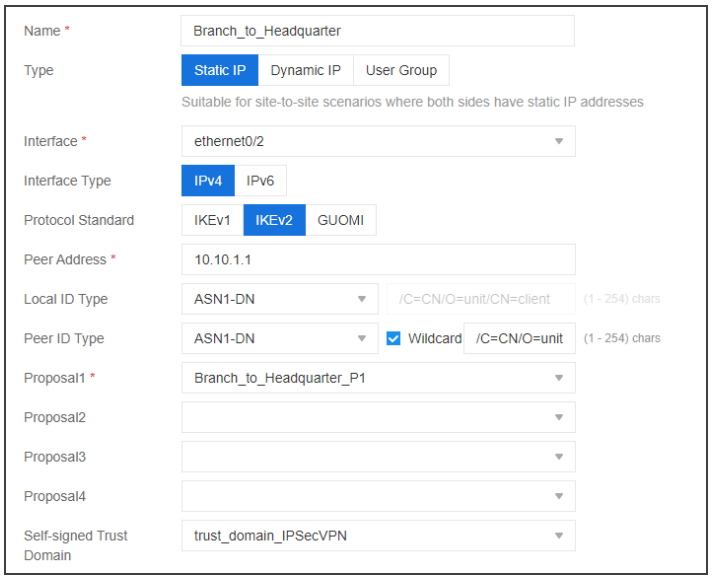
- Trust Domain: trust_domain_IPSecVPN
- Content: PKCS#12-DER
- Password: hillstone
- Confirm Password: hillstone
- Action: Import
- Certificate: Click **Browse** to select local certificate.

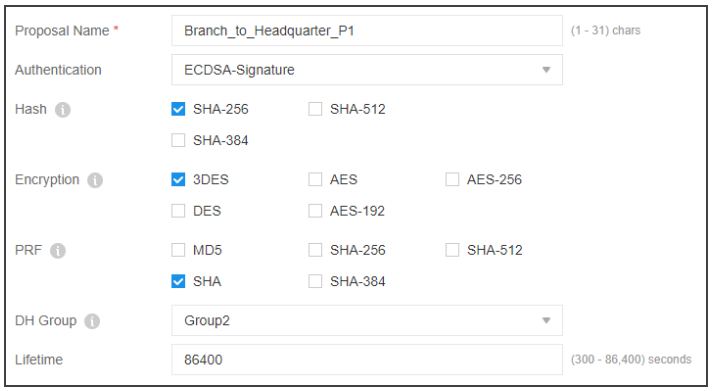
Step 3: Configuring IPSec VPN

Select **Network > VPN > IPSec VPN**, click **New**.

- Peer Name: click ⊕ button to configure VPN peer in the drop-down list.
  - Name: Branch_to_Headquarter
  - Type: Static IP
  - Interface: ethernet0/2
  - Protocol Standard: IKEv2
  - Peer Address: 10.10.1.1
  - Local ID Type: ASN1-DN
  - Peer ID Type: ASN1-DN, Wildcard: /C=CN/-/O=unit/CN=client
  - Proposal1: click ⊕ button to configure P1 proposal for IKE SA in the drop-down list.
    - Proposal Name: Branch_to_Headquarter_P1
    - Authentication: ECDSA-Signature
    - Hash: SHA-256
    - Encryption: 3DES
    - DH Group: Group2
  - Self-signed Trust Domain: trust_domain_IPSecVPN
- Name: tunnel

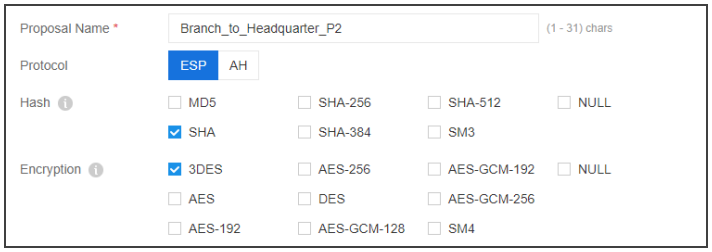






Step 3: Configuring IPSec VPN

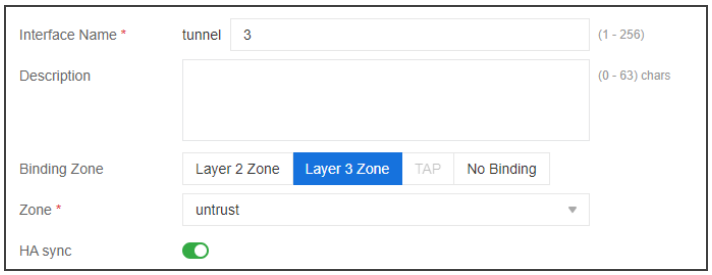
- Encapsulation Mode: Tunnel
- P2 Proposal: click ⊕ button to configure P2 proposal for IPSec SA in the drop-down list.
  - Proposal Name: Branch_to_Headquarter_P2
  - Protocol: ESP
  - Hash: SHA
  - Encryption: 3DES
  - Proxy ID: Click New to configure proxy ID.
    - Local IP/Netmask: 172.16.1.2/32
    - Remote IP/Netmask: 192.168.1.2/32
    - Service: Any



Step 4: Configuring tunnel interface

Select **Network > Interface**, and click **New > Tunnel Interface**.

- Interface Name: 3
- Zone: untrust
- Tunnel Binding
  - Type: IPSec VPN
  - Name: tunnel

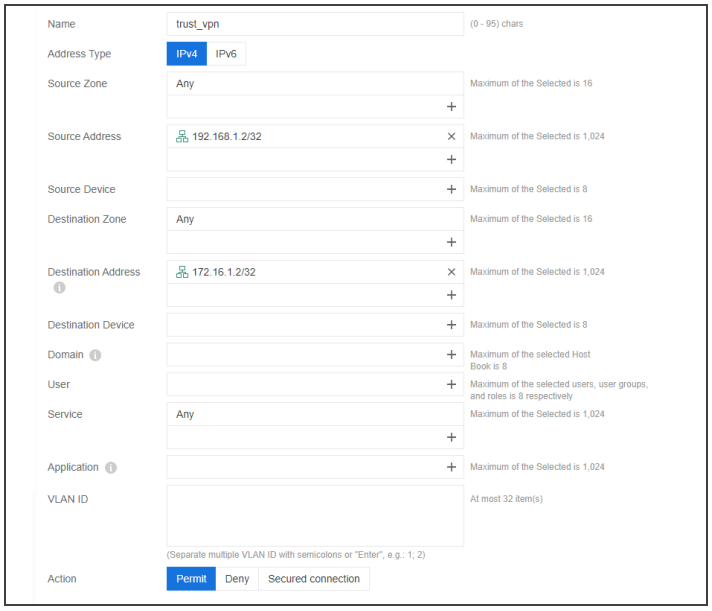




Step 5: Configuring security policies

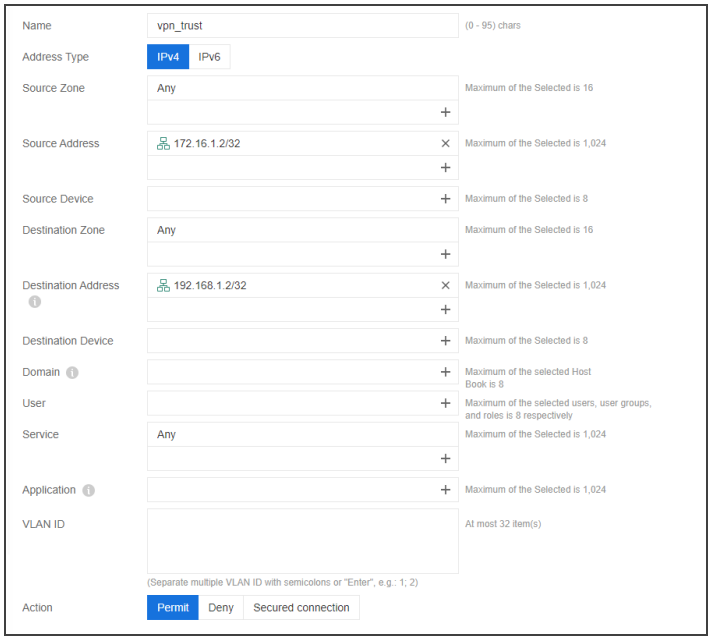
Select **Policy > Security Policy**, and click **New**.

- Name: trust_vpn
- Source Address: 192.168.1.2/32
- Destination Address: 172.16.1.2/32
- Action: Permit



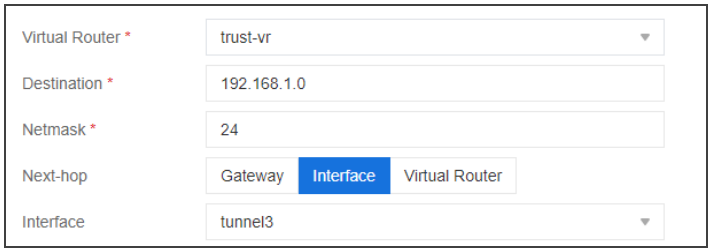
Select **Policy > Security Policy**, and click **New**.

- Name: vpn_trust
- Source Address: 172.16.1.2/32
- Destination Address: 192.168.1.2/32
- Action: Permit



Step 6: Configuring route

Select **Network > Routing > Destination Routing**, and click **New**.

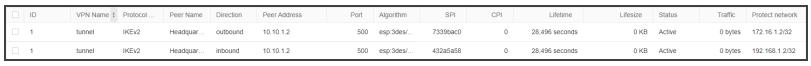


- Destination: 192.168.1.0
- Subnet Mask: 24
- Next Hop: Interface
- Interface: tunnel13

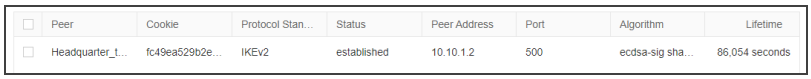
Step 7: Check if IPSec VPN tunnel has been established

Use PC1 in the headquarters to ping PC2 in the branch. It works.

Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <ISAKMP SA> tab tab, you will see the status of the tunnel.



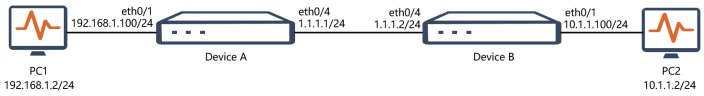
选择“网络 > VPN > IPSec VPN > IPSec VPN监控 > IPSec SA”，可以看到IPsec VPN第二阶段已经成功建立。Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <IPSec SA> tab, you will see the status of the tunnel.



Establishment of IPSec VPN Based on Certificate Authentication

This example introduces how to establish IPSec VPN tunnels based on certificate authentication to improve communication security.

As shown in the figure below, an IPsec VPN security tunnel based on certificate authentication is established between Device A and Device B. PC1 is the host of Device A, and PC2 is the host of Device B. It is required to protect the data flow between the subnet (192.168.1.0/24) represented by PC1 and the subnet (10.1.1.0/24) represented by PC2. RSA Signature is used for authentication, ESP protocol is used for security protocol, SHA is adopted for Hash algorithm, 3DES is adopted for encryption algorithm, so as to ensure the integrity and security of communication data.



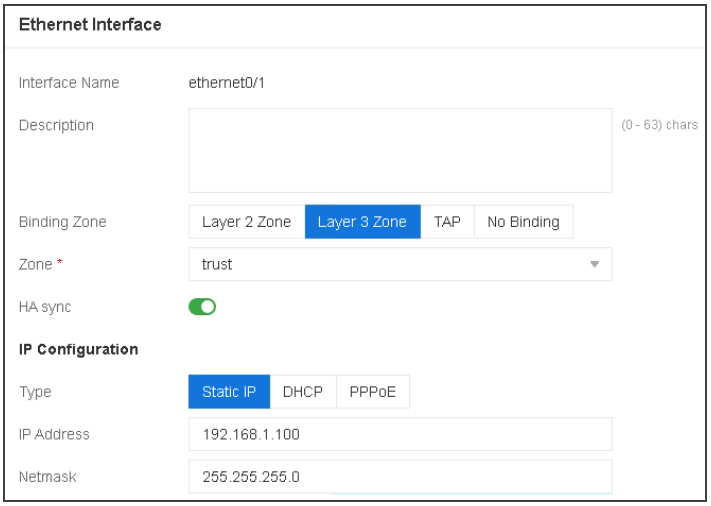
Configuration Steps

Device A

Step 1: Configuring interface

Select **Network > Interface**, and double click ethernet0/1.

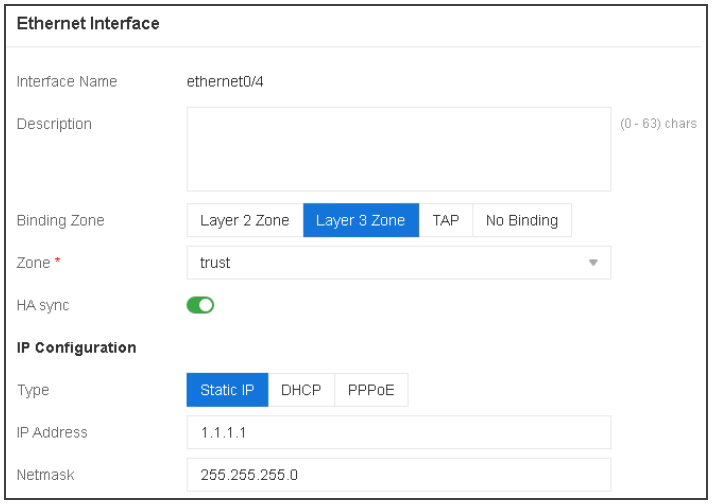
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0



Step 1: Configuring interface

Select **Network > Interface**, and double click ethernet0/4.

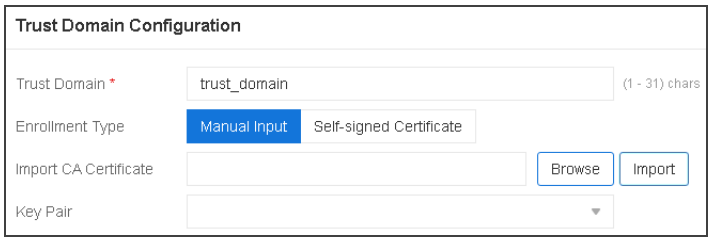
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address： 1.1.1.1
- Netmask: 255.255.255.0



Step 2: Configuring the trust domain and importing the authentication certificate

Select **System > PKI > Trust Domain**, and click **New**.

- Trust Domain: trust_domain
- Enrollment Type: Manual Input

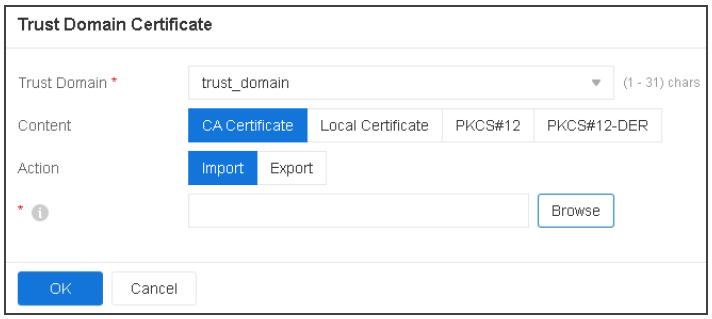


Select **System > PKI > Trust Domain Certificate**.

- Trust Domain: trust_domain
- Content: Select "CA Certificate" and "Local Certificate" respectively

  Tip: If the certificate is in ". p12" format, please select "PKCS#12-DER".

- Action: Import. Click **Browse** and select the local certificate of Device A and the CA certificate of Device B to be imported from the local PC.

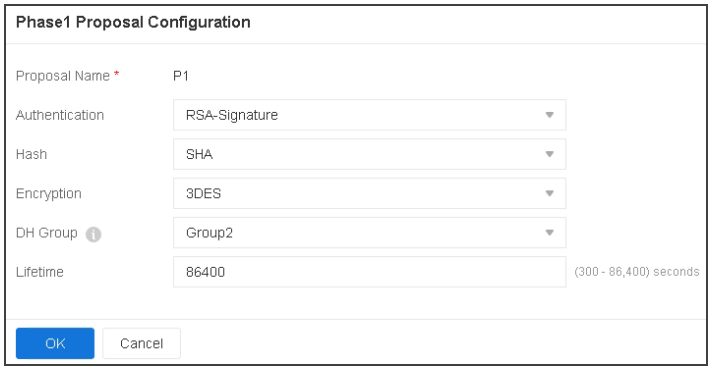


Step 3: Configuring IPSec VPN

1.Configuring Phase 1 Proposal.

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **Peer Name** drop-down list, then on the **VPN Peer Configuration** page, and click the button ⊕ in the **Proposal1** drop-down list.

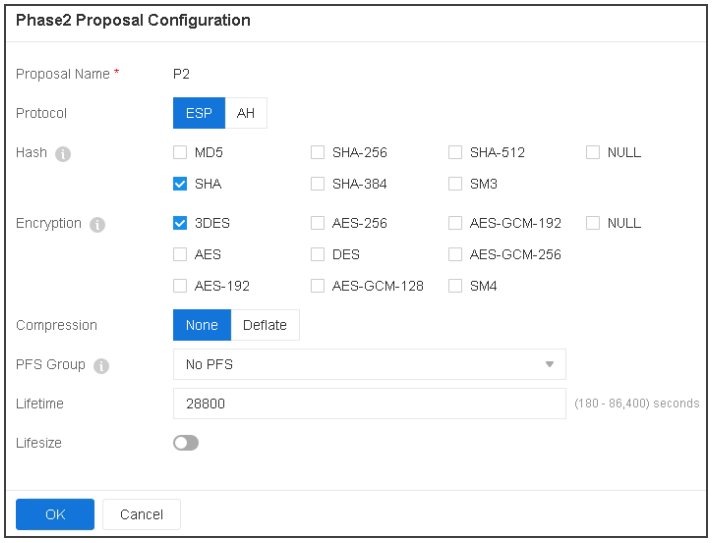


- Proposal Name: P1
- Authentication: RSA-Signature
- Hash: SHA
- Encryption: 3DES
- DH group: Group2

2.Configuring Phase 2 Proposal.

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **P2 Proposal** drop-down list.



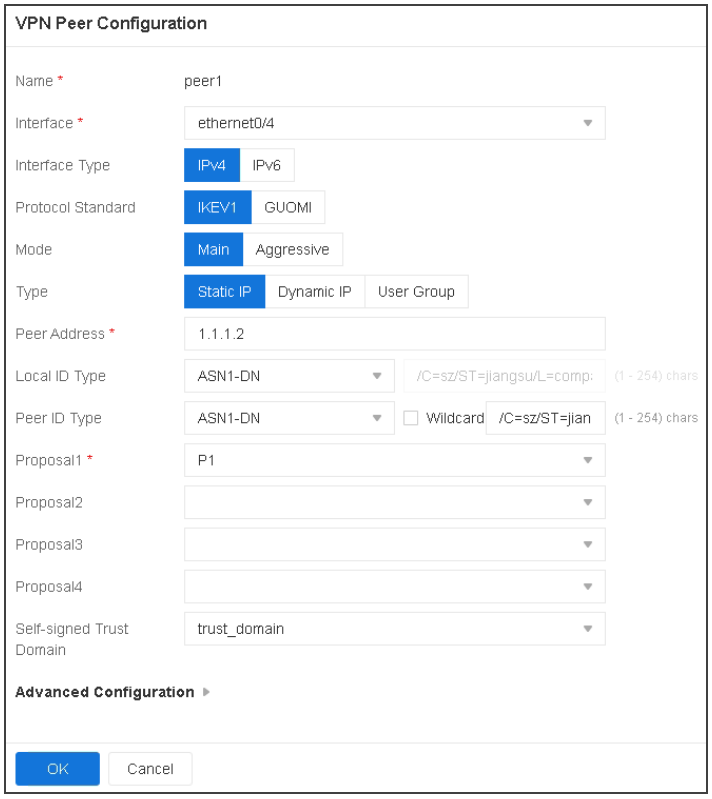
- Proposal Name: P2
- Protocol: ESP
- Hash: SHA
- Encryption: 3DES

Step 3: Configuring IPSec VPN

3.Configuring peer

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **Peer Name** drop-down list.

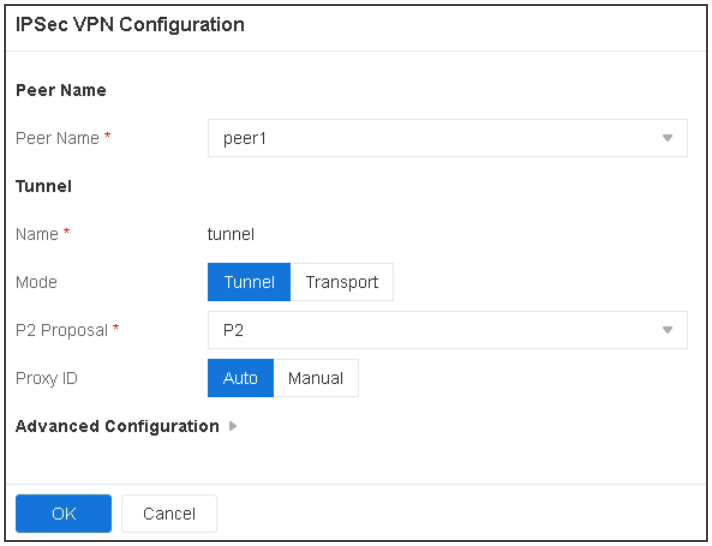


- Name: peer1
- Interface: ethernet0/4
- Interface Type: IPv4
- Protocol Standard: IKEV1
- Mode: Main
- Type: Static IP
- Peer Address: 1.1.1.2
- Local ID Type: ASN1-DN
- Peer ID Type: ASN1-DN，peer ID value is the "Subject" name of the local certificate on the peer device, which needs to be obtained from the peer device.
- Proposal1: P1
- Self-signed Trust Domain: trust_domain

Step 4: Configuring a tunnel instance

Select **Network > VPN > IPSec VPN**, and click **New**.

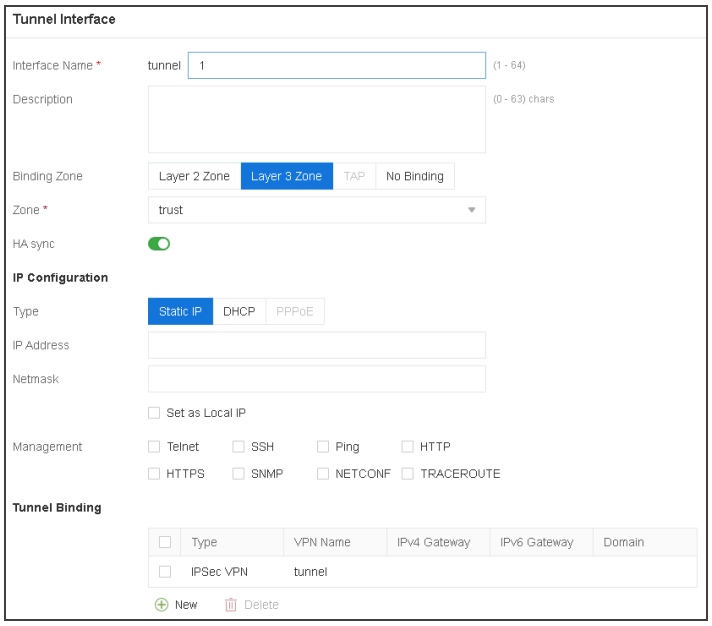
- Peer Name
  - Peer Name: peer1
- Tunnel
  - Name: tunnel
  - Mode: Tunnel
  - P2 Proposal: P2
  - Proxy ID: Auto



Step 5: Configuring a tunnel interface and binding it to the tunnel instance

Select **Network > Interface**, click **New** and select **Tunnel Interface**

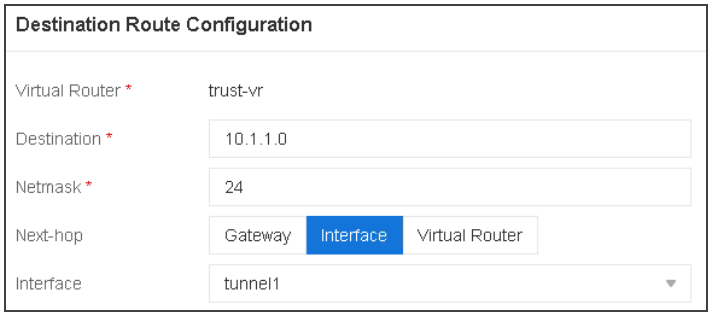
- Basic
  - Interface Name: 1
  - Binding Zone: Layer 3 Zone
  - Zone: trust
- Tunnel Binding
  - Type: IPSec VPN
  - VPN Name: tunnel



Step 6: Configuring a tunnel route

Select **Network > Routing > Destination Route**, and click **New**.

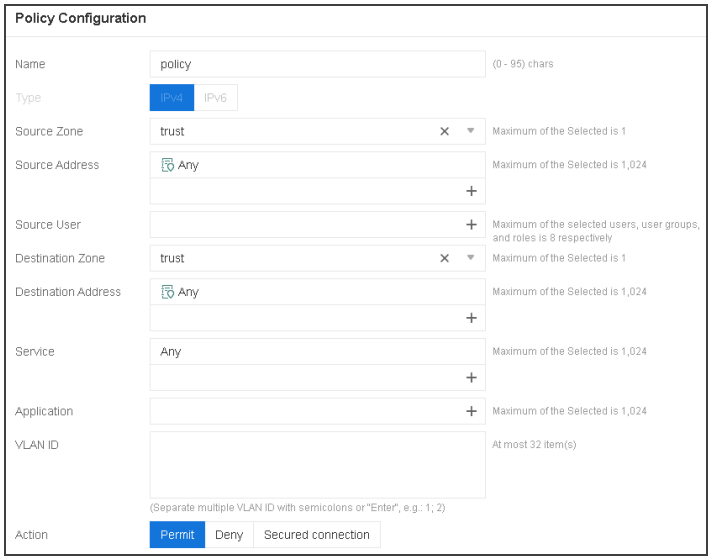
- Virtual Router: trust-vr
- Destination: 10.1.1.0
- Netmask: 24
- Next-hop: Interface
- Interface: tunnel1



Step 7: Configuring a security policy

Select **Policy > Security Policy > Policy**, and click **New**.

- Name: policy
- Source Zone: trust
- Source Address: Any
- Destination Zone: trust
- Destination Address: Any
- Service: Any
- Action: Permit

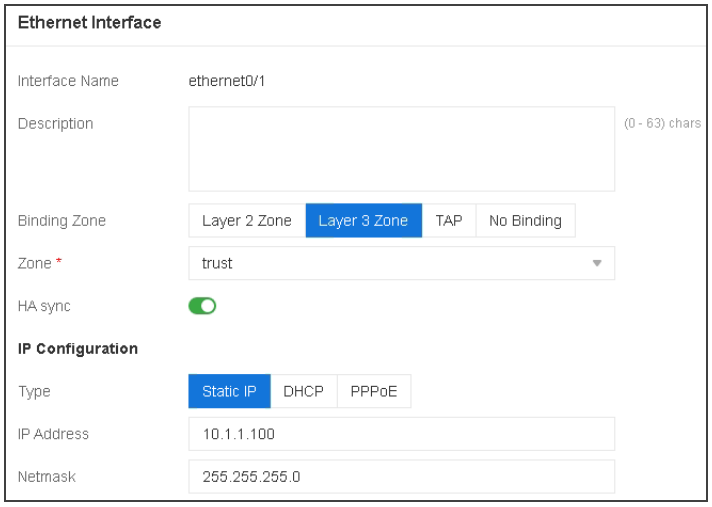


Device B

Step 1: Configuring interface

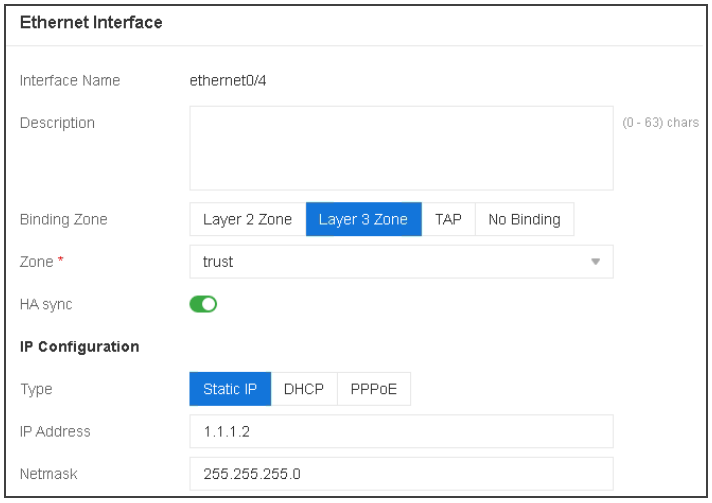
Select **Network > Interface**, and double click ethernet0/1.

- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 10.1.1.100
- Netmask: 255.255.255.0



Select **Network > Interface**, and double click ethernet0/4.

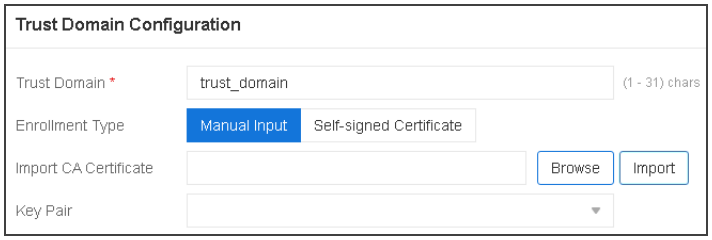
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address： 1.1.1.2
- Netmask: 255.255.255.0



Step 2: Configuring the trust domain and importing the authentication certificate

Select **System > PKI > Trust Domain**, and click **New**.

- Trust Domain: trust_domain
- Enrollment Type: Manual Input

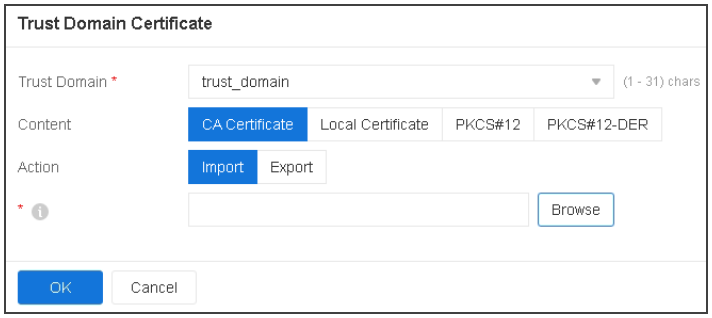


Select **System > PKI > Trust Domain Certificate**.

- Trust Domain: trust_domain
- Content: Select "CA Certificate" and "Local Certificate" respectively

  Tip: If the certificate is in ". p12" format, please select "PKCS#12-DER".

- Action: Import. Click **Browse** and select the local certificate of Device B and the CA certificate of Device A to be imported from the local PC.

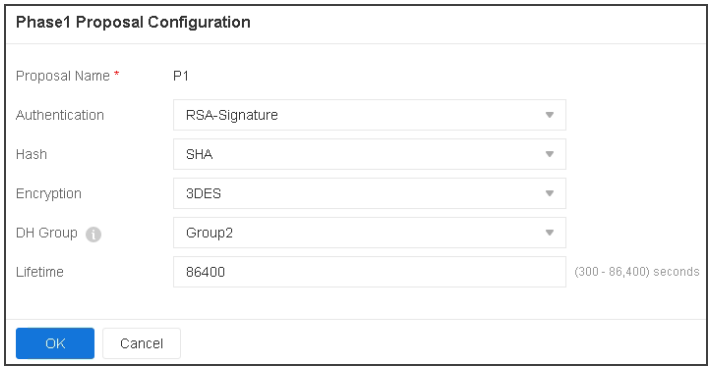


Step 3: Configuring IPSec VPN

1.Configuring Phase 1 Proposal

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **Peer Name** drop-down list, then on the **VPN Peer Configuration** page, and click the button ⊕ in the **Proposal1** drop-down list.

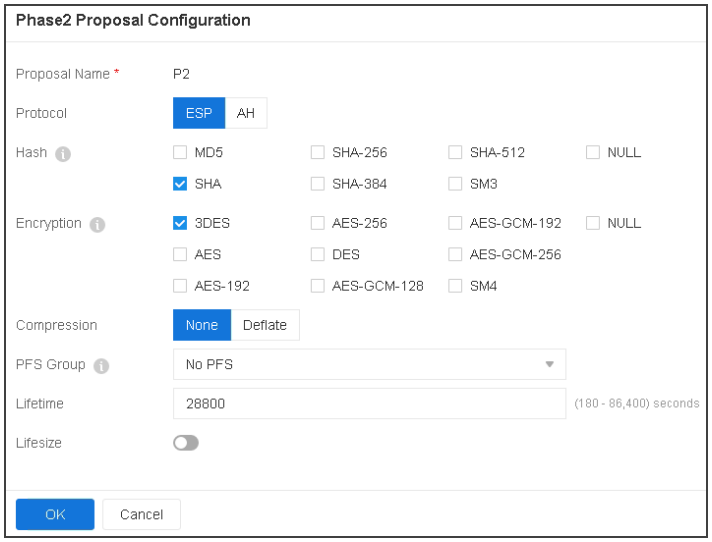


- Proposal Name: P1
- Authentication: RSA-Signature
- Hash: SHA
- Encryption: 3DES
- DH group: Group2

2.Configuring Phase 1 Proposal

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **P2 Proposal** drop-down list.



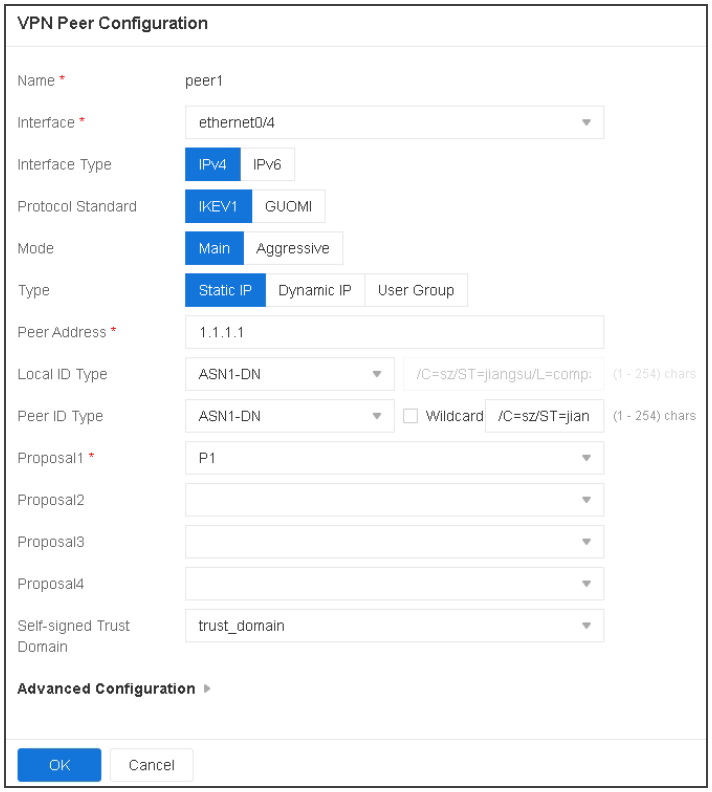
- Proposal Name: P2
- Protocol: ESP
- Hash: SHA
- Encryption: 3DES

Step 3: Configuring IPSec VPN

3.Configuring Peer

Select **Network > VPN > IPSec VPN**, and click **New**.

On the **IPSec VPN Configuration** page, click the button ⊕ in the **Peer Name** drop-down list.

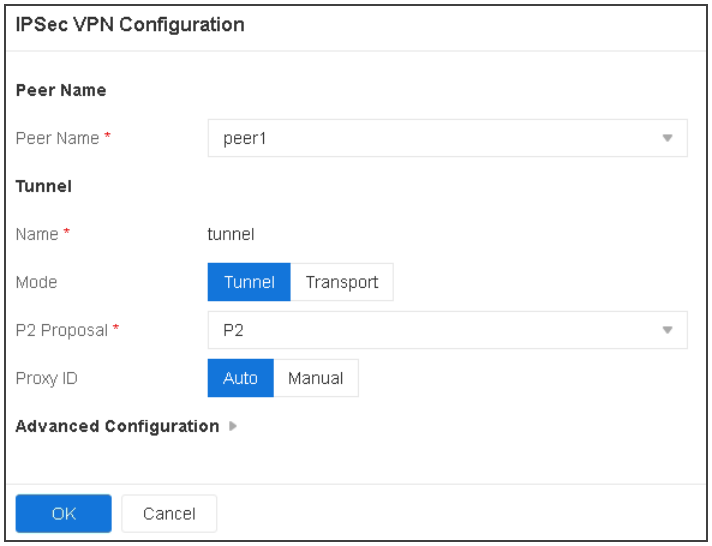


- Name: peer1
- Interface: ethernet0/4
- Interface Type: IPv4
- Protocol Standard: IKEV1
- Mode: Main
- Type: Static IP
- Peer Address: 1.1.1.1
- Local ID Type: ASN1-DN
- Peer ID Type: ASN1-DN， peer ID value the "Subject" name of the local certificate on the peer device, which needs to be obtained from the peer device.
- Proposal1: P1
- Self-signed Trust Domain: trust_domain

Step 4: Configuring a tunnel instance

Select **Network > VPN > IPSec VPN**, and click **New**.

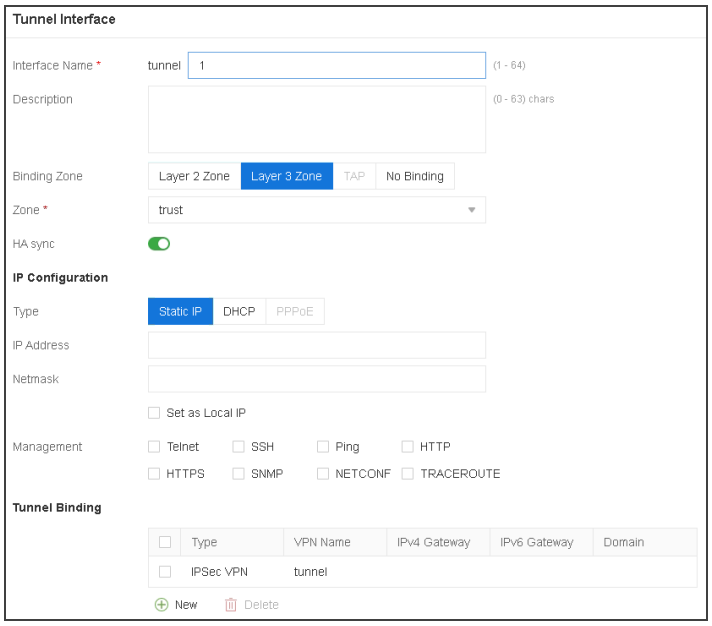
- Peer Name
  - Peer Name: peer1
- Tunnel
  - Name: tunnel
  - Mode: Tunnel
  - P2 Proposal: P2
  - Proxy ID: Auto



Step 5: Configuring a tunnel interface and binding it to the tunnel instance

Select **Network > Interface**, click **New** and select **Tunnel Interface**

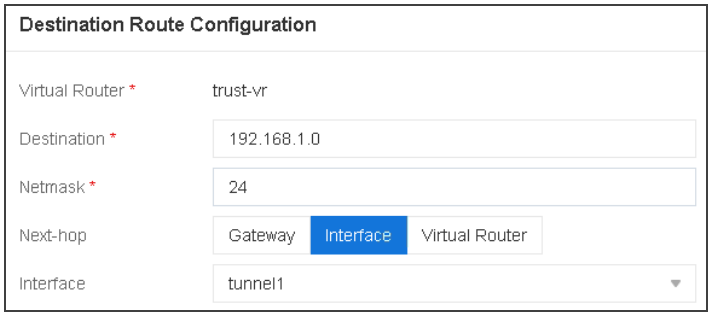
- Basic
  - Interface Name: 1
  - Binding Zone: Layer 3 Zone
  - Zone: trust
- Tunnel Binding
  - Type: IPSec VPN
  - VPN Name: tunnel



Step 6: Configuring a tunnel route

Select **Network > Routing > Destination Route**, and click **New**.

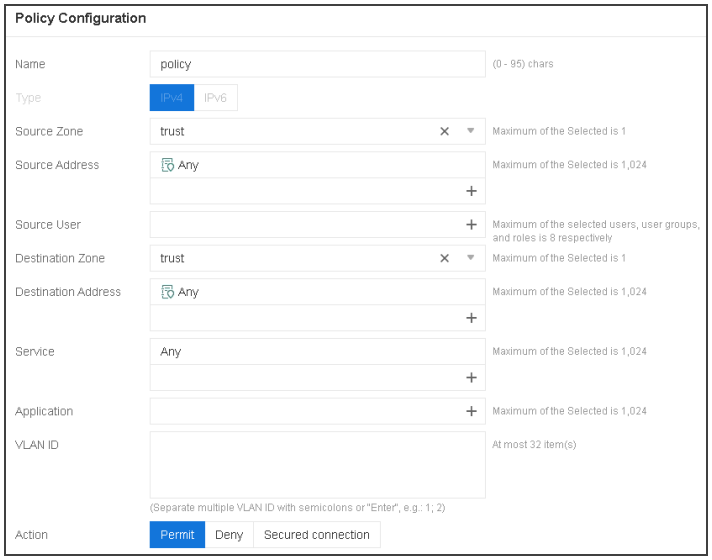
- Virtual Router: trust-vr
- Destination: 192.168.1.0
- Netmask: 24
- Next-hop: Interface
- Interface: tunnel1



Step 7: Configuring a security policy

Select **Policy > Security Policy > Policy**, and click **New**.

- Name: policy
- Source Zone: trust
- Source Address: Any
- Destination Zone: trust
- Destination Address: Any
- Service: Any
- Action: Permit



Step 8: Check if the network has been interconnected

After the above configuration steps are completed, PC1 and PC2 can ping each other, indicating that the networks between them has been interconnected.

```
root@hillstone:~# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2) 56(84) bytes of data.
64 bytes from 10.1.1.2: icmp_seq=1 ttl=62 time=1.81 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=62 time=1.62 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=62 time=1.77 ms
64 bytes from 10.1.1.2: icmp_seq=4 ttl=62 time=1.41 ms
^C
--- 10.1.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.417/1.656/1.810/0.155 ms
```

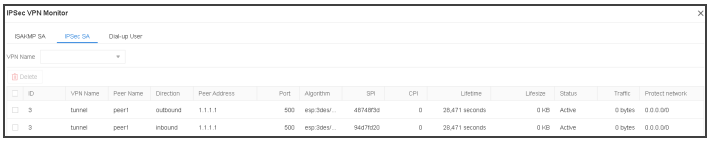
```
root@hillstone:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=62 time=1.72 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=62 time=3.58 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=62 time=1.65 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=62 time=1.77 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.655/2.183/3.587/0.813 ms
```

Step 9: Check if IPSec VPN tunnel has been established

Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <ISAKMP SA> tab, it can be seen that the phase 1 of IPSec VPN has been successfully established.



Go to **Network > VPN > IPSec VPN**, and click **IPSec VPN Monitor** on the top right corner, under the <IPSec SA> tab, it can be seen that the phase 2 of IPSec VPN has been successfully established.



Realizing Dynamic Switch between IPSec Links Using IPSec VPN Smart Link

This example tells how to configure IPSec VPN smart link to realize dynamic switch between IPSec links.

As shown in the figure below, IPSec VPN tunnel is to connect the Device A in a branch office and the Device B in the headquarter. If the packet loss rate or latency of the tunnel that is established based on Link1 exceeds the specified threshold, the system would switch to Link2 to establish a new IPSec VPN tunnel. ESP protocol is used for security protocol, SHA-256 is adopted for Hash algorithm, AES-256 is adopted for encryption algorithm, so as to ensure the integrity and security of communication data.



Configuration Steps

Device A

Step 1: Configuring interface

```
1.Configuring the interface connected to private network.
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 173.16.1.1/24
hostname(config-if-eth0/1)# exit
2.Configuring the interface connected to Internet.
hostname(config)# interface xethernet3/0
hostname(config-if-xe3/0)# zone untrust
hostname(config-if-xe3/0)# ip address 1.1.1.1/24
hostname(config-if-xe3/0)# exit
```

Step 2: Configuring an AAA server and pre-shared key

```
hostname(config)# aaa-server local type local

hostname(config-aaa-server)# user test1

hostname(config-user)# ike-id fqdn client1

hostname(config-user)# exit

hostname(config-aaa-server)# exit

hostname(config)# exit

hostname# exec generate-user-key rootkey hillstone1 userid client1

userkey: OG64Mk1CPfRLKou3yCwOehMLfQw=
```

Step 3: Configuring IPSec VPN

```
1.Configuring P1 proposal.
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# hash sha256
hostname(config-isakmp-proposal)# encryption aes-256
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# exit
2.Configuring P2 proposal.
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha256
hostname(config-ipsec-proposal)# encryption aes-256
hostname(config-ipsec-proposal)# exit
3. Configuring ISAKMP peer. You are suggested to enable DPD function to
avoid that the old SA cannot be cleared in time after the link switch.
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# type usergroup
hostname(config-isakmp-peer)# local-id fqdn server1
hostname(config-isakmp-peer)# aaa-server local
hostname(config-isakmp-peer)# interface xethernet3/0
hostname(config-isakmp-peer)# pre-share hillstone1
hostname(config-isakmp-peer)# nat-traversal
hostname(config-isakmp-peer)# generate-route
```

```
hostname(config-isakmp-peer)# dpd

hostname(config-isakmp-peer)# exit
```

Step 4: Creating IPsec VPN tunnel

```
hostname(config)# tunnel ipsec vpn1 auto

hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2

hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1

hostname(config-tunnel-ipsec-auto)# id local 173.16.1.0/24 remote
173.15.1.0/24 service any

hostname(config-tunnel-ipsec-auto)# exit
```

Step 5 : Creating the tunnel interface to the IPsec VPN tunnel

```
hostname(config)# interface tunnel1

hostname(config-if-tun1)# zone trust

hostname(config-if-tun1)# tunnel ipsec vpn1

hostname(config-if-tun1)# exit
```

Step 6: Configuring security policies

```
hostname(config)# rule from 173.16.1.0/24 to 173.15.1.0/24 service any per-
mit
```

Device B

Step 1: Configuring interface.

```
1.Configuring the interface connected to private network.
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 173.15.1.1/24
hostname(config-if-eth0/1)# exit
2.Configuring the interface connected to Internet.
hostname(config)# interface xethernet0/2.1
hostname(config-if-xe0/2.1)# zone untrust
hostname(config-if-xe0/2.1)# ip address 191.1.101.1/24
hostname(config-if-xe0/2.1)# exit
hostname(config)# interface xethernet0/2.2
hostname(config-if-xe0/2.2)# zone untrust
hostname(config-if-xe0/2.2)# ip address 191.1.102.1/24
hostname(config-if-xe0/2.2)# exit
```

Step 2: Configuring smart link rules

```
hostname(config)# ipsec smart-link profile smart_profile1
hostname(config-ipsec-smart-link-profile)# link 1 interface xethernet0/2.1
peer 1.1.1.1
hostname(config-ipsec-smart-link-profile)# link 2 interface xethernet0/2.2
peer 1.1.1.1
hostname(config-ipsec-smart-link-profile)# link-track-threshold delay 500
loss-rate 30
hostname(config-ipsec-smart-link-profile)# exit
```

Step 3: Configuring IPSec VPN

```
1.Configuring P1 proposal.
hostname(config)# isakmp proposal p1
hostname(config-isakmp-proposal)# hash sha256
hostname(config-isakmp-proposal)# encryption aes-256
hostname(config-isakmp-proposal)# group 2
hostname(config-isakmp-proposal)# exit
2.Configuring P2 proposal.
hostname(config)# ipsec proposal p2
hostname(config-ipsec-proposal)# protocol esp
hostname(config-ipsec-proposal)# hash sha256
hostname(config-ipsec-proposal)# encryption aes-256
hostname(config-ipsec-proposal)# exit
3. Configuring ISAKMP peer.
hostname(config)# isakmp peer peer1
hostname(config-isakmp-peer)# isakmp-proposal p1
hostname(config-isakmp-peer)# mode aggressive
hostname(config-isakmp-peer)# local-id fqdn client1
hostname(config-isakmp-peer)# peer-id fqdn server1
hostname(config-isakmp-peer)# pre-share OG64Mk1CPfRLKou3yCwOehMLfQw=
hostname(config-isakmp-peer)# nat-traversal
hostname(config-isakmp-peer)# generate-route
hostname(config-isakmp-peer)# exit
```

Step 4: Creating IPsec VPN tunnel .

```
hostname(config)# tunnel ipsec vpn1 auto
hostname(config-tunnel-ipsec-auto)# ipsec-proposal p2
hostname(config-tunnel-ipsec-auto)# isakmp-peer peer1
hostname(config-tunnel-ipsec-auto)# id local 173.15.1.0/24 remote
173.16.1.0/24 service any
hostname(config-tunnel-ipsec-auto)# smart-link-profile smart_profile1
hostname(config-tunnel-ipsec-auto)# auto-connect
hostname(config-tunnel-ipsec-auto)# exit
```

Step 5 : Binding the tunnel interface to the IPsec VPN tunnel.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# tunnel ipsec vpn1
hostname(config-if-tun1)# exit
```

Step 6: Configuring route

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 173.16.1.0/24 tunnel1
hostname(config-vrouter)# exit
```

Step 7: Configuring security policies

```
hostname(config)# rule from 173.15.1.0/24 to 173.16.1.0/24 service any per-
mit
```

Step 8: Check if IPSec VPN tunnel has been established

1.With the command **`show isakmp sa`**, you can see that the first phase of IPsec VPN has been successfully established.

```
hostname# show isakmp sa

Total: 1

L-time - Lifetime

================================================================================-
====

Cookies Gateway Port Algorithm Lifetime

--------------------------------------------------------------------------------
----

99933c2b~  1.1.1.1  500 pre-share sha256/aes-256 86388

================================================================================-
====
```

2.With the command **show ipsec sa**, you can see that the second phase of IPsec VPN has been successfully established.

```
hostname# show ipsec sa

Total: 1

S - Status, I - Inactive, A - Active;

================================================================================-
====

Id VPN Peer IP Port Algorithms SPI Life(s) S

--------------------------------------------------------------------------------
----

1 vpn1 >1.1.1.1 500 esp:aes-256/sha256 6ddafe72 27332 A

1 vpn1 <1.1.1.1 500 esp:aes-256/sha256 309c97c0 27332 A

================================================================================-
====
```

Step 9: When the packet loss rate or latency of the tunnel that is established based on Link1(191.1.101.1->1.1.1.1) exceeds the specified threshold, verify that the system can successfully switch to Link2(191.1.102.1->1.1.1.1) to establish a new IPSec VPN tunnel.

1.With the command **`show ipsec smart-link-profile smart_profile1`**, you can see that the Link1 is currently used to establish IPSec tunnel.

```
hostname(config)# show ipsec smart-link-profile smart_profile1

Total: 1

Status:I - Invalid, A - Active, C - Current negotiation link, * - Cycle
start link

==========================================================================-
====

Name: smart_profile1

Tunnel name: vpn1

Status: enable

Loss-rate(%): 30

Delay(ms): 500

Track-source: 191.1.101.1

Track-destination: 1.1.1.1

Track-interval(s): 3

Track-count: 10

Switch-cycles: 5

Switch-back-time(s): 600

Switched-count: 0

Switched-cycles: 0

Link-list:

Id interface local-ip peer-ip delay(ms) loss-rate(%) Status

1 xethernet0/2.1 191.1.101.1 1.1.1.1 1 0 *AC

2 xethernet0/2.2 191.1.102.1 1.1.1.1 0 0 I

==========================================================================-
====
```

2.When the packet loss rate or latency of the tunnel that is established based on Link1 exceeds the specified threshold, verify that the system can successfully switch to Link2 to establish a new IPSec VPN tunnel. With the command **`show ipsec smart-link-profile smart_profile1`**,you can see that the Link2 has been automatically switched to establish an IPSec tunnel.

```
2022-12-26 19:27:28, Event WARNING@VPN: IPSec smart link smart_profile1 is
switched from link1 to link2, because the time delay 509 is higher than the
threshold 500(IPSec Tunnel=vpn1, Loss Rate=0%, Time Delay=509ms).
hostname(config)# show ipsec smart-link-profile smart_profile1
Total: 1
Status:I - Invalid, A - Active, C - Current negotiation link, * - Cycle
start link
==========================================================================-
====
Name: smart_profile1
Tunnel name: vpn1
Status: enable
Loss-rate(%): 30
Delay(ms): 500
Track-source: 191.1.102.1
Track-destination: 1.1.1.1
Track-interval(s): 3
Track-count: 10
Switch-cycles: 5
Switch-back-time(s): 600
Switched-count: 1
Switched-cycles: 0
Link-list:
Id interface local-ip peer-ip delay(ms) loss-rate(%) Status
1 xethernet0/2.1 191.1.101.1 1.1.1.1 509 0 *I
```

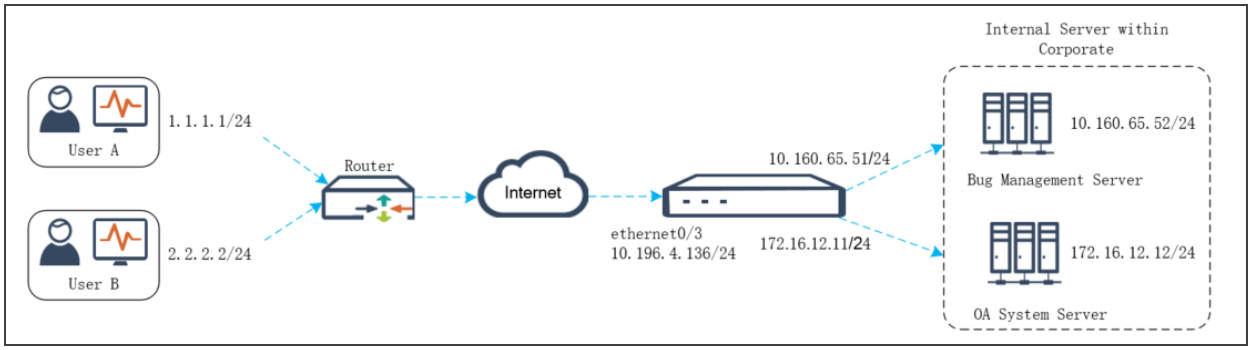
```
2 xethernet0/2.2 191.1.102.1 1.1.1.1 0 0 AC

================================================================================-

===
```

Allowing Remote Users to Access a Private Network Using SSL VPN

This example shows how to use SSL VPN to provide remote users with access to corporate internal network.

Networking Scenario

The topology describes remote users A and B on the Internet trying to visit the internal server within a corporate. Using SSL VPN tunnel, the connection between remote users and private server is encrypted and safe. Besides, enabling the Two-Step Verification function based on the SMS Modem method to enhance the security of user's login; Remote User A belongs to group1 and Remote User B belongs to role1. Users in group 1 are allowed to access the Bug system and users whose role is role1 are allowed to access the OA system; transmitting data over TCP protocol to strengthen communication stability.



Configuration Steps

Step 1: Creating a local user

Select **Object > User > Local User**. Under Local Server "local", click **New > User**.



- Name: test1
- Password: 123456
- Confirm Password: 123456
- Mobile + country code: Configure your valid mobile number. When you log in to the SSL VPN client, if the SMS authentication function is enabled, the SMS gateway or SMS modem will send the verification code to the mobile.

Repeat the steps above to create a user named **test2**.

Step 2: Binding the user "test1" to a user group

Select **Object > User > Local User**. Under Local Server "local", click **New > User Group**.



- Name: group1
- User: test1

Step 3: Binding the user "test2" to a role

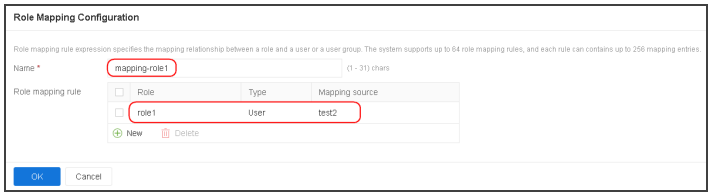
Select **Object** > **Role** > **Role**. Click **New**.

- Role name: role1



Select **Object** > **Role** > **Role Mapping**. Click **New**.

- Name: mapping-role1
- Role mapping rule: Role-"role1"; Type-"User"; Mapping source-"test2"



Select Object > AAA Server. Under Local Server "local", click **Edit**.

- Role mapping rule: mapping-role1

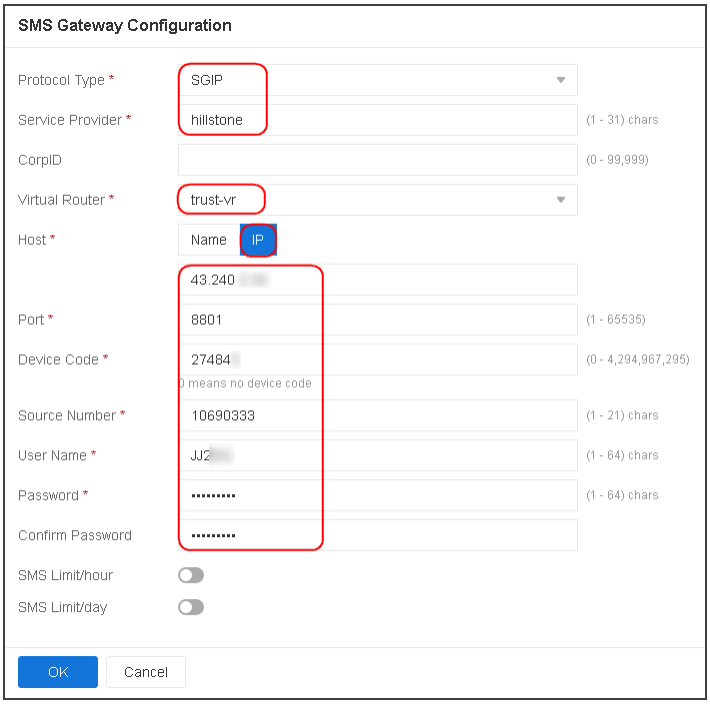


Note: When you bind the user to a role, no matter to which server type the user belongs, you need to configure a role mapping rule of the local server. Otherwise, the user cannot deploy a tunnel route of the corresponding role when logging into the client.

Step 4: Configuring SMS Gateway

Select **System > SMS Parameters > SMS Gateway**, click **New**.

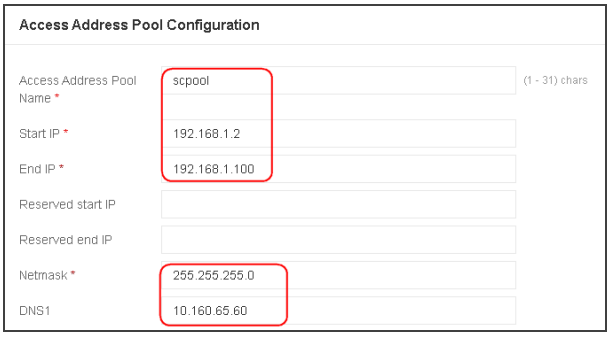
- Protocol Type： SGIP
- Service Provider： hillstone
- Virtual Router： trust-vr
- Host： IP； 43.240.X.X
- Port： 8801
- Company Code： 27484X
- Source Number: 10690333
- User name and Password： Enter the actual user name and password to log in SMS gateway.



Step 5: Configuring SCVPN address pool

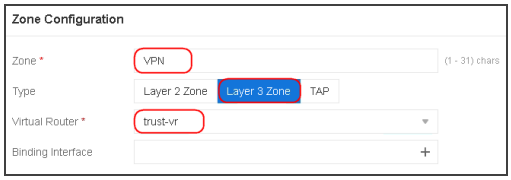
Select **Object > Access Address Pool**. In the IPv4 tab, click **New**.

- Address Pool Name: scpool
- Start IP: 192.168.1.2
- End IP: 192.168.1.100
- Netmask: 255.255.255.0
- DNS1: 10.160.65.60



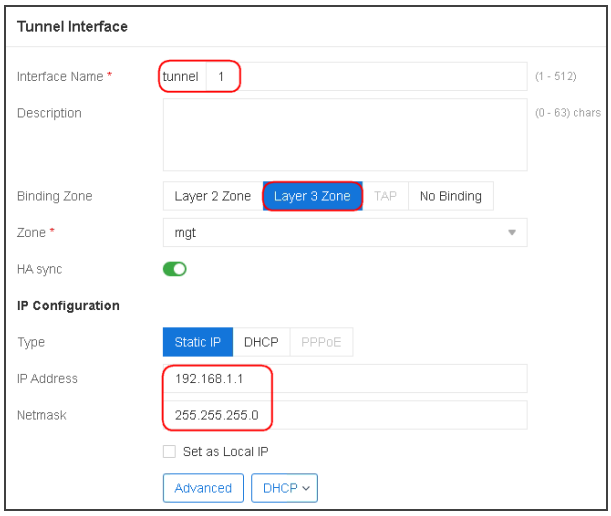
Step 6: Creating tunnel interface

Select **Network > Zone**, and click **New**.



- Zone: VPN
- Type: Layer 3 Zone
- Virtual Router： trust-vr

Select **Network > Interface**, and click **New > Tunnel Interface**.

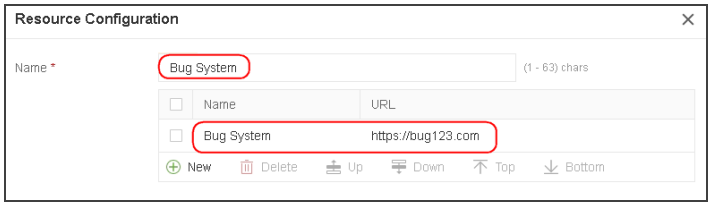


- Interface Name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: VPN
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0

Note: Tunnel interface must be of the same network segment of SSL VPN address pool.

Step 7: Configuring resources

Select **Network** > **VPN** > **SSL VPN**. In the upper-right corner, select **Configuration** > **Resource List**. In the **Resource List** panel, click **New**.

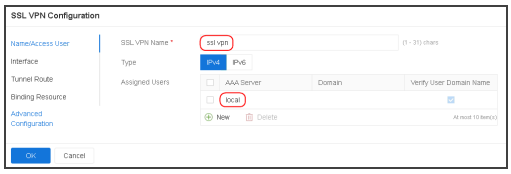


- Name: Bug System
- Resource: Name "Bug System"; URL: "https://bug123.com"

Repeat the steps above to create a resource named OA system (with an entry whose name is "OA System" and URL is "https://oa123.com").

Step 8: Configuring SCVPN

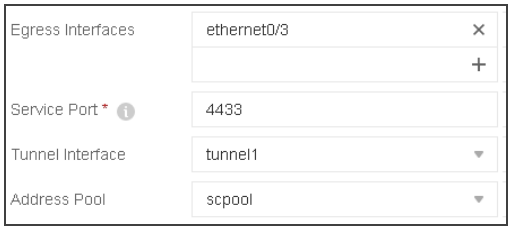
Select **Network** > **VPN** > **SSL VPN**, and click **New**.



In the Name/Access User tab:

- SSL VPN Name: ssl vpn
- Assigned Users:: Click **New**, and select **local**for the **AAA server**drop-down list

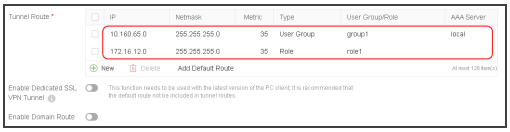
In the Interface tab:



- Egress Interfaces: ethernet0/3
- Service port: 4433
- Tunnel Interface: tunnel1
- Address Pool: scpool

Step 8: Configuring SCVPN

In the Tunnel Route tab, configure two tunnel routes:



tunnel route of User Group group1:

- IP: 10.160.65.0
- Netmask: 255.255.255.0
- Type: User Group
- User Group/Role: group1
- AAA Server: local

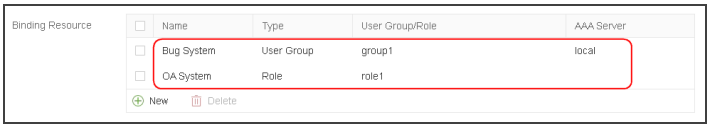
tunnel route of Role role1:

- IP: 172.16.12.0
- Netmask: 255.255.255.0
- Type: Role
- User Group/Role: role1

The IP address of tunnel route and the IP address of internal server must fall into the same CIDR block.

Step 8: Configuring SCVPN

In the Binding Resource tab, click **New** and bind two resources.



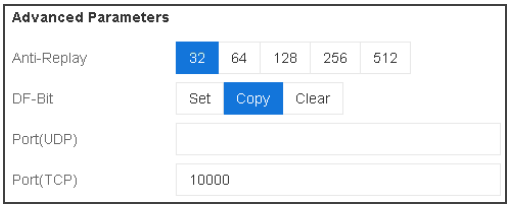
Resource of User Group group1:

- Name: Bug System
- Type: User Group
- User Group/Role: group1
- AAA Server: local

Resource of Role role1:

- Name: OA System
- Type: Role
- User Group/Role: role1

Click **Advanced Configuration**, in the Parameters tab:

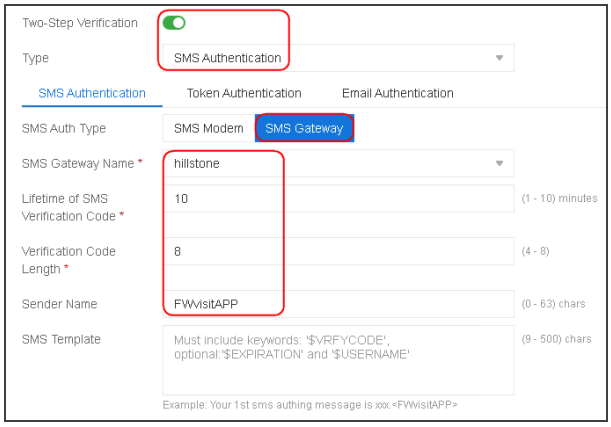


- Advanced Parameters
  - Port(TCP): 10000

After configuring SCVPN on the StoneOS device, you need to add the following configuration to the SCVPN client: Enable the Communication Stability Optimization function. Therefore, the SCVPN client can communicate with the StoneOS device over TCP protocol.

Step 8: Configuring SCVPN

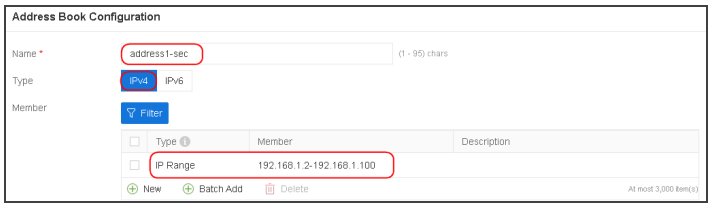
Click **Advanced Configuration**, in the Two-Step Verification tab:



- Two-Step Verification： Click the **Enable** button
- Type： SMS Authentication
- SMS Auth Type： SMS Gateway
- SMS Gateway Name： hillstone
- Lifetime of SMS Verification Code： 10
- Sender Name： FWvisitAPP
- Verification Code Length： 8

Step 9: Creating policy from VPN to any

Select **Object** > **Address Book**. Click **New** and configure the source address of security policies policy1 and policy2.

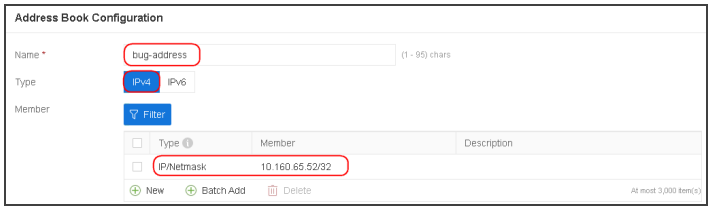


- Name: address1-src
- Type: IPv4
- Member: IP Range; 192.168.1.2-192.168.1.100

We recommend that the configuration of address member is consistent with the IP range of SSL VPN access address pool.

Step 9: Creating policy from VPN to any

Select **Object** > **Address Book**. Click **New** and configure the address book of internal server resource.



Configure the address book of Bug System:

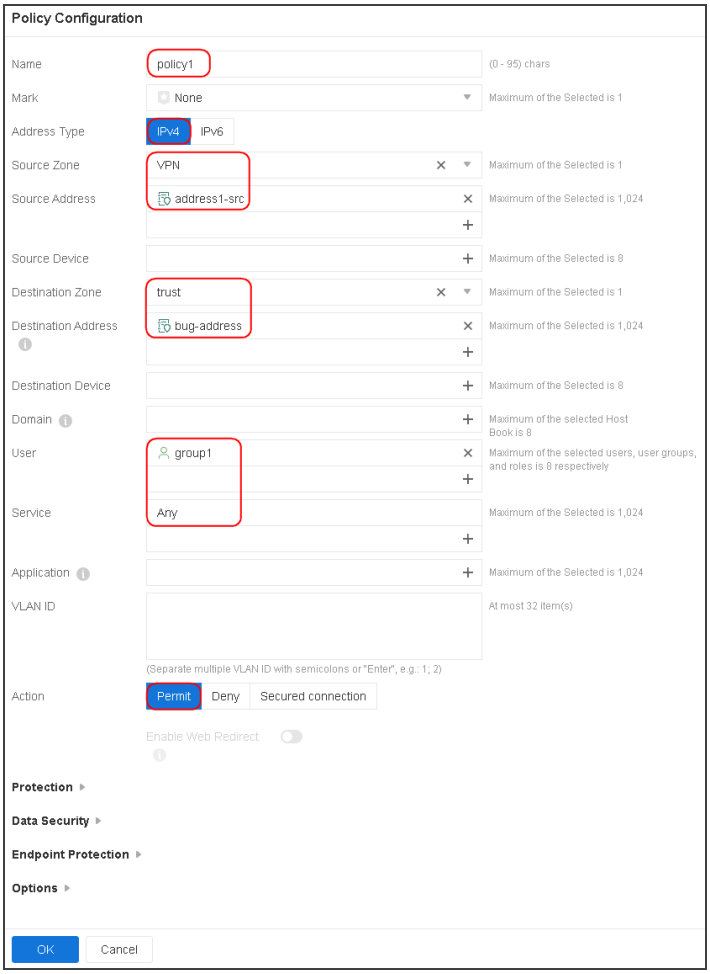
- Name: bug-address
- Type: IPv4
- Member: IP/Netmask; 10.160.65.52/32

Repeat the steps above to configure the address book of OA System.

- Name: oa-address
- Type: IPv4
- Member: IP/Netmask; 172.16.12.12/32

Step 9: Creating policy from VPN to any

Select **Policy** > **Security Policy** > **Policy**. Then, select **New** > **Policy** and configure the security policy of the user test1.



- Name: policy1
- Address Type: IPv4
- Source Zone: VPN
- Source Address: address1-src
- Destination Zone: trust
- Destination Address: bug-address
- User: group1
- Service: Any
- Action: Permit

Repeat the steps above to configure the security policy of the user test2.

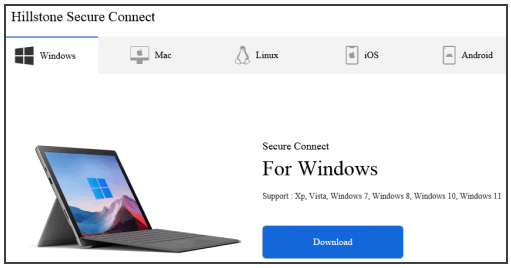
- Name: policy2
- Address Type: IPv4
- Source Zone: VPN
- Source Address: address1-src
- Destination Zone: trust
- Destination Address: oa-address
- User: role1

Step 9: Creating policy from VPN to any

- Service: Any
- Action: Permit

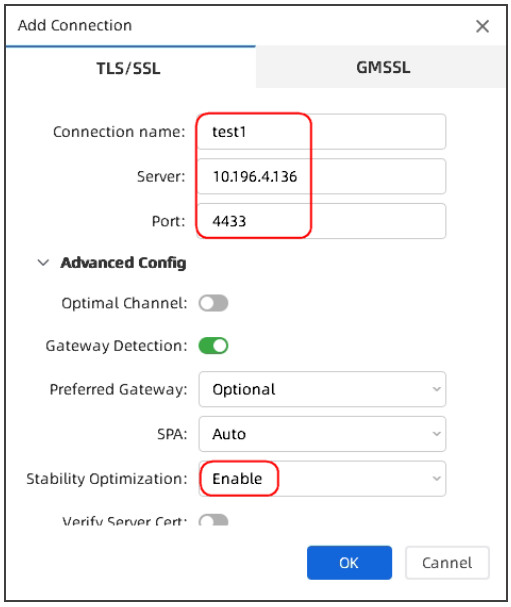
Step 10: Results

After configuration above, the user test1 enters address "https://10.196.4.136:4433" in a browser. In the pop-up page, select Windows tab and click **Download**.



After the user opens the client, click **Add Connection** in the upper-right corner. In the dialog box that appears, enter the following information:

- Connection name: test1
- Server: 10.196.4.136
- Port: 4433
- Stability Optimization: Enable (After the user successfully logs in to the SSL VPN client, it will use the TCP protocol to securely access resources of Sever in the trust zone)

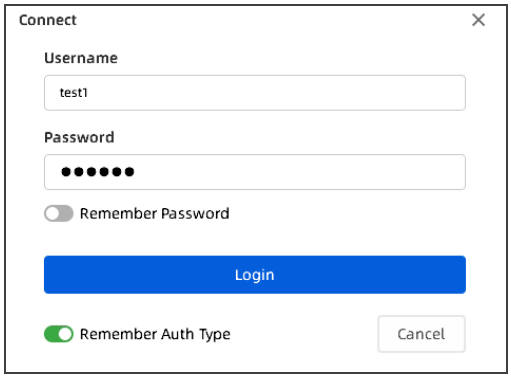


Click **OK**. A login information entry is generated.

Step 10: Results

Click **Connect**. The **Connect** dialog box appears.

- Username: test1
- Password: 123456



After you enter the information above, the **SMS Authentication** dialog box appears. Then, perform the secondary authentication of VPN login.

View the 8-digit verification code received on the mobile phone of the user test1, enter it into the field, and then click Verify.

After the client displays a successful connection, the PC of the user test1 can securely access Bug System on the internal network via SSL VPN. In addition, click the **Route** tab on the client and you can view the tunnel route deployed by the device to the user test1, who belongs to the user group group1.

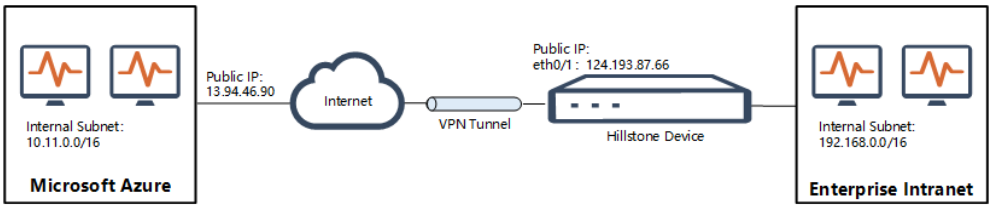
Repeat the steps above for the PC of the user test2.
After the client displays a successful connection, the PC of the user test2 can securely access OA System on the internal network via SSL VPN. In addition, click the **Route** tab on the client and you can view the tunnel route deployed by the device to the user test2, who belongs to the role role1.

Connecting to Microsoft Azure Using Site-to-Site VPN

Today, more and more customers are using public cloud service providers such as Microsoft Azure to deploy their server or services, to get high performance, reliable services that are easy to deploy and get to market fastest.

This example shows how to configure site-to-site VPN to establish a VPN tunnel (IPSec VPN tunnel) between Microsoft Azure and Hillstone device.

The topology is shown as below, the Hillstone device is the gateway for the enterprise. It requires an IPsec VPN tunnel between the company and Microsoft Azure through the Hillstone device. The authentication algorithm uses SHA and the encryption algorithm uses 3DES, thus the local service can be connected with hosted cloud services.



*** Note:** This topology uses laboratory environment. In this recipe, 124.193.87.66 represents Hillstone device public IP, 192.168.0.0/16 represents the internal subnet of enterprise, 13.94.46.90 represents public IP of Microsoft Azure, 10.11.0.0/16 the internal subnet of Microsoft Azure.

The configuration process as follows:

Configure Microsoft Azure:

1. Create a virtual network
2. Create the gateway subnet
3. Create the VPN gateway
4. Create the local network gateway
5. Create the VPN connection

Configure Hillstone device:

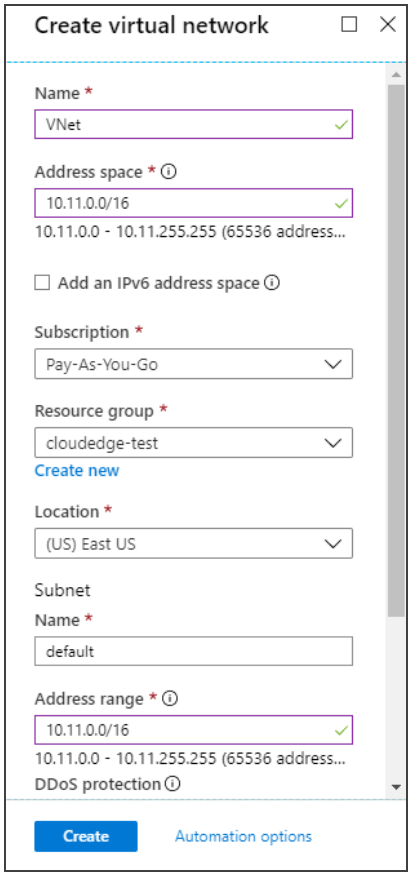
1. Configuring IPSec VPN
2. Creating IPsec VPN IKEv2 tunnel
3. Binding the tunnel interface to the IPsec VPN IKEv2 tunnel
4. Configuring route

Configure Microsoft Azure

In Microsoft Azure, configure the following settings:

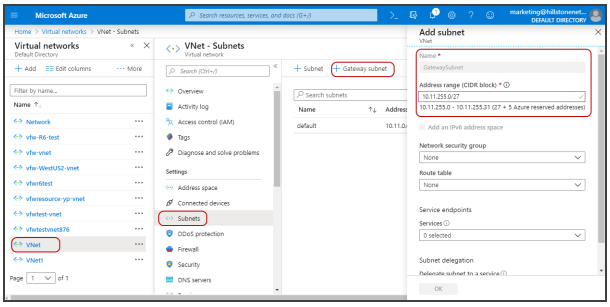
Step 1 : Create a virtual network

1. Access the Microsoft Azure website via the browser and sign in with your Azure account.
2. Click **Virtual networks** in the "Azure service" section of the Home page to open the virtual network page.
3. Click **+Add**.
4. In the **Create virtual network** page, configure the following information (take the environment in the topology as an example):
    - Name: VNet
    - Address space: 10.11.0.0/16
    - Subscription: select the existing subscription to use: “Pay-As-You-Go”
    - Resource group: cloudedge-test
    - Location: East US
    - Subnet name: default
    - Subnet address range: 10.11.0.0/16
5. Click **Create** to create the virtual network.



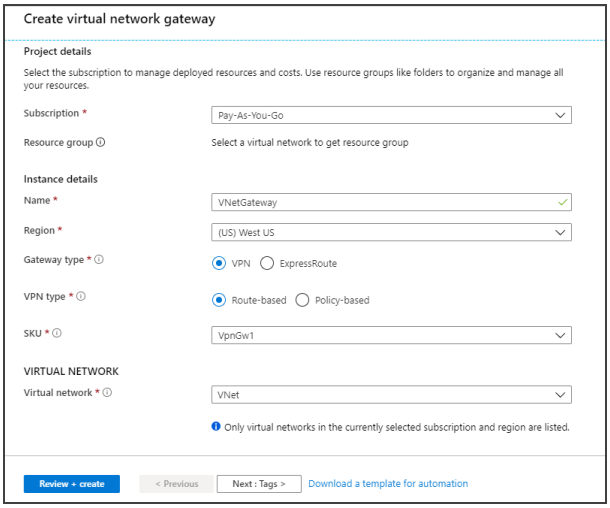
Step 2: Create the gateway subnet

1. In the list of virtual network page, select the created virtual network "VNet" in the list and click its name.
2. In the **Settings** section on the left side of the virtual network detail page, select **Subnet**.
3. In "VNet-Subnets" page. click **+Gateway subnet**.
4. In **Add subnet** page, configure the following information (take the environment in the topology as an example):
    - Name: The default value "GatewaySubnet"
    - o Address range (CIDR block): 10.11.255.0/27
5. Click **OK** to create the gateway subnet.



Step 3: Create a VPN geteway

1. Click **Create a resource** in the "Azure service" section of the Home page.
2. In **Search the Marketplace field**, search **Virtual Network Gateway**.
3. Click **Create**.
4. In **Create virtual network gateway** page, configure the following information (take the environment in the topology as an example):
    - Name: VNetGateway
    - Region: West US (choose the one where your virtual network is located)
    - Gateway type: VPN
    - VPN type: Route-based
    - SKU: VpnGw1 (About SKU, refer to https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsku)
    - Virtual network: VNet (choose the one to which you want to add the gateway)
    - Public IP address: Create new (only dynamic Public IP address allocation is supported currently; input the public address name)



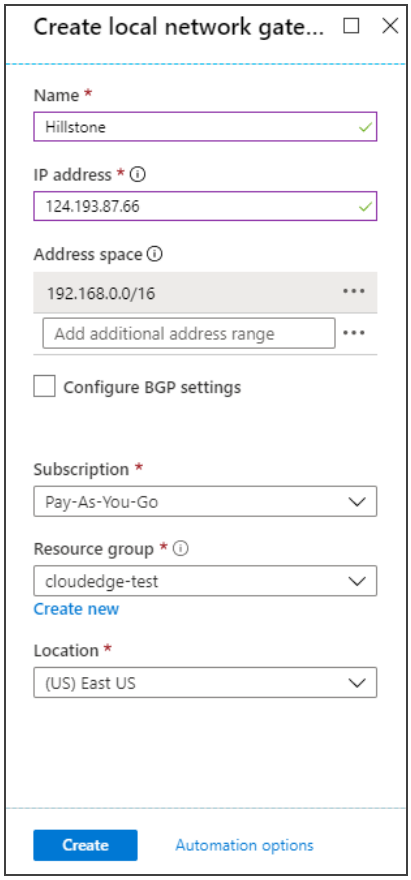
Step 3: Create a VPN geteway

- Public IP address name: PublicIP

5. Click **Review +create** and wait for the virtual network gateway deployment. After the virtual network gateway created, the public IP address will be assigned

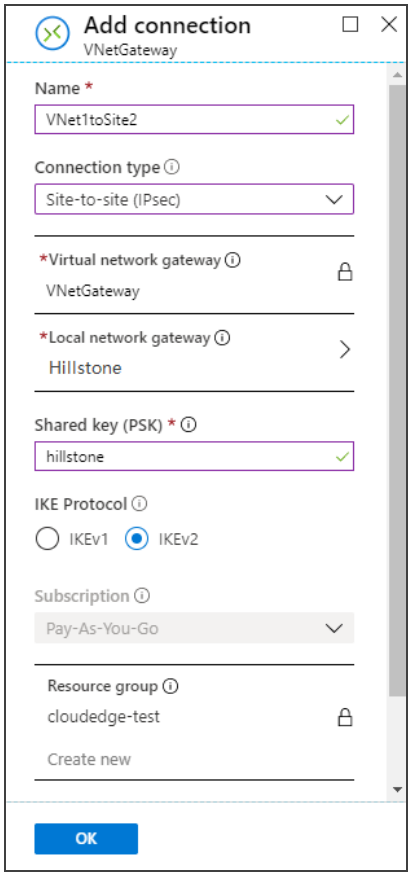
Step 4: Create the local network gateway

1. Click **Create a resource** in the "Azure service" section of the Home page.
2. In **Search the Marketplace field**, search **Local Network Gateway**
3. Click **Create**.
4. In **Create local network gateway** page, configure the following information (take the environment in the topology as an example):
   - Name: Hillstone
   - IP address: 124.193.87.66
   - Address space: 192.168.0.0/16
   - Subscription: select the existing subscription to use: "Pay-As-You-Go"
   - Resource group: cloudedge-test
   - Location: East US
5. Click **Create** to create the local network gateway.



Step 5: Create the VPN connection (This step is performed after completing the "Configure Hillstone Device")

1. Click the created virtual network gateway **VNetGateway** in the **Recent resources** list on the home page.
2. In the **Settings** section on the left side of the virtual network gateway detail page, select **Connections**
3. Click **Add**.
4. In **Add connection** page, configure the following information (take the environment in the topology as an example):
   - Name: VNet1toSite2
   - Connection type: Site-to-site (IPSec)
   - Virtual network gateway: VNetGateway
   - Loacl network gateway: Hillstone
   - Shared key (PSK): hillstone (Consistent with "Configure Hillstone Device")
   - Resource group: cloudedge-test
5. Click **OK** to create the connection.



Note:

- About VPN devices and IPsec/IKE parameters for Site-to-Site VPN Gateway connections, refer to the Microsoft Azure documentation: https://docs.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-about-vpn-devices.

- About "Create a Site-to-Site connection in the Azure portal", refer to the Microsoft Azure documentation: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal.

Configure Hillstone Device

Step 1: Configuring IPSec VPN

```
1.Configuring P1 proposal for IKEv2 SA.
hostname(config)# ikev2 proposal Azure_to_Hillstone_P1
hostname(config-ikev2-proposal)# hash sha
hostname(config-ikev2-proposal)# encryption 3des
hostname(config-ikev2-proposal)# group 2
hostname(config-ikev2-proposal)# lifetime 10800
hostname(config-ikev2-proposal)# exit
2.Configuring P2 proposal for IPSec IKEv2 SA.
hostname(config)# ikev2 ipsec-proposal Azure_to_Hillstone_P2
hostname(config-ikev2-ipsec-proposal)#hash sha
hostname(config-ikev2-ipsec-proposal)#encryption aes
hostname(config-ikev2-ipsec-proposal)#lifetime 3600
hostname(config-ikev2-ipsec-proposal)#exit
3. Configuring IKEv2 peer.
hostname(config)# ikev2 peer peer1
hostname(config-ikev2-peer)# interface ethernet0/1
hostname(config-ikev2-peer)# match-peer 13.94.46.90
hostname(config-ikev2-peer)# ikev2-proposal Azure_to_Hillstone_P1
hostname(config-ikev2-peer)# local-id ip 124.193.87.66
4.Creating IKEv2 Profile.
hostname(config-ikev2-peer)# ikev2-profile esp-peer1
hostname(config-ikev2-profile)# remote id ip 13.94.46.90
hostname(config-ikev2-profile)# remote key hillstone
hostname(config-ikev2-profile)# traffic-selector src subnet 192.168.0.0/16
```

```
hostname(config-ikev2-profile)# traffic-selector dst subnet 10.11.0.0/16
hostname(config-ikev2-profile)# exit
hostname(config-ikev2-peer)# exit
hostname(config)#
```

Step 2: Creating IPsec VPN IKEv2 tunnel

```
hostname(config)# tunnel ipsec Azure ikev2
hostname(config-ikev2-tunnel)# ikev2-peer peer1
hostname(config-ikev2-tunnel)# ipsec-proposal Azure_to_Hillstone_P2
hostname(config-ikev2-tunnel)# auto-connect
hostname(config-ikev2-tunnel)# exit
hostname(config)#
```

Step 3 : Binding the tunnel interface to the IPsec VPN IKEv2 tunnel

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# tunnel ikev2 Azure
hostname(config-if-tun1)# exit
hostname(config)#
```

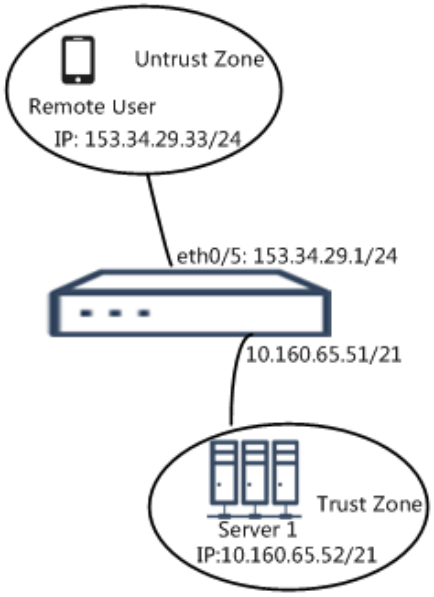
Step 4: Configuring route

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 10.11.0.0/16 tunnel1
hostname(config-vrouter)# exit
```

Using an iOS/Android Device to Remotely Access Intranet Services

This example introduces how to use an iOS/Android device to remotely access the resources in the private network.

In the topology below, a remote user located in the Internet uses an iOS/Android device to access the intranet server **Server1**. The authentication method requires username and password, and the connection is based on SSL VPN. Please first see step 1 to 5 in "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 199 to create a SSL VPN instance.

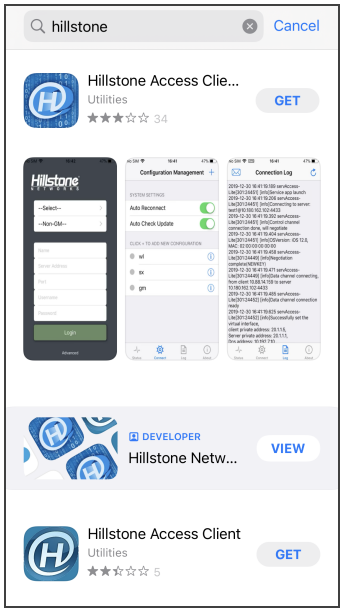


Using an iOS Device to Remotely Access Intranet Services

Take the VPN client of version 2.0.8 for example.

Step 1: Downloading and installing Hillstone Access Client

In APP Store, search Hillstone Access Client, click **Get** to download and install this application.



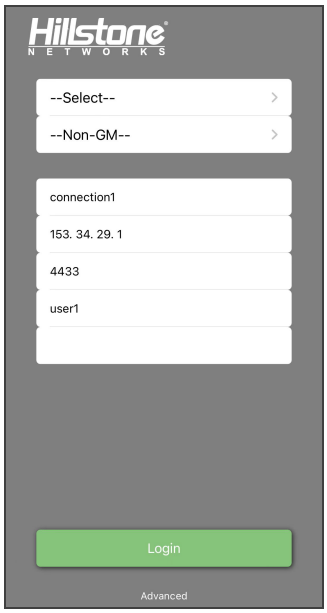
Step 2: Connecting to the device

Click the HSAccess icon in the iOS desktop.

In the login page:

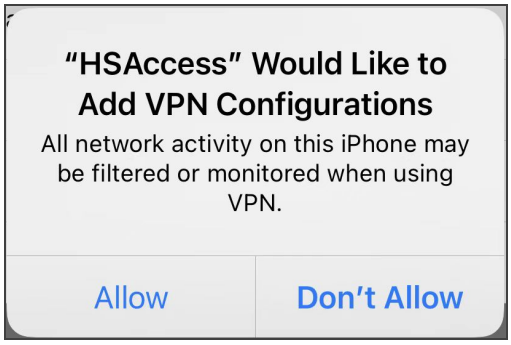
- Connection: connection1
- Server: 153.34.29.1
- Port: 4433
- Account: user1
- Password: 123456

Click **Login**. The client starts to connect to the server.



Step 3: Installing the VPN configuration profile

In the Add VPN Configurations dialog, click **Allow** to install the VPN configuration profile.



Enter your passcode.



Step 4: Creating a VPN connection

In iOS, select **Settings > VPN**.

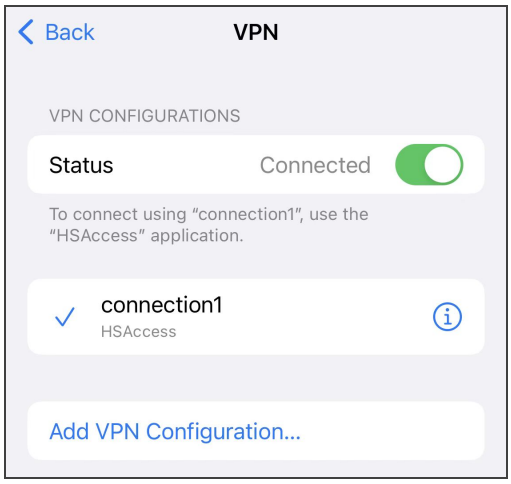
In the list, select **connection1**.

Turn on the VPN switch. iOS connects to the VPN.

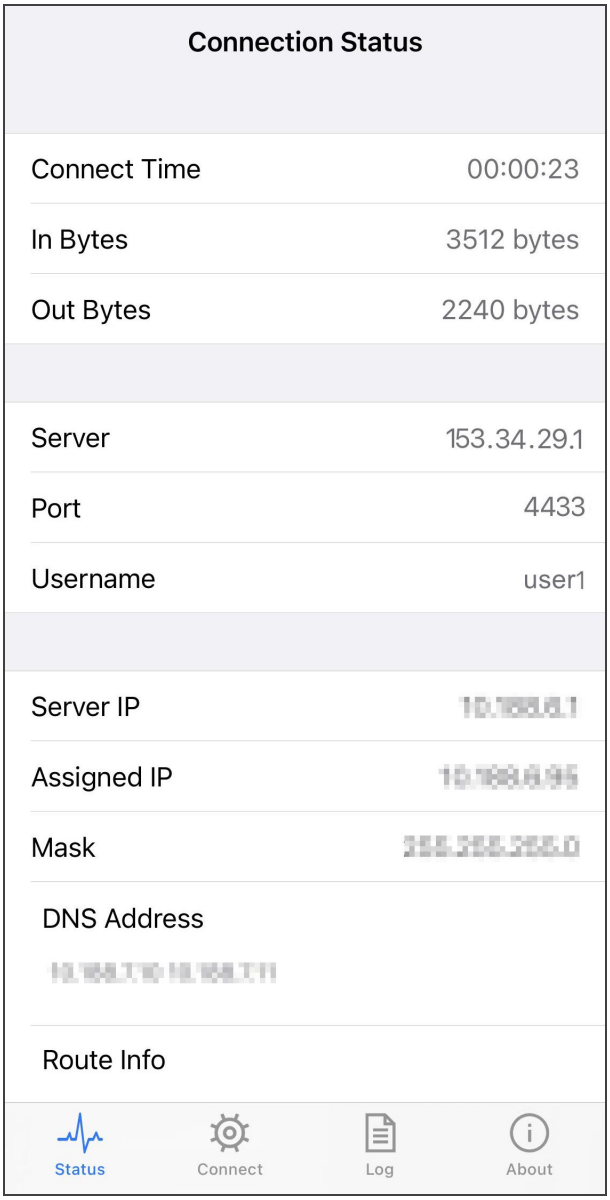


Step 5: Verifying the connection status.

When the VPN status is **Connected** and the Connection tab of the client displays **Connected**, the client successfully establishes VPN connection to the device.



Step 5: Verifying the connection status.



Step 6: Accessing intranet services

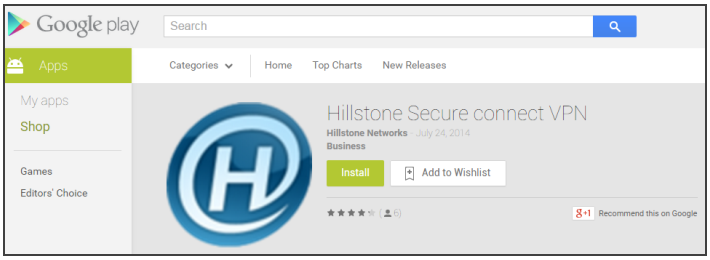
Use the iOS device to visit Server1.

Using an Android Device to Remotely Access Intranet Services

Step 1: Downloading and installing Hillstone Secure Connect

Visit Google Play to download and install Hillstone Secure Connect VPN.

https://play.google.com/store/apps/details?id=com.hillstone.vpn

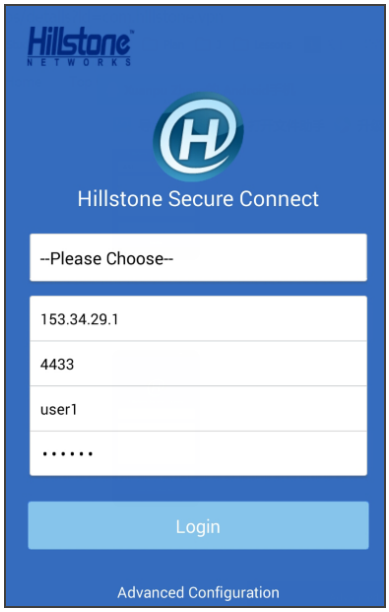


Step 4: Creating a VPN connection

In Android, click the Hillstone Secure Connection icon:

- Server: 153.34.29.1
- Port: 4433
- Account: user1
- Password: 123456

Click **Login**.



After the VPN connection is established successfully, the key icon will appear at the notification area of your Android system.



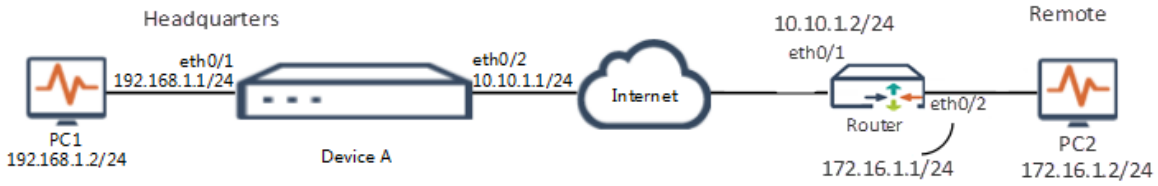
Step 6: Accessing intranet services

Use the Android device to visit Server1.

Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN

This example shows how to use L2TP over IPSec VPN to provide remote users with access to corporate internal network.

The topology is shown as below. A remote user, located at home or a hotel, accesses the Internet through a router with NAT enabled. This remote user uses L2TP over IPSec VPN to visit the server (PC1) in the corporate internal network. And this server is protected by the device A.



*Due to lab environment, use 10.10.1.0./24 to represent the public network segment.

The configuration process consists of five parts:

- Configure basic settings
- Configure IPSec VPN
- Configure L2TP VPN
- Set up a VPN connection in Windows/ Mac
- Adjust whether to use IPSec for L2TP VPN

Configuring Basic Settings

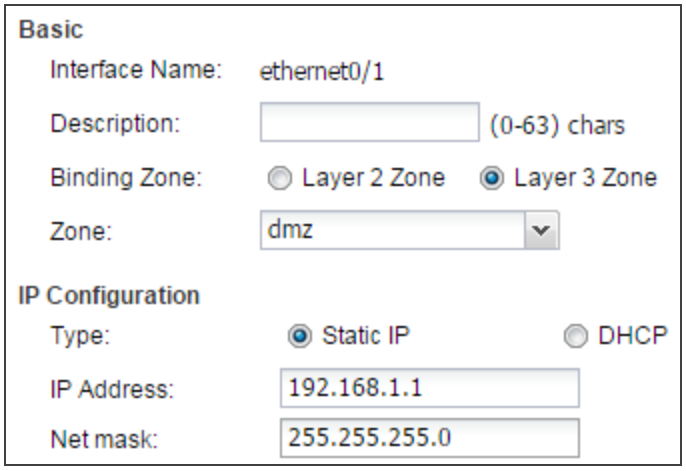
In device A, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/1.

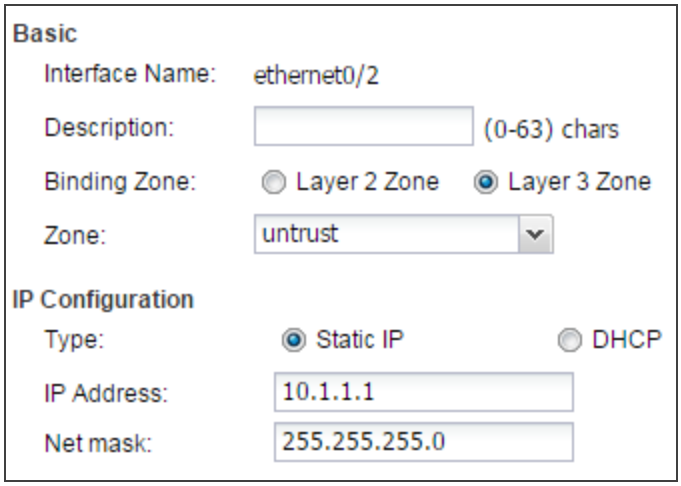
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

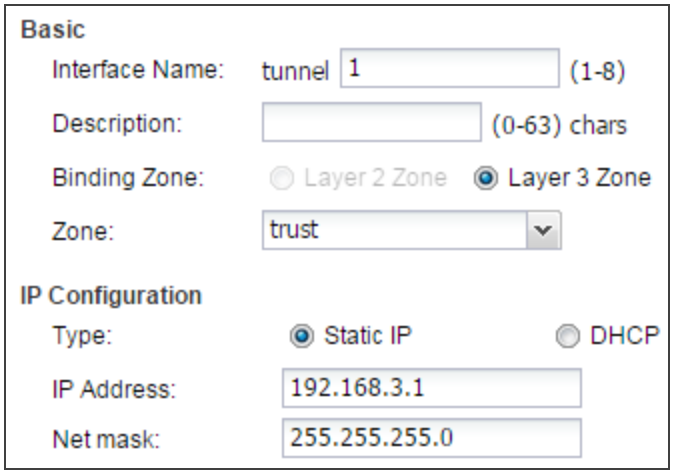


Step 1: Configuring an interface

Configuring the tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.

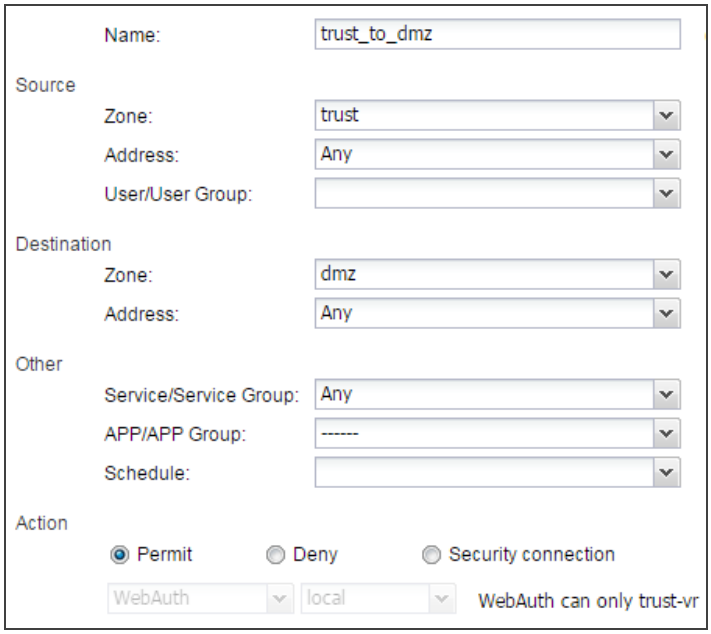
- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 192.168.3.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 2: Configuring a security policy

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the DMZ zone where the internal server locates.

Select **Policy > Security Policy > New**.



- Name: trust_to_dmz
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

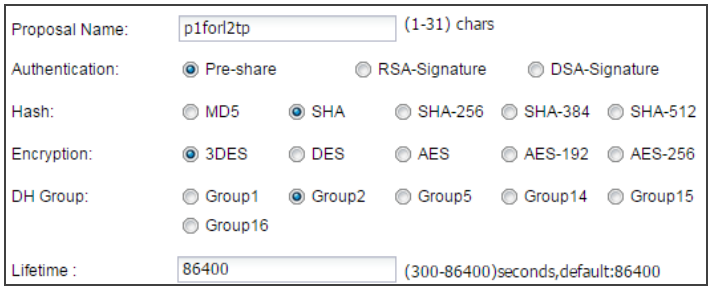
Configuring IPSec VPN

In device A, configure the following settings:

Step 1: Creating a P1 proposal and a P2 proposal

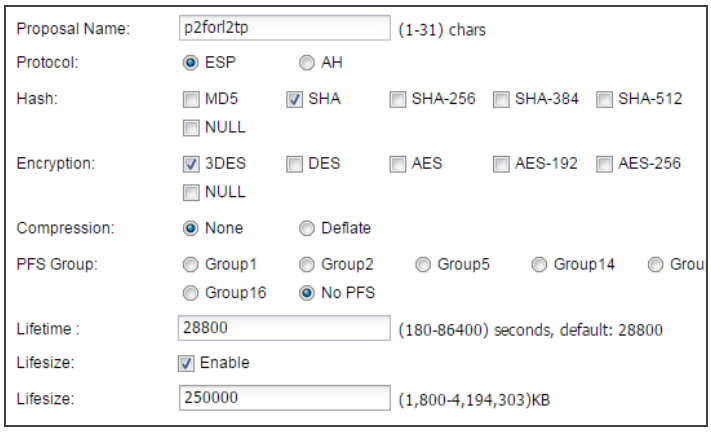
Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forl2tp
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



In the P2 Proposal tab, click **New**.

- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800
- Lifesize: Enable
  - Lifesize: 250000



Step 2: Configuring a VPN peer

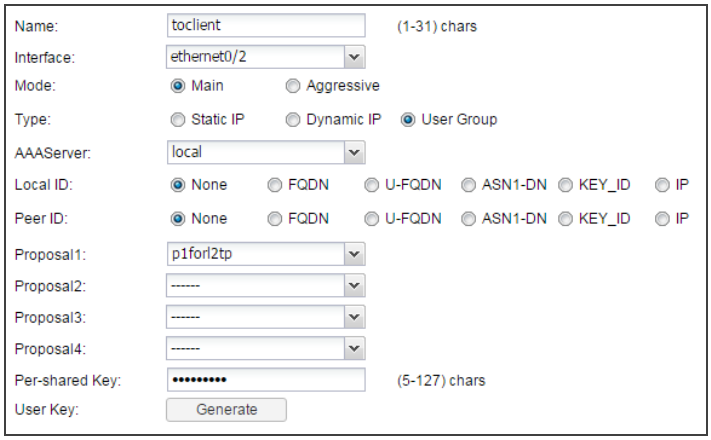
Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

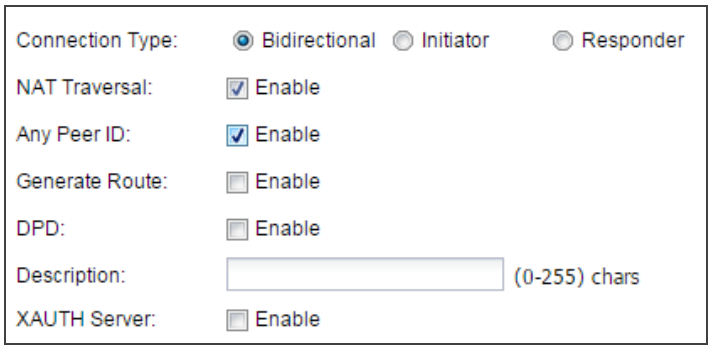
In the Basic tab, configure the following settings:

- Name: toclient
- Interface: ethernet0/2
- Mode: Main
- Type: User Group
- AAA Server: local
- Proposal1: p1forl2tp
- Pre-shared Key: hillstone

In the Advanced tab, configure the following settings:

- NAT Traversal: Enable
- Any Peer ID: Enable
- Keep the default of other parameters



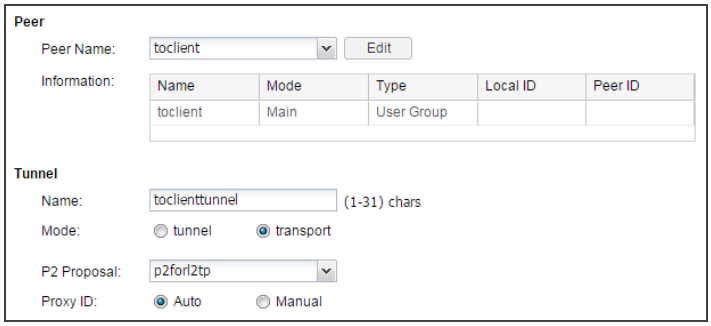


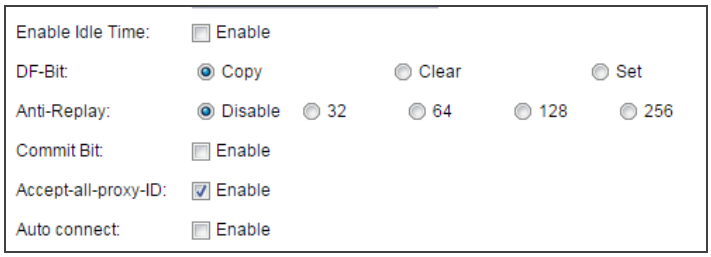
Step 3: Configuring IKE VPN

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the following settings:

- Peer
  - Peer Name: toclient
- Tunnel
  - Name: toclienttunnel
  - Mode: transport
  - P2 proposal: p2forl2tp





In the Advanced tab, configure the following settings:

- Accept-all-proxy-ID: Enable
- Keep the default of other parameters

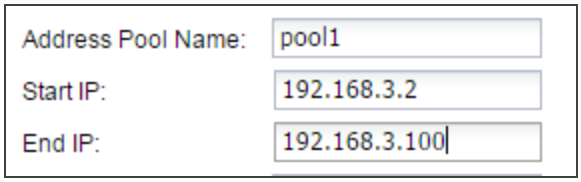
Configuring L2TP VPN

In device A, configure the following settings:

Step 1: Creating a L2TP pool

Select **Network > VPN > L2TP VPN > Address Pool**.

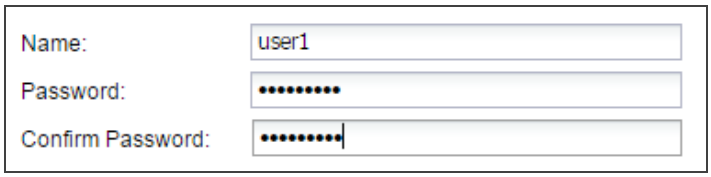
In the Address Pool dialog, click **New**.



- Address Pool Name: pool1
- Start IP: 192.168.3.2
- End IP: 192.168.3.100

Step 2: Adding a user in the 'local' AAA server

Select **Object > User > Local User > New > User**.



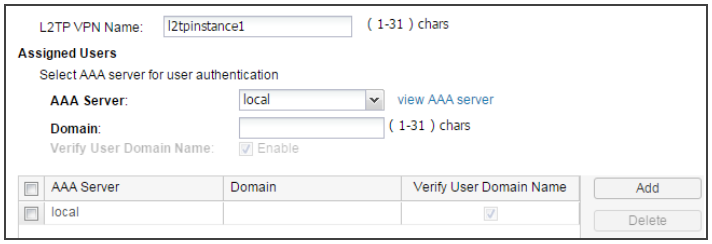
- Name: user1
- Password: hillstone
- Confirm Password: hillstone

Step 3: Configuring a L2TP VPN instance

Select **Network > VPN > L2TP VPN > New**.

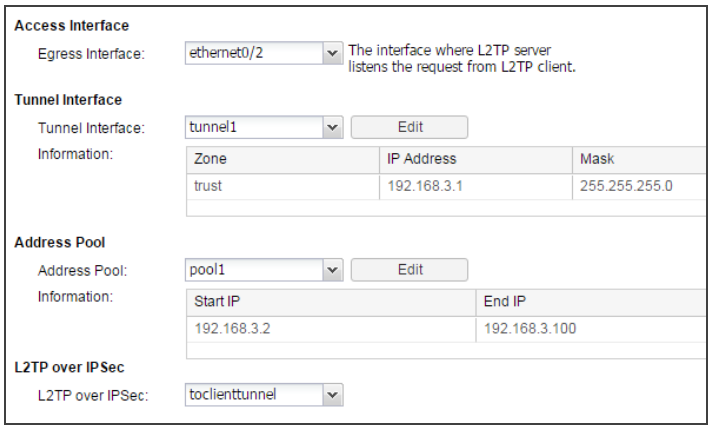
In the Name/Access User tab, configure the following settings:

- L2TP VPN Name: l2tpinstance1
- AAA Server: local
- Click **Add**



In the Interface/Address Pool/IPSec Tunnel tab, configure the following settings:

- Egress Interface: ethernet0/2
- Tunnel Interface: tunnel1
- Address Pool: pool1
- L2TP over IPSec: toclienttunnel



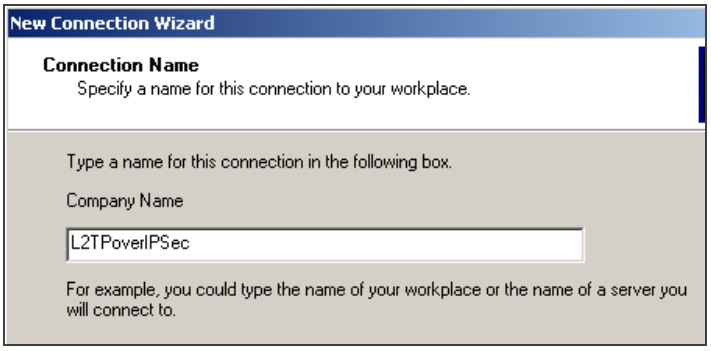
Setting up a VPN Connection

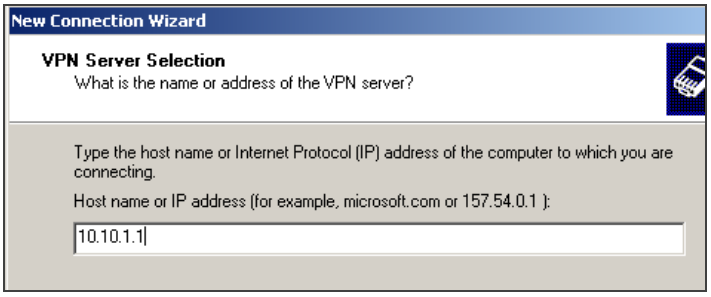
The steps of setting up a VPN connection differ in different PC operating systems. Take Windows 7, Windows XP/2003 and Mac OS for example.

Steps of setting up a VPN connection in Windows XP/2003

Set up a connection:

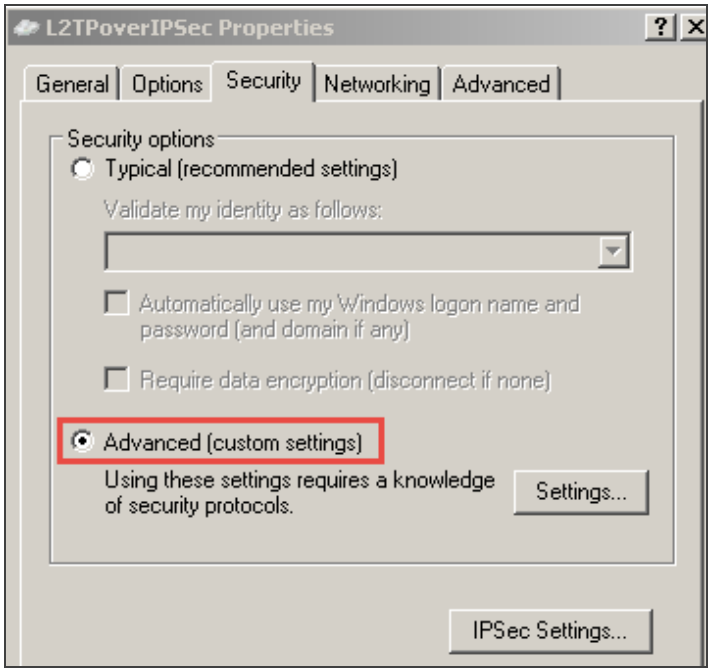
1. In Control Panel , double-click **Network Connections**.
2. From the Network Tasks pane, Click **Create a new connection**. The New Connection Wizard dialog appears
3. In the pop-up dialog, click **Next**.
4. Select **Connect to the network at my workplace**. Then click **Next**.
5. Select **Virtual Private Network connection**. Then click **Next**.
6. Enter a name for this connection in the **Company Name** text box: **L2TPoverIPSec**. Then click **Next**.
7. Enter the IP address of the VPN server: 10.10.1.1. Then click **Next**.
8. Click **Finish**.

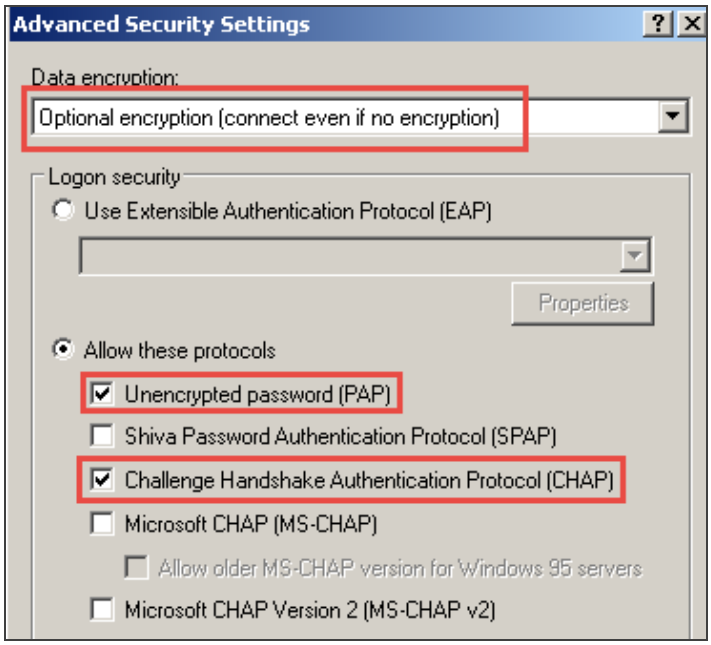




Steps of setting up a VPN connection in Windows XP/2003

Configure the Security properties of this connection:





1. After you have completed the new connection wizard, the Connect L2TPover-IPSec dialog appears.
2. Click **Properties**. The L2TPoverIPSec Properties dialog appears.
3. Select the **Security** tab.
4. Select **Advanced (custom settings)**. Then click **Settings**. The Advanced Security Settings dialog appears.
5. In the **Data encryption** drop-down menu, select **Optional encryption (connect even if no encrypting)**.
6. In the Logon security section, select **Allow these protocols**.
7. Continue to select **Unencrypted password (PAP)** and **Challenge Handshake Authentication Protocol (CHAP)**.
8. Click **OK** to close the **Advanced Security Settings** dialog and return to the L2TPover-IPSec Properties dialog.
9. Click **IPSec Settings**.
10. Select **Use pre-shared key for authen-**

Steps of setting up a VPN connection in Windows XP/2003

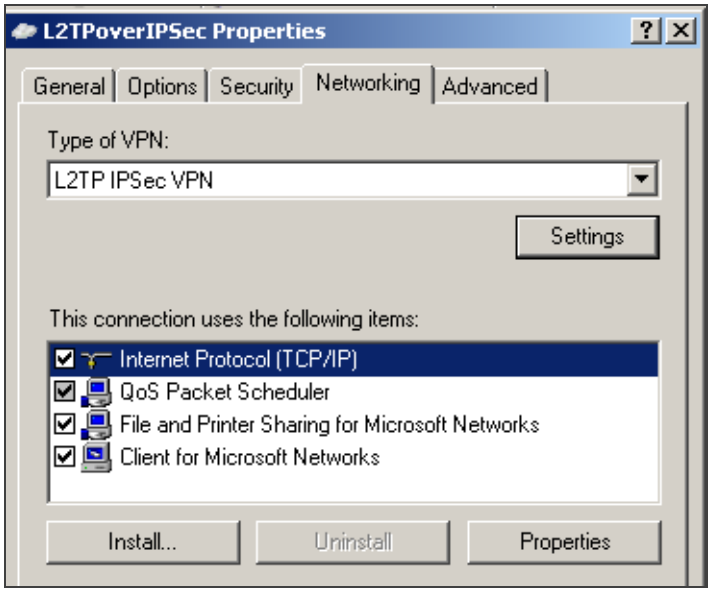
tication and enter the pre-shared key **hillstone**.

11. Click **OK** to close the IPSec Settings dialog.



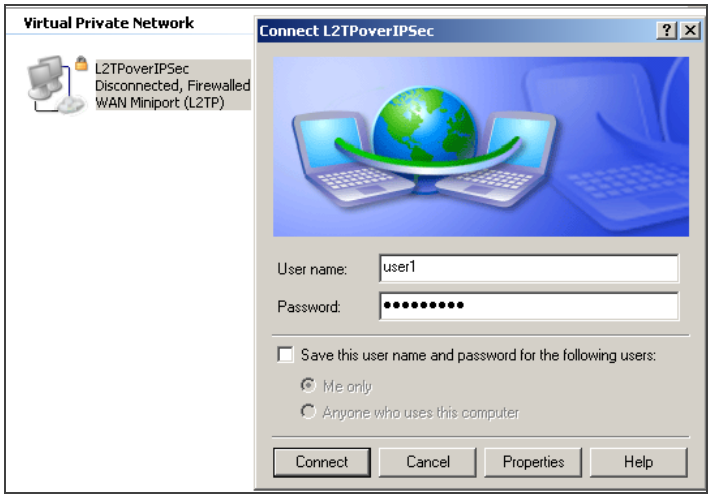
Configure the Networking properties of this connection:

1. In the L2TPoverIPSec Properties dialog, select the **Networking** tab.
2. In the Type of VPN drop-down menu, select **L2TP IPSec VPN**.
3. Ensure that you have select the **Internet Protocol (TCP/IP)** check box.
4. Click **OK** to save the configurations.



Connect to the L2TPoverIPSec VPN:

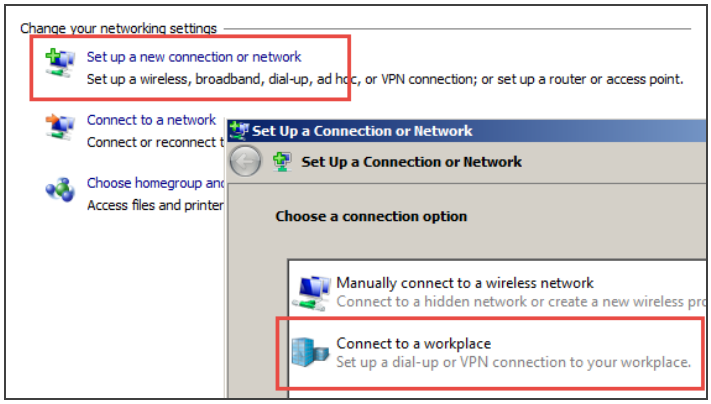
1. Find the **L2TPoverIPSec** connection and double-click it.
2. Enter the user name: user1
3. Enter the password: hillstone
4. Click **Connect**.
5. After the connection is successful, you can visit the internal server 192.168.1.2

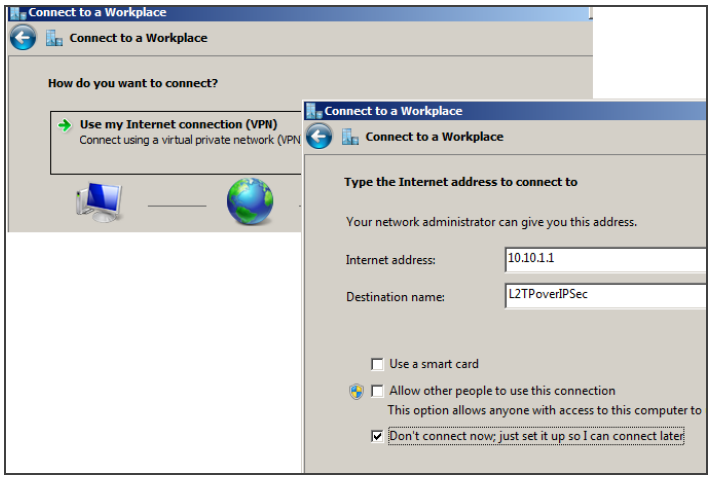


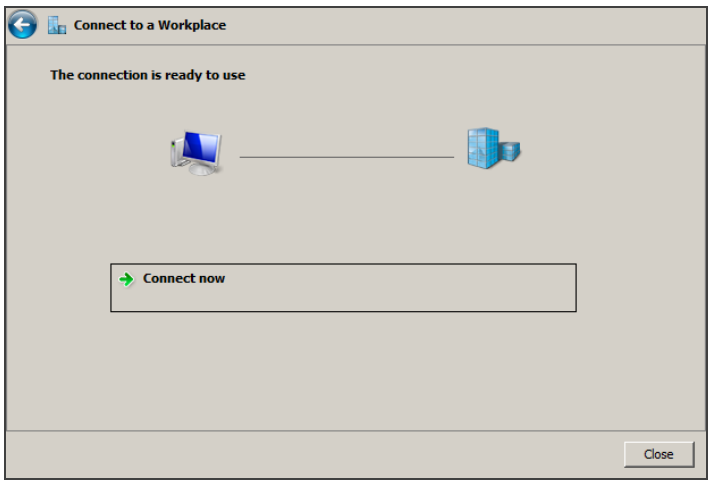
Steps of setting up a VPN connection in Windows 7

Set up a connection:

1. Select **Control Panel > Network and Internet > Network and Sharing Center**.
2. Click **Set up a new connection or network**.
3. In the pop-up dialog, select **Connect to a workplace**. Then click **Next**.
4. Select **Use my Internet connection (VPN)**.
5. Enter the IP address of the VPN server: 10.10.1.1
6. Enter the destination name: L2TPover-IPSec
7. Select **Don't connect now; just set it up so I can connect later**. Then click **Next**.
8. Enter the username: user1
9. Enter the password: hillstone
10. Click **Creat**.
11. After the connection is ready to use, click **Close**.



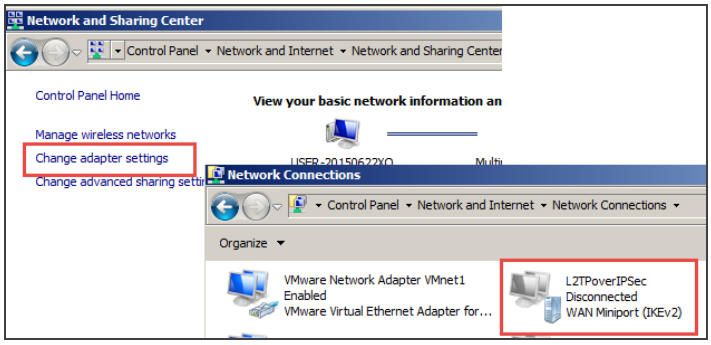


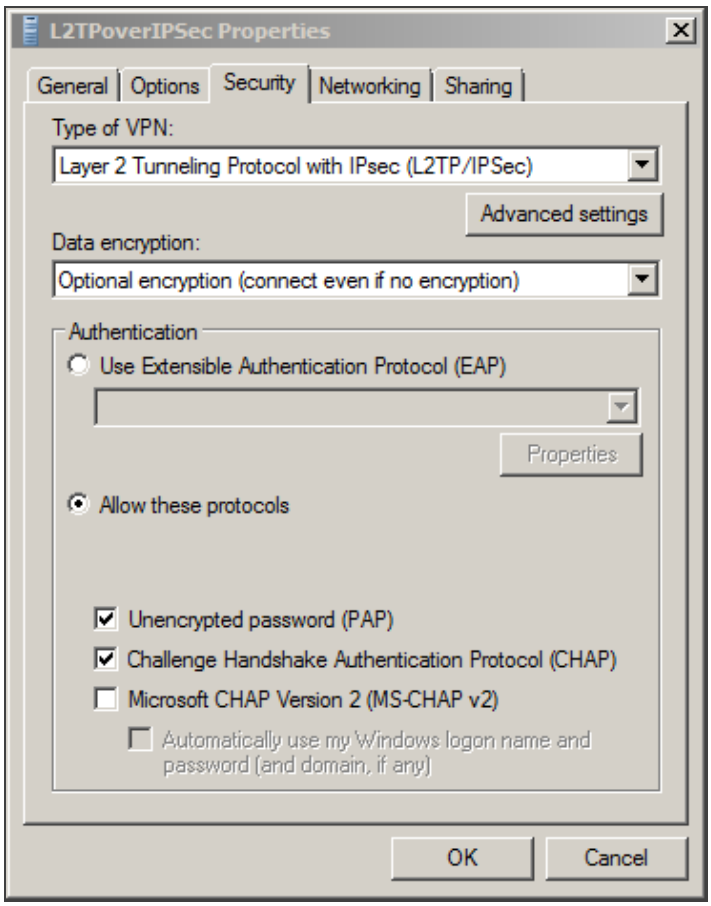


Steps of setting up a VPN connection in Windows 7

Configure the Security properties of this connection:

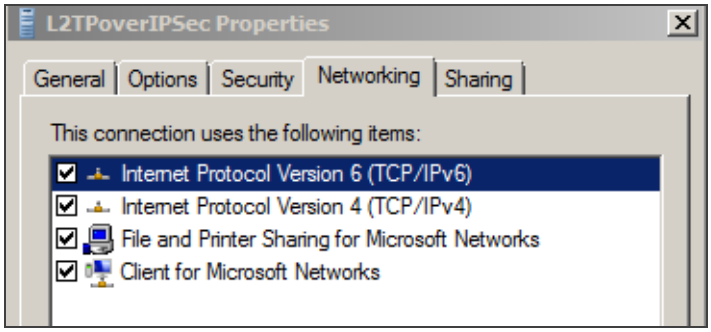
1. In the Network and Sharing Center, click **Change adapter settings**.
2. Find the **L2TPoverIPSec** connection and right-click it.
3. In the pop-up menu, select **Properties**. The L2TPoverIPSec Properties dialog appears.
4. Select the **Security** tab.
5. In the **Type of VPN** drop-down menu, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**.
6. Click **Advanced settings**, select **Use pre-shared key for authentication**, then enter the key **hillstone**.
7. In the **Data encryption** drop-down menu, select **Optional encryption (connect even if no encryption)**.
8. In the **Authentication** section, select **Allow these protocols** and then select **Unencrypted password (PAP)** and **Challenge Handshank Authentication Protocol (CHAP)**.





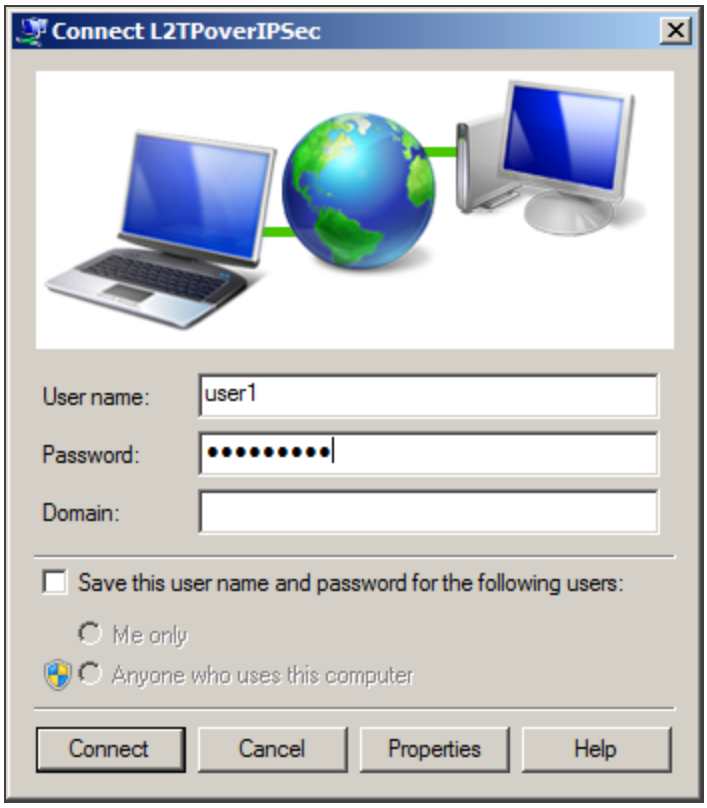
Steps of setting up a VPN connection in Windows 7

Configure the Networking properties of this connection:



1. In the L2TPoverIPSec Properties dialog, select the **Networking** tab.
2. Ensure that you have select the **Internet Protocol Version 4 (TCP/IPv4)** check box.
3. Click **OK** to save the configurations.

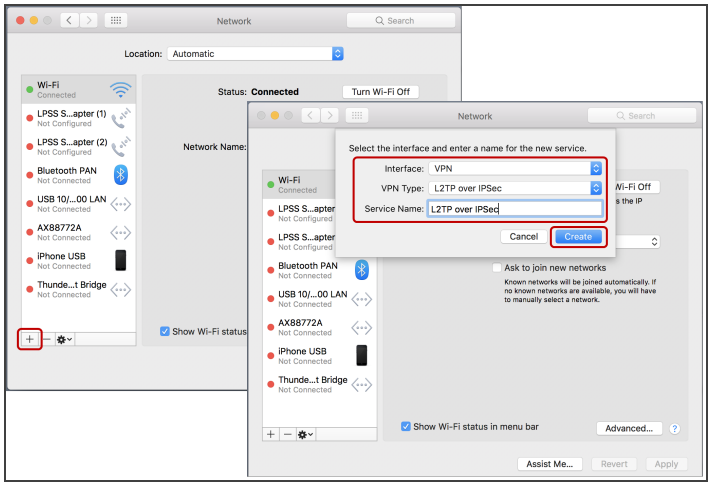
Connect to the L2TPoverIPSec VPN:



1. Find the **L2TPoverIPSec** connection and double-click it.
2. Enter the password: hjllstone
3. Click **Connect**.
4. After the connection is successful, you can visit the intranet server 192.168.1.2

Steps of setting up a VPN connection in Mac OS

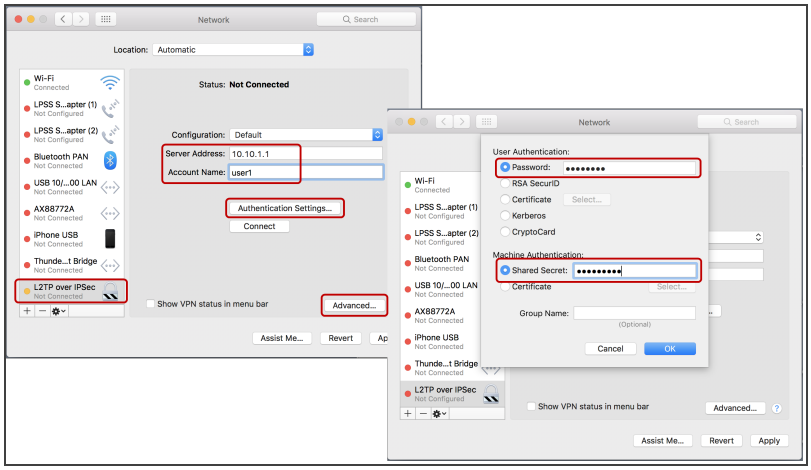
Set up a connection:



1. Select **System Preferences > Network**.
2. Click + to create a new network connection
3. Enter the connection configuration in the pop-up dialog.
4. Click Interface drop-down list and select VPN
5. Click **VPN Type** drop-down list and select **L2TP over IPSec**.
6. Enter the **Service Name**: L2TP over IPSec.
7. Click Create.

Steps of setting up a VPN connection in Mac OS

Configure the properties of connection:

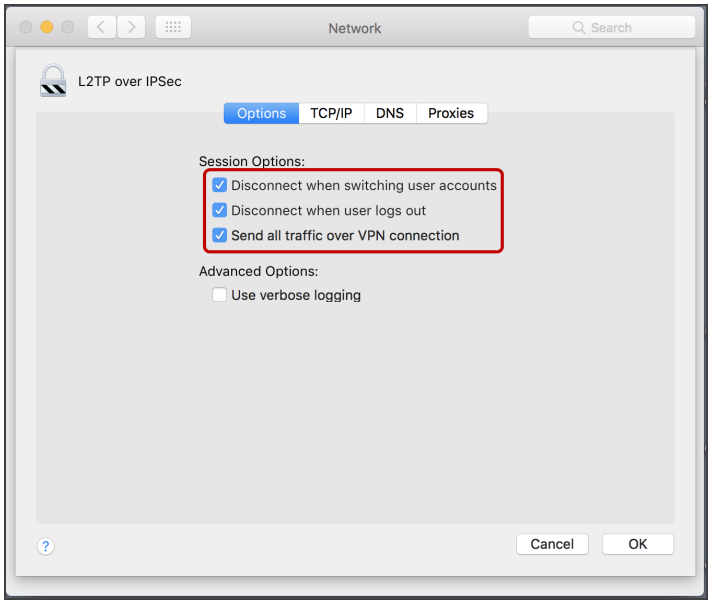


1. Find **L2TP over IPSec** on the left web page and click it.
2. Enter the **Server Address**on the right web page: 10.10.1.1.
3. Enter the **Account Name**: user1.
4. Click **Authentication Settings** button and enter authentication password in the pop-up dialog.
5. In the **User Authentication** section, select **Password**button and enter the corresponding password: hillstone.
6. In the **Machine Authentication** section, select **Shared Secret** button in the Machine Authentication and enter the **Shared Secret**: hillstone.
7. Click **OK** to save the configurations.

Steps of setting up a VPN connection in Mac OS

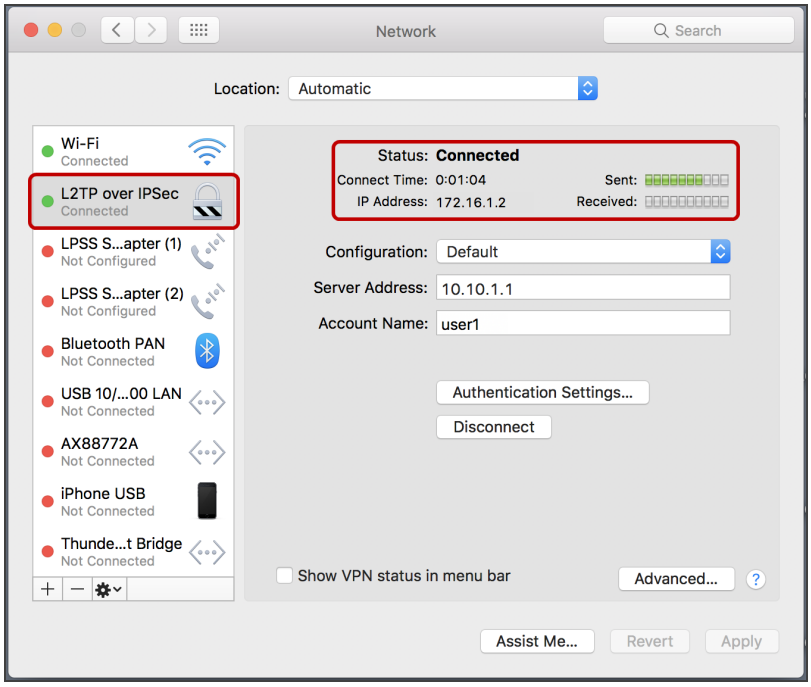
Configure the advanced properties of connection:

1. Click **Advanced** button.
2. Configure the advanced properties in the pop-up dialog.
3. Select all the check boxes in **Session Options** and make sure that the check box of **Send all traffic over VPN connection** is selected.
4. Click **OK** to save the configurations.



Connect to the L2TP over IPSec VPN:

1. Find **L2TP over IPSec** on the left web page and click it.
2. Click **Connect** button on the right page.
3. The status shows **Connecting**.
4. After connecting successfully, the page shows Status: **Connected**, Connect Time and so on.
5. Click **Apply** to save the configurations.
6. After the connection is successful, you can visit the intranet server 192.168.1.2.
7. If you need to disconnect the connection, click **Disconnect** button.

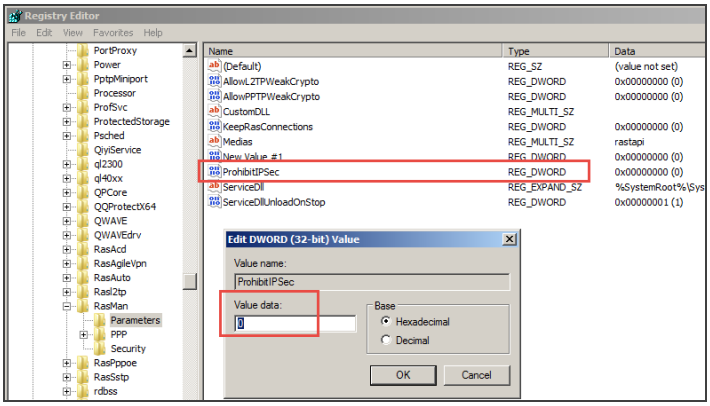


Adjusting Whether to Use IPSec for L2TP VPN

By default, the L2TP VPN is required by Windows to use IPSec. For the above L2TP over IPSec VPN, you do not need to modify the system's registry.

If the system has disabled IPSec, take the following steps to make the system use L2TP over IPSec:

Enable IPSec



1. Select **Start > Run**.
2. In **Run**, enter **regedit**.
3. Click **OK**.
4. Navigate to **HKEY_Local_Machine\System\CurentControl Set\Services\RasMan\Parameters**.
5. In the right pane, find the entry **ProhibitIPSec** whose type is **REG_DWORD**.
6. Double-click this entry and modify the value in the **Value data** text box to **0**.
   - **0** represents that the system enables IPSec.
   - **1** represents that the system disables IPSec.
7. Save the modifications and restart the system.

Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN

This example shows how to use L2TP over IPSec VPN to provide remote users (iOS/Android) with access to corporate internal network.

The topology is shown as below. A remote user, located at home or a hotel, accesses the Internet via mobile 3G/4G or Wi-Fi. This remote user (iOS/Android) uses L2TP over IPSec VPN to visit the server (PC1) in the corporate internal network. And this server is protected by the device A.



*Due to lab environment, use 10.10.1.0./24 to represent the public network segment.

The configuration process consists of five parts:

- Configure basic settings
- Configure IPSec VPN
- Configure L2TP VPN
- Set up a VPN connection in iOS/Android

Configuring Basic Settings

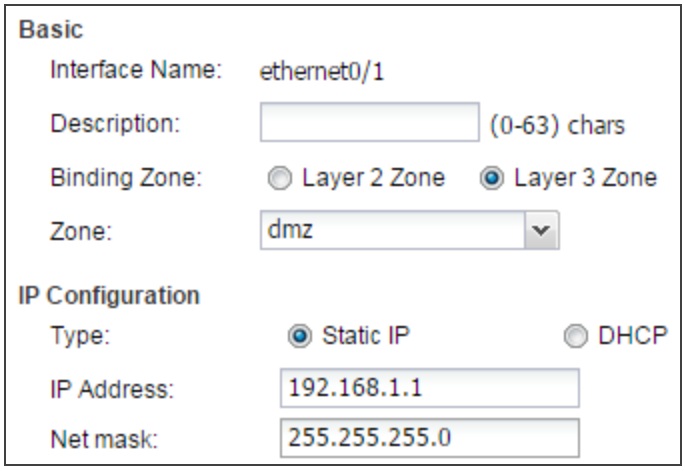
In device A, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/1.

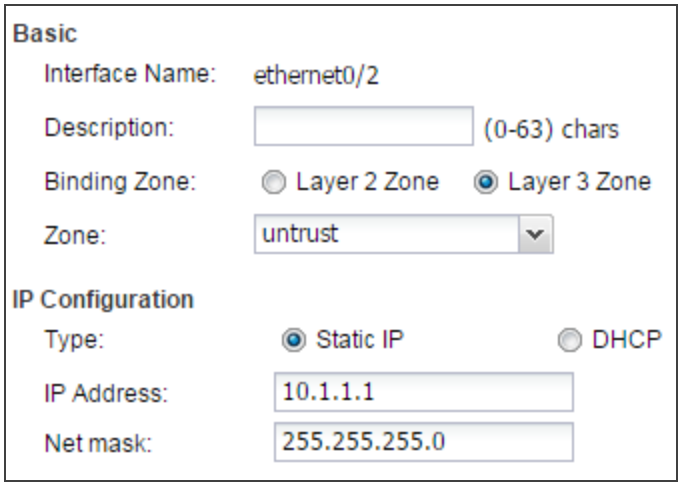
- Binding Zone: Layer 3 Zone
- Zone: dmz
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/2.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.10.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

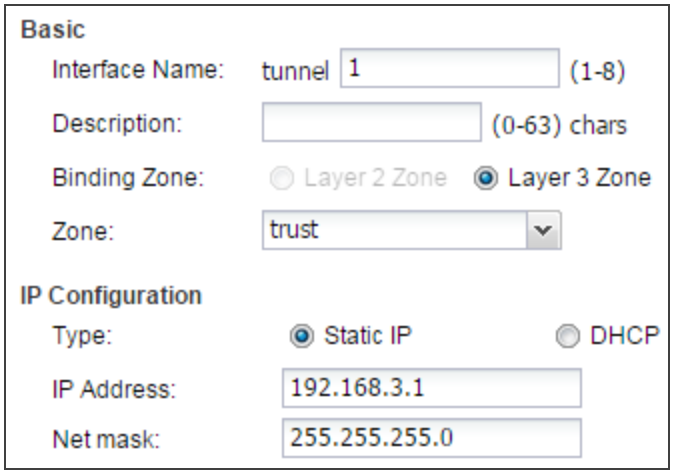


Step 1: Configuring an interface

Configuring the tunnel interface.

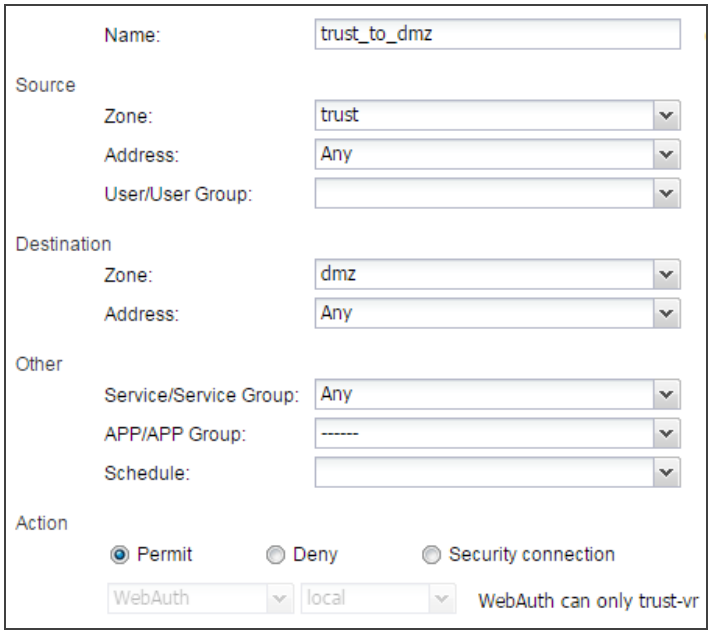
Select **Network > Interface > New > Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 192.168.3.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 2: Configuring a security policy

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the DMZ zone where the internal server locates.



Select **Policy > Security Policy > New**.

- Name: trust_to_dmz
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: dmz
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

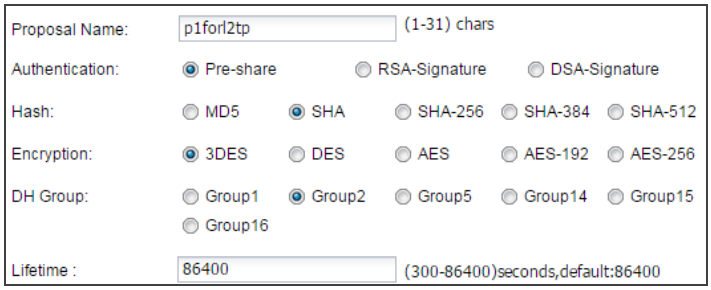
Configuring IPSec VPN

In device A, configure the following settings:

Step 1: Creating a P1 proposal and a P2 proposal

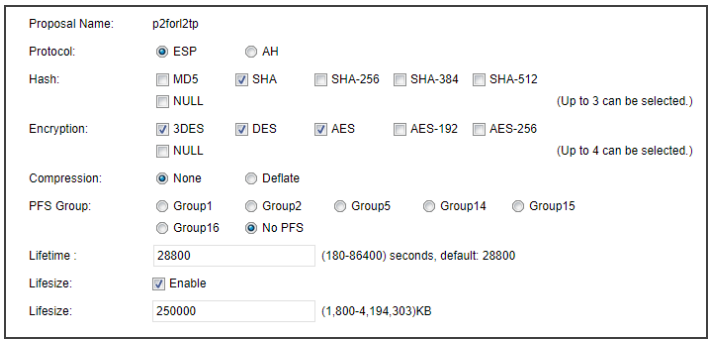
Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forl2tp
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



In the P2 Proposal tab, click **New**.

- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES, DES, AES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800
- Lifesize: Enable
  - Lifesize: 250000

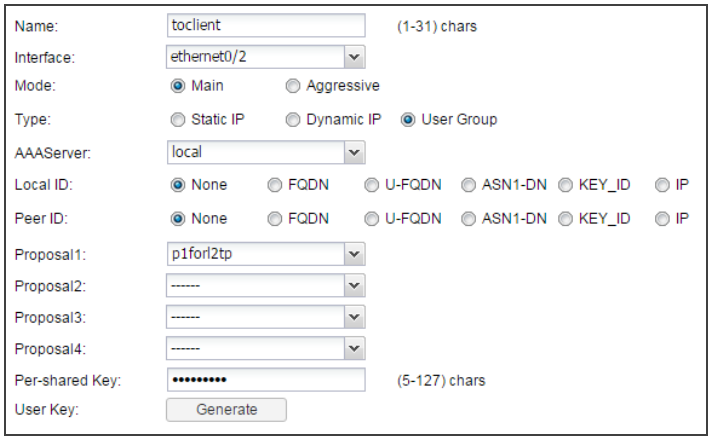


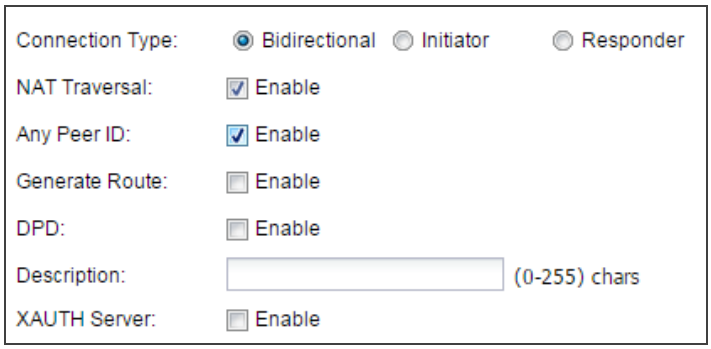
Step 2: Configuring a VPN peer

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

In the Basic tab, configure the following settings:

- Name: toclient
- Interface: ethernet0/2
- Mode: Main
- Type: User Group
- AAA Server: local
- Proposal1: p1forl2tp
- Pre-shared Key: hillstone





In the Advanced tab, configure the following settings:

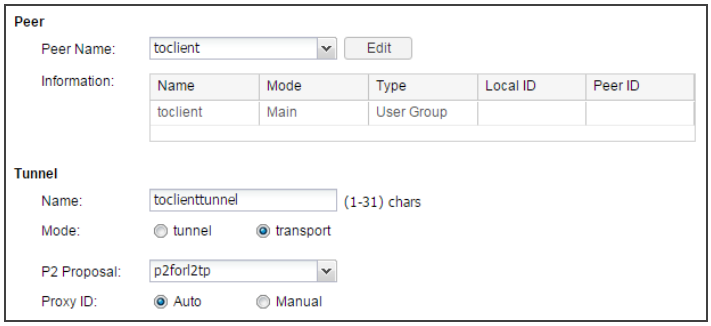
- NAT Traversal: Enable
- Any Peer ID: Enable
- Keep the default of other parameters

Step 3: Configuring IKE VPN

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

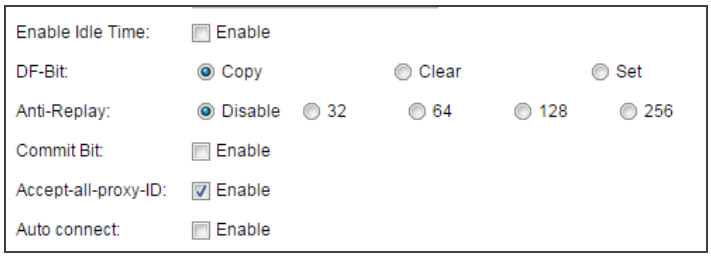
In the Basic tab, configure the following settings:

- Peer
  - Peer Name: toclient
- Tunnel
  - Name: toclienttunnel
  - Mode: transport
  - P2 proposal: p2forl2tp



In the Advanced tab, configure the following settings:

- Accept-all-proxy-ID: Enable
- Keep the default of other parameters



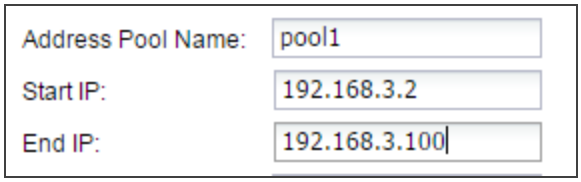
Configuring L2TP VPN

In device A, configure the following settings:

Step 1: Creating a L2TP pool

Select **Network > VPN > L2TP VPN > Address Pool**.

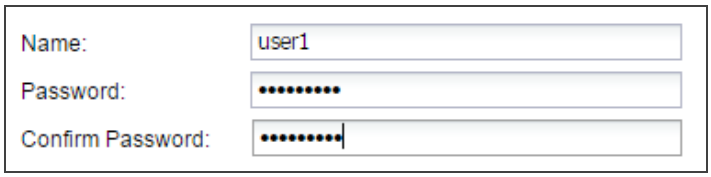
In the Address Pool dialog, click **New**.



- Address Pool Name: pool1
- Start IP: 192.168.3.2
- End IP: 192.168.3.100

Step 2: Adding a user in the 'local' AAA server

Select **Object > User > Local User > New > User**.



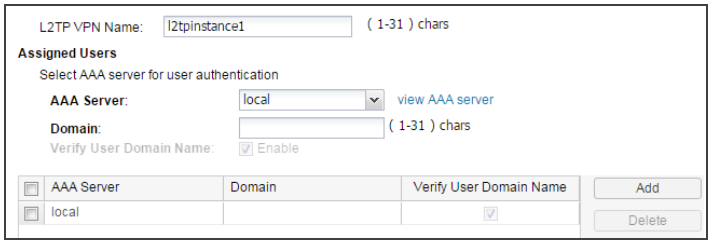
- Name: user1
- Password: hillstone
- Confirm Password: hillstone

Step 3: Configuring a L2TP VPN instance

Select **Network > VPN > L2TP VPN > New**.

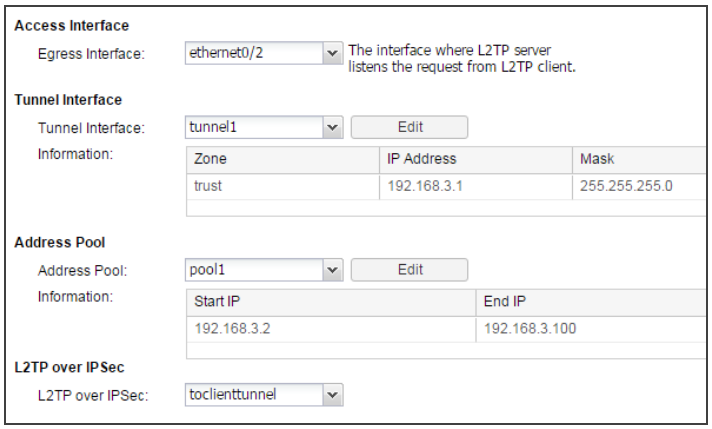
In the Name/Access User tab, configure the following settings:

- L2TP VPN Name: l2tpinstance1
- AAA Server: local
- Click **Add**



In the Interface/Address Pool/IPSec Tunnel tab, configure the following settings:

- Egress Interface: ethernet0/2
- Tunnel Interface: tunnel1
- Address Pool: pool1
- L2TP over IPSec: toclienttunnel



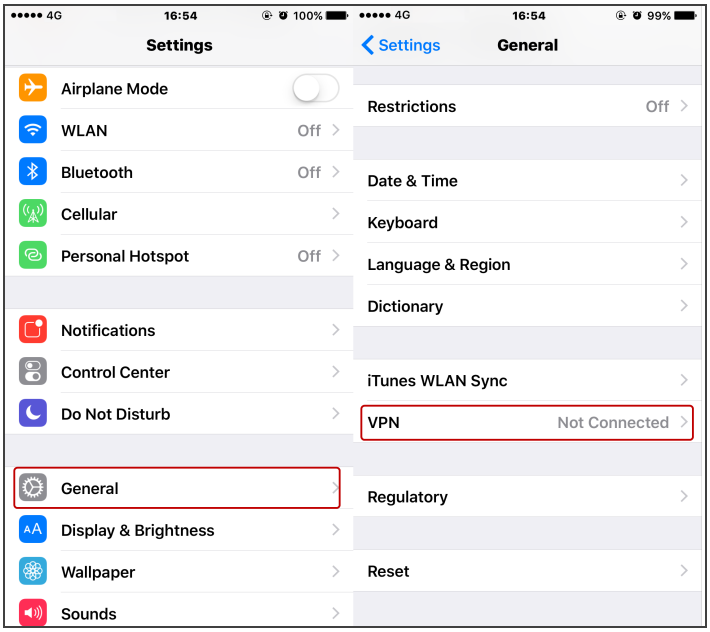
Set up a VPN connection in iOS/Android

Take iOS 10 and Android 7 as examples.

Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)

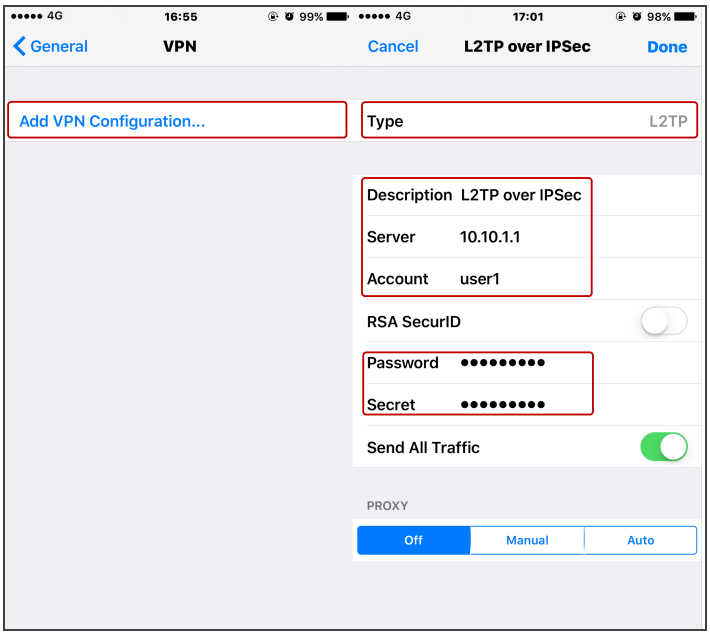
Enter VPN configuration page:

1. Select **Settings** > **General** in your iPhone.
2. Swipe down and click **VPN**.
3. Click **Add VPN Configuration**…



Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Configuring VPN properties:

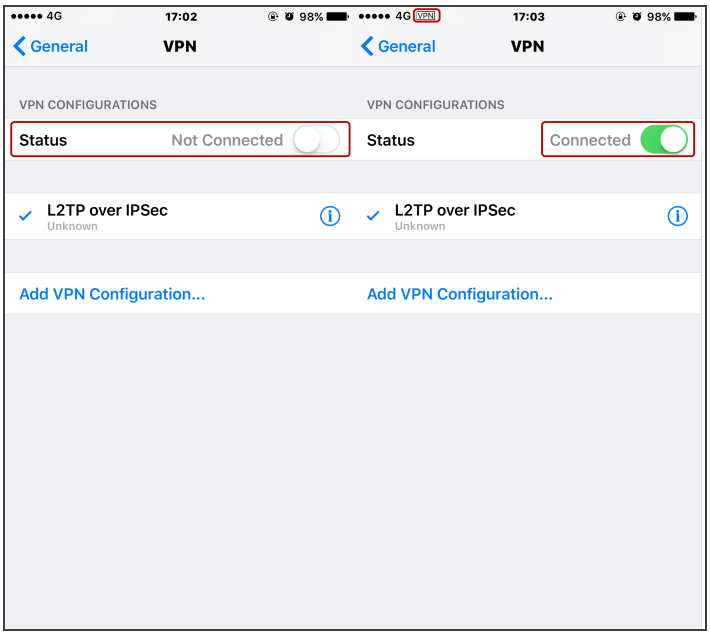


1. Click **Add VPN Configuration** on VPN page.
2. Enter the following configurations on Add Configuration page.
   - Type: Click the drop-down list and select **L2TP**.
   - Description: Enter the custom name **L2TP over IPSec** to mark the L2TP connection.
   - Server: 10.10.1.1
   - Account: user1, the login account that has been added in local AAA server
   - Password: hillstone, the corresponding password of the account.
   - Secret: hillstone, the pre-shared key.
3. Click Done on the top right corner.

Steps of setting up a VPN connection in iOS 10. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enabling VPN and connect L2TP over IPSec VPN:

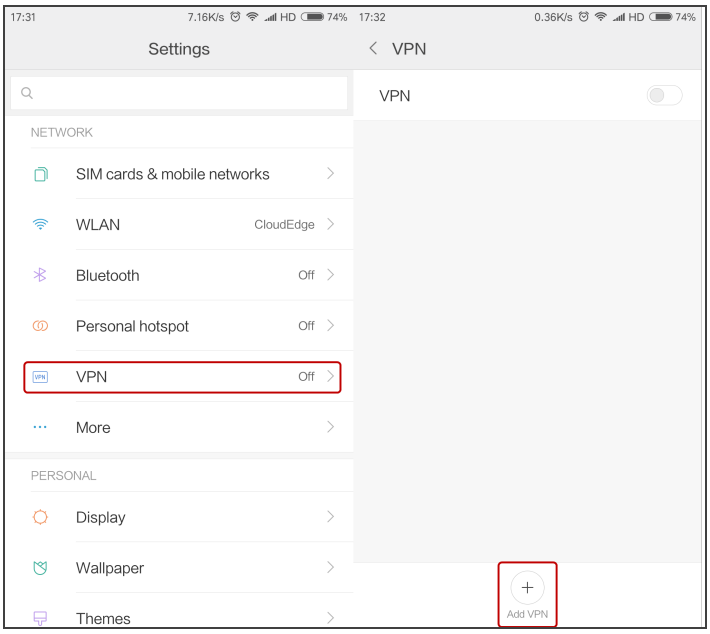
1. Select the configured VPN: **L2TP over IPSec**.
2. Swipe the **Status** button.
3. After VPN being connected successfully, the status shows **Connected** and there will appear VPN on the top of screen.
4. After VPN being connected successfully, you can access the internal server: 192.168.1.2.



Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

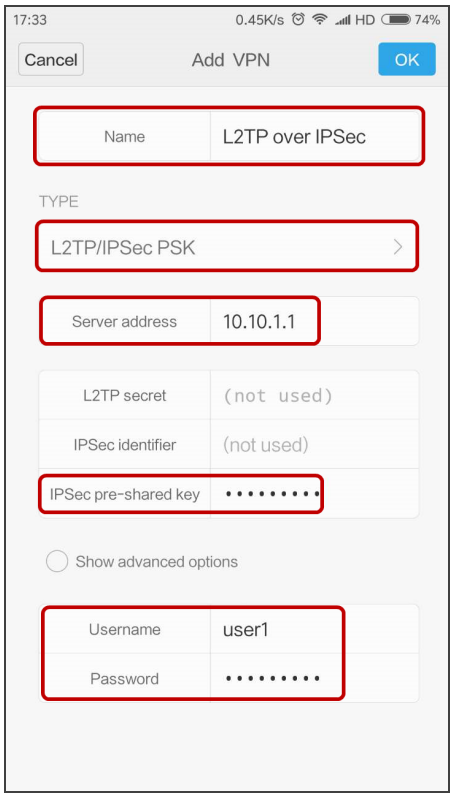
Enter the VPN configuration page:

1. Select **Settings > VPN** in your Android phone.
2. Click **Add VPN** at the bottom of screen.



Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Configuring VPN properties:

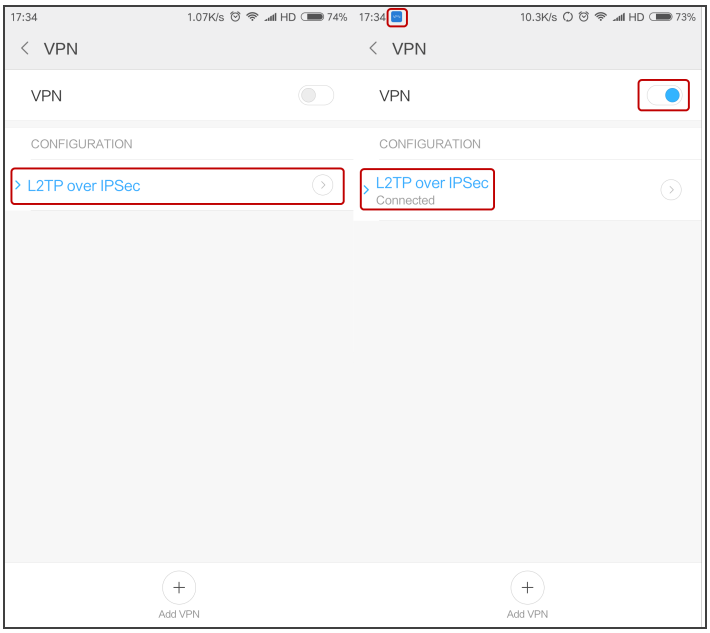


1. Enter the following configurations on Add VPN page.
   - Enter the custom name **L2TP over IPSec** to mark the L2TP connection.
   - TYPE: Click the drop-down list and select **L2TP/IPSec PSK**.
   - Server address: 10.10.1.1
   - IPSec pre-shared key: hillstone
   - Account: user1, the login account that has been added in local AAA server.
   - Password: hillstone, the corresponding password of the account.
2. Click OK on the top right corner.

Steps of setting up a VPN connection in Android. (Before configuring your iPhone, make sure that it can access the Internet normally.)

Enabling VPN and connect L2TP over IPSec VPN:

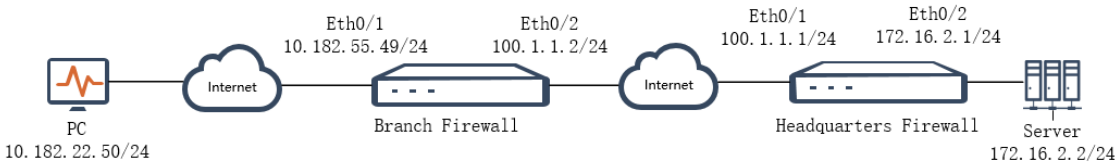
1. Select the configured VPN: **L2TP over IPSec**.
2. Swipe the **VPN** button.
3. After VPN being connected successfully, the status shows **Connected** and there will appear a VPN sign on the top screen.
4. After VPN being connected successfully, you can access the internal server: 192.168.1.2.



Allowing Remote Users (PC) to Access a Private Network Using L2TP and SSL VPN

This example shows how to use L2TP and SSL VPN to provide remote users with access to corporate internal network.

The topology is shown below. A remote user (PC) , located at a branch office of the corporate , uses SSL VPN to visit the branch firewall . The branch firewall functions as an L2TP client to establish a tunnel connection with the headquarters firewall. Then, the traffic from the remote user(PC) is routed to the L2TP tunnel , and the remote user (PC) in the branch office can communicate with the server in the corporate internal network.



* This example is used in a laboratory environment. Please configure the IP addresses of each interface according to the actual connections.

Configure the Branch Firewall

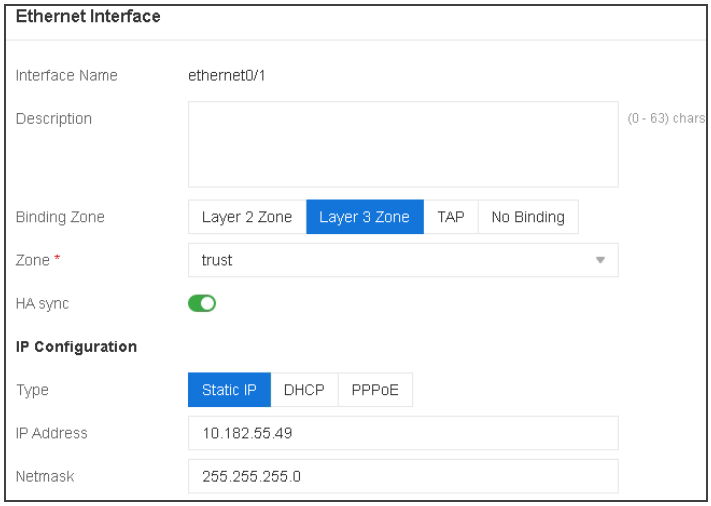
In Branch Firewall, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the branch network

Select **Network > Interface**, and double-click ethernet0/1.

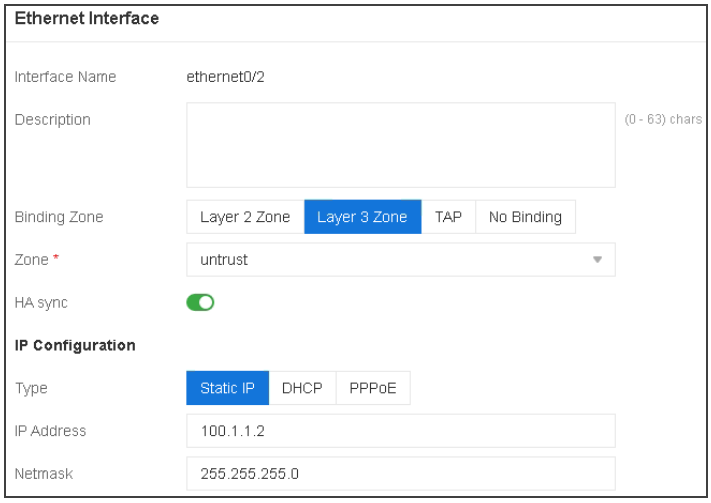
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 10.182.55.49
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/2.

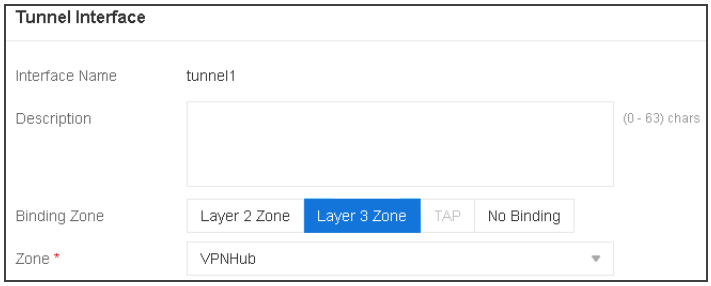
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 100.1.1.2
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 1: Configuring an interface

Configuring the L2TP VPN tunnel interface.

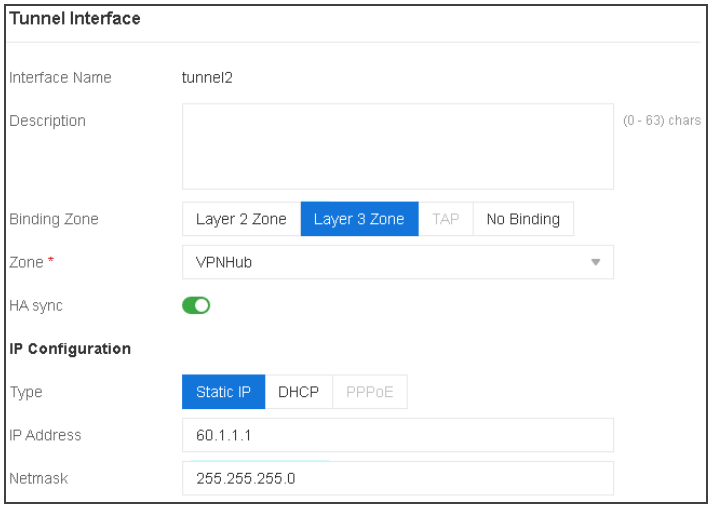
Select **Network > Interface > New > Tunnel Interface**.



- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: VPNHub
- Keep the default of other parameters

Configuring the SSL VPN tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.



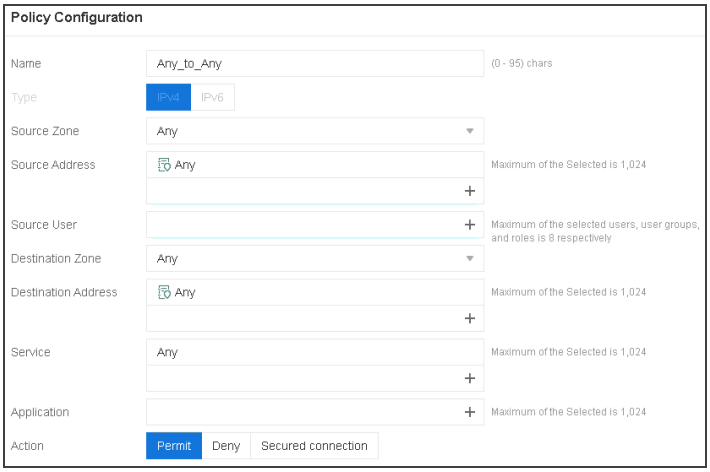
- Interface name: tunnel2
- Binding Zone: Layer 3 Zone
- Zone: VPNHub
- IP Address: 60.1.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

Step 2: Configuring a security policy and NAT

Configure a traffic-all-pass policy

Select **Policy > Security Policy > New**.

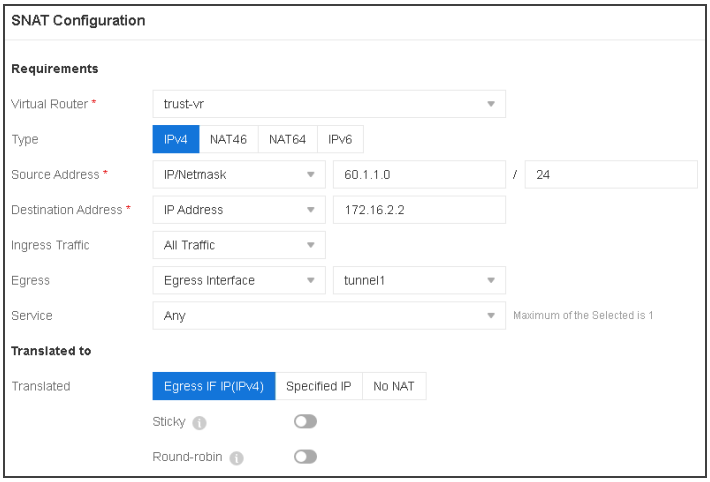
- Name: Any_to_Any
- Source
  - Zone: Any
  - Address: Any
- Destination
  - Zone: Any
  - Address: Any
- Service : Any
- Action: Permit



Step 2: Configuring a security policy and NAT

Configure source NAT to convert the IP address of the branch network to the IP address of the L2TP tunnel interface

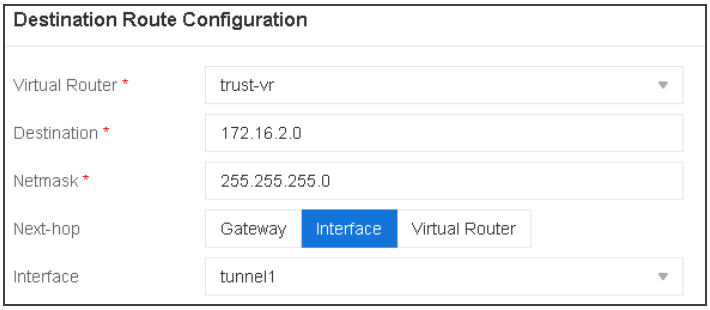
Select **Policy > NAT > SNAT**. Click **New**



- Virtual Router : trust-vr
- Source Address
  - IP/Netmask：60.1.1.0/24
- Destination Address
  - IP Address：172.16.2.2
- Egress：Egress interface ： tunnel1
- Translated to : Egress IF IP(IPv4)
- Keep the default of other parameters

Step 3: Configuring a routing

Select **Network > Routing > Destination Route > New**.



- Destination：172.16.2.0
- Netmask：255.255.255.0
- Next-hop：Interface
- Interface：tunnel1

Step 4: Adding a user in the 'local' AAA server

Select **Object > User > Local User > New > User**.

- Name: user1
- Password: hillstone
- Confirm Password: hillstone

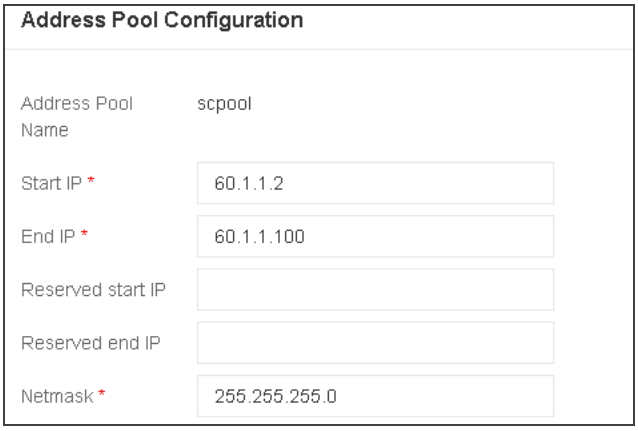


Step 5: Configure SSL VPN

Configure SSL VPN address pool . Select **Network > VPN > SSL VPN**, and click **Configuration > Address Pool** , click **New**.

- Address Pool Name: scpool
- Start IP: 60.1.1.2
- End IP: 60.1.1.100
- Mask: 255.255.255.0
- Keep the default of other parameters

Note: SSL VPN address pool must be of the same network segment of Tunnel interface tunnel2.



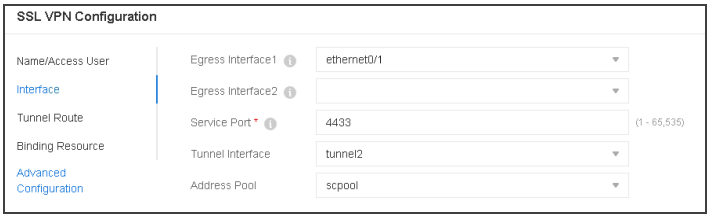
Step 5: Configure SSL VPN

Select **Network > VPN > SSL VPN**, and click **New**.



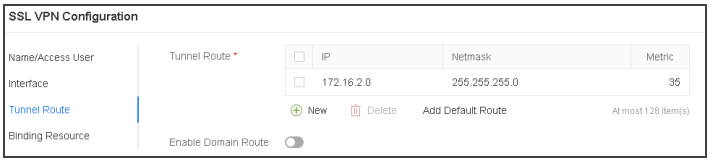
In the Name/Access User tab:

- SSL VPN Name: ssl1
- AAA Server: click **New** , and select **local**



In the Interface tab:

- Egress Interface 1: ethernet0/1
- Service port: 4433
- Tunnel Interface: tunnel2
- Address Pool: scpool



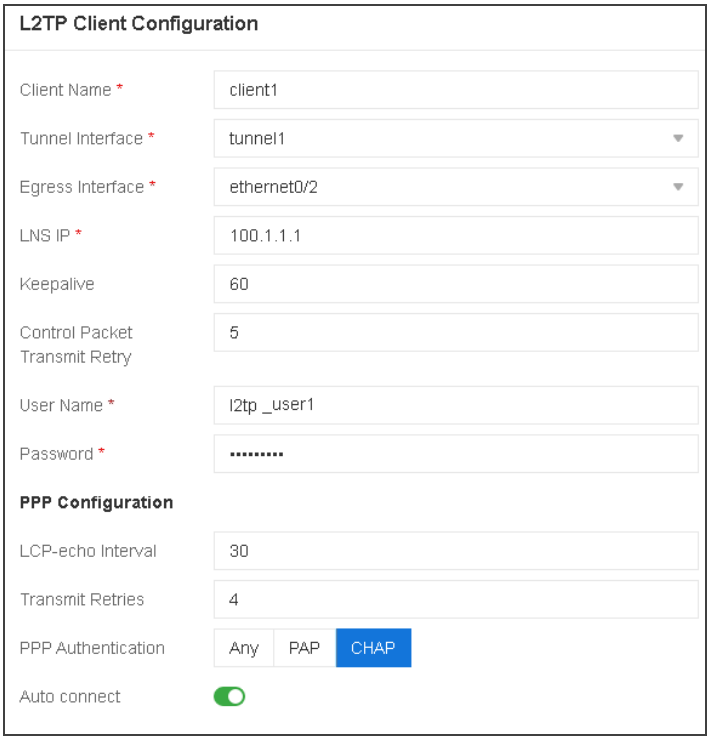
In the Tunnel Route tab:

- IP: 172.16.2.0
- Netmask: 255.255.255.0

Note : Tunnel route must be of the same network segment of internal server ("Server")

Step 6: Configuring a L2TP Client instance

Select **Network > VPN > L2TP VPN >L2TP Client > New**.



- Client Name: client1
- Tunnel Interface: tunnel1
- Egress Interface: ethernet0/2
- LNS IP：100.1.1.1
- Keepalive：60 seconds
- Control Packet Transmit Retry：5 times
- User Name：l2tp_user1
- Password：hillstone
- LCP-echo Interval：30 seconds
- Transmit Retries：4 times
- PPP Authentication：CHAP
- Auto connect：Enabled

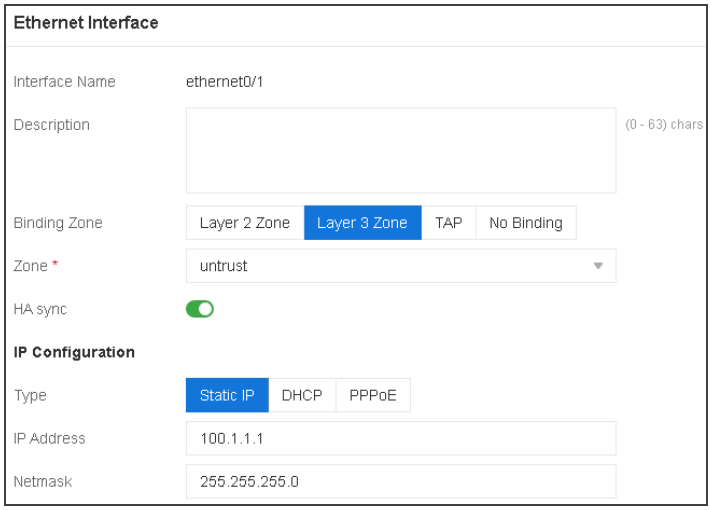
Configure Headquarters Firewall

In the Headquarters Firewall, configure the following settings:

Step 1: Configuring an interface

Configuring the interface connected to the Internet

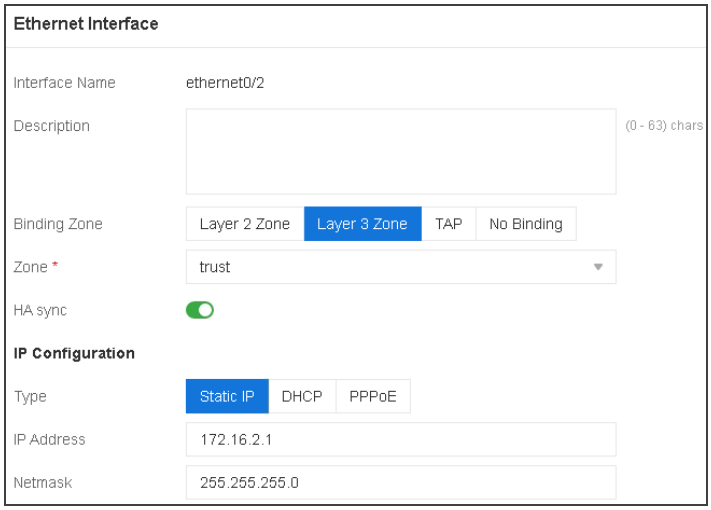
Select **Network > Interface**, and double-click ethernet0/1.



- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 100.1.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

Configuring the interface connected to internal network

Select **Network > Interface**, and double-click ethernet0/2.



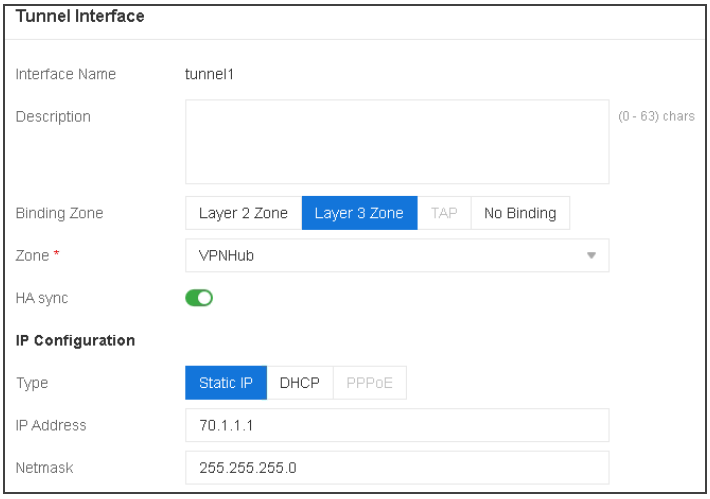
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 172.16.2.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

Step 1: Configuring an interface

Configuring the L2TP VPN tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.

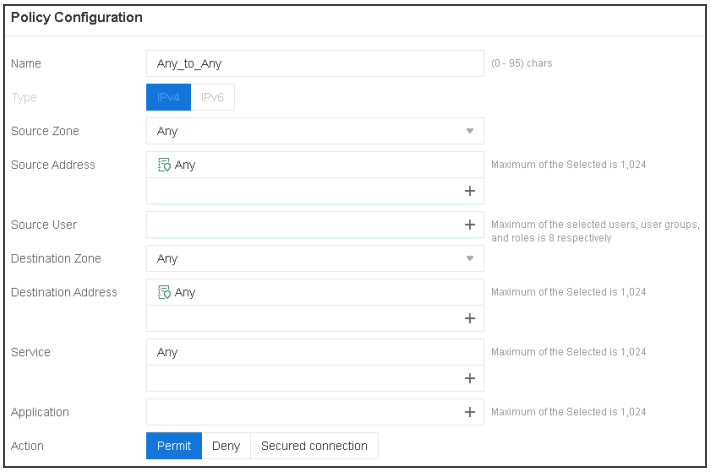
- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: VPNHub
- IP Address: 70.1.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Step 2: Configuring a security policy

Configure a traffic-all-pass policy

Select **Policy > Security Policy > New**



- Name: Any_to_Any
- Source
  - Zone: Any
  - Address: Any
- Destination
  - Zone: Any
  - Address: Any
- Service: Any
- Action: Permit

Step 3: Adding a user in the 'local' AAA server

Select **Object > User > Local User > New > User.**

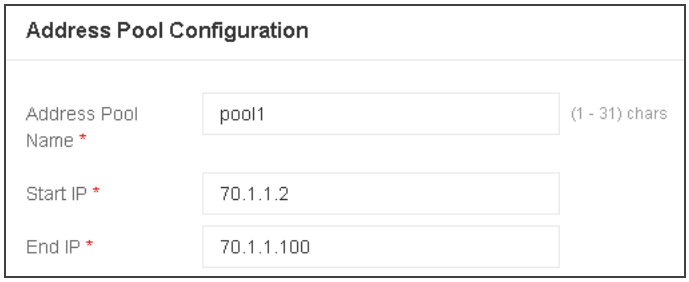


- Name: l2tp_user1
- Password: hillstone
- Confirm Password: hillstone

Step 4: Creating a L2TP pool

Select **Network > VPN > L2TP VPN > Address Pool**.

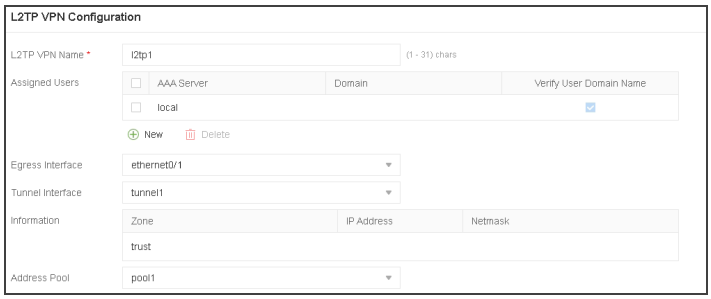
In the Address Pool dialog, click **New**.



- Address Pool Name: pool1
- Start IP: 70.1.1.2
- End IP: 70.1.1.100

Step 5: Configuring a L2TP VPN

Select **Network > VPN > L2TP VPN > New**.



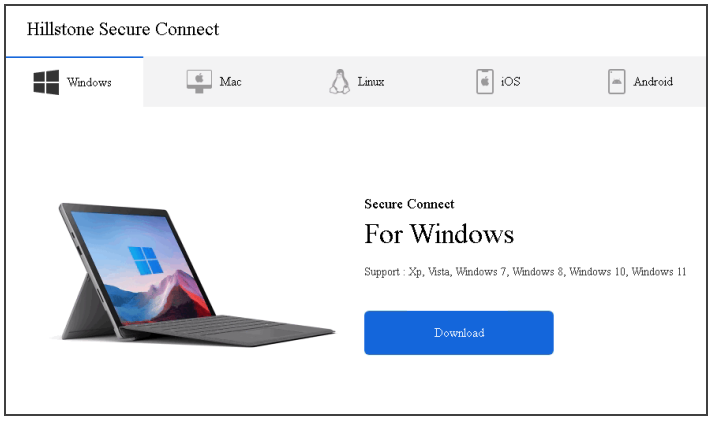
- L2TP VPN Name: l2tp1
- AAA Server: local
- Egress Interface: ethernet0/1
- Tunnel Interface: tunnel1
- Address Pool: pool1
- Keep the default of other parameters

Setting up a VPN Connection

After completing the above configuration, users in the branch office can dial-up to connect to the intranet server.

Step 1: Download Hillstone Secure Connect client

Enter https://10.182.55.49:4433 in the browser, and download the SCVPN client on the page that pops up. The IP address: 10.182.55.49 is the IP address of the egress interface of the SSL VPN



Step 2: Log in

The remote user open the Hillstone Secure Connect client, and enter information below:

- Server: 10.182.55.49
- Port: 4433
- Username: user1
- Password: hillstone

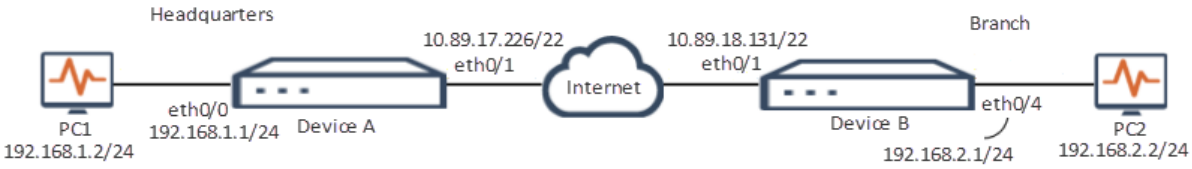
When the icon in the taskbar becomes green, the client is connected. Then, the remote user access the internal server via SSL VPN and L2TP VPN.



Connection between Two Private Networks Using GRE over IPSec VPN

This example introduces how to create GRE over IPSec VPN to protect the communication between the private network of the headquarters and the private network of the branch.

The topology is shown as below. Device A acts as the gateway of the headquarters and device B acts as the gateway of the branch. To protect the communication between two private networks, use GRE over IPSec VPN.



*Due to lab environment, use 10.89.16.0/22 to represent the public network segment.

The configuration process consists of five parts:

- Configure basic settings
- Configure IPSec VPN
- Configure GRE VPN
- Configure route and policies

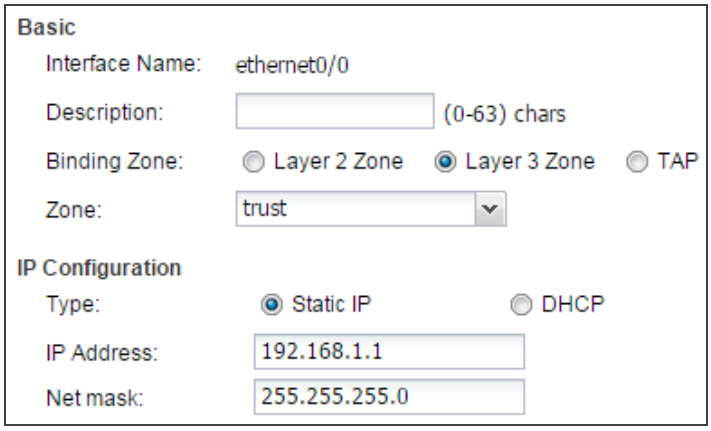
Configuring Basic Settings

Step 1: Configuring interfaces for device A

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/0.

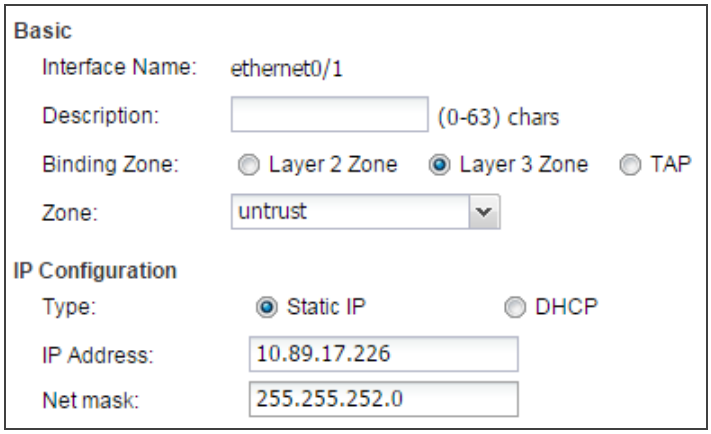
- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.1.1
- Netmask: 255.255.255.0
- Keep the default of other parameters



Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/1.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.89.17.226
- Netmask: 255.255.252.0
- Keep the default of other parameters

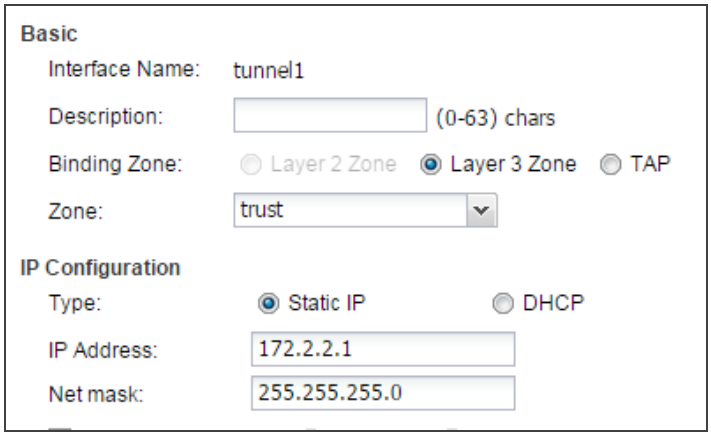


Step 1: Configuring interfaces for device A

Configuring the tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 172.2.2.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

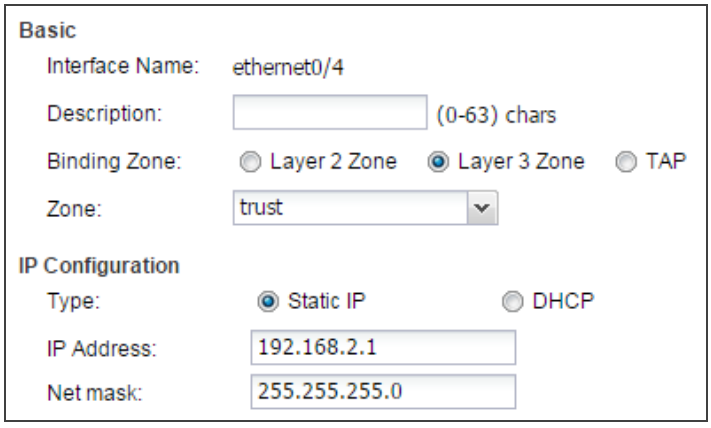


Step 2: Configuring interfaces for device B

Configuring the interface connected to the intranet

Select **Network > Interface**, and double-click ethernet0/4.

- Binding Zone: Layer 3 Zone
- Zone: trust
- Type: Static IP
- IP Address: 192.168.2.1
- Netmask: 255.255.255.0
- Keep the default of other parameters

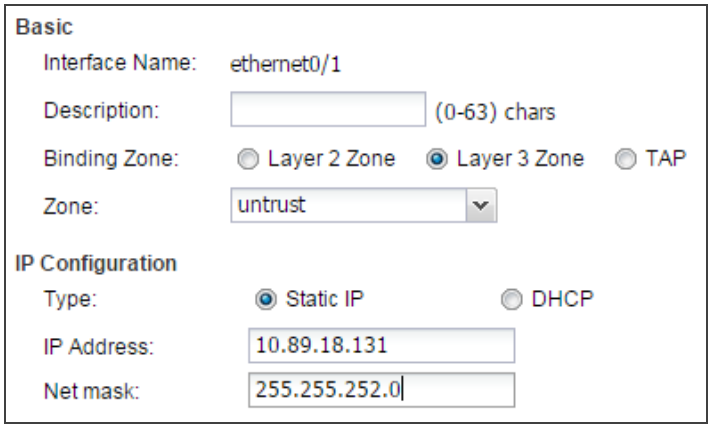


Step 2: Configuring interfaces for device B

Configuring the interface connected to Internet

Select **Network > Interface**, and double-click ethernet0/1.

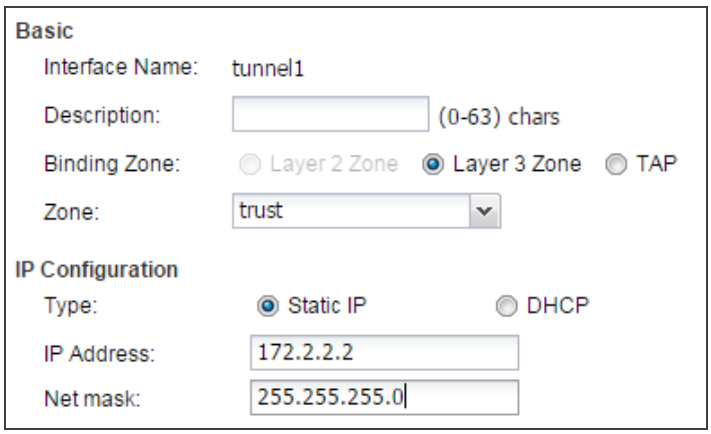
- Binding Zone: Layer 3 Zone
- Zone: untrust
- Type: Static IP
- IP Address: 10.89.18.131
- Netmask: 255.255.252.0
- Keep the default of other parameters



Configuring the tunnel interface.

Select **Network > Interface > New > Tunnel Interface**.

- Interface name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: trust
- IP Address: 172.2.2.2
- Netmask: 255.255.255.0
- Keep the default of other parameters



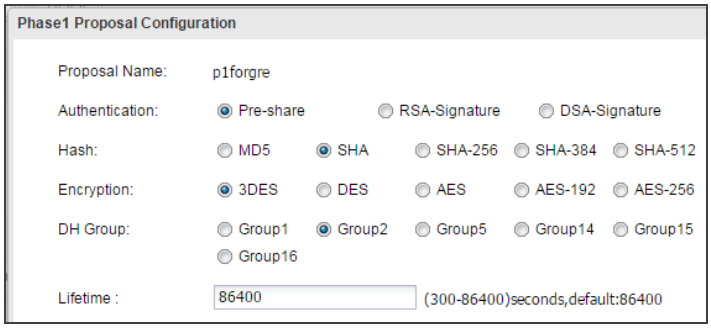
Configuring IPSec VPN

Step 1: Configuring IPSec VPN for device A

Create a P1 proposal and a P2 proposal.

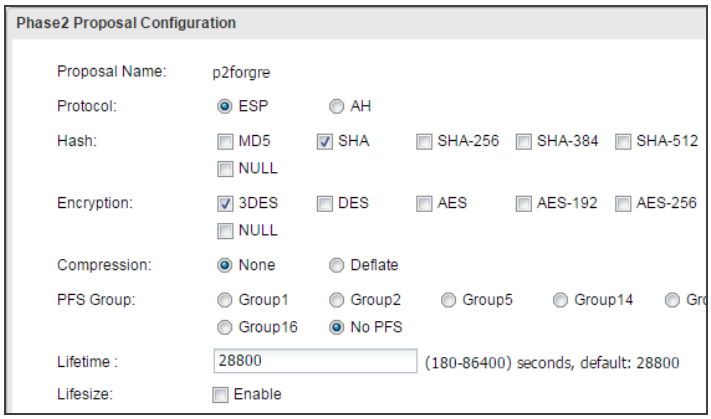
Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forgre
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



In the P2 Proposal tab, click **New**.

- Proposal Name: p2forl2tp
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800

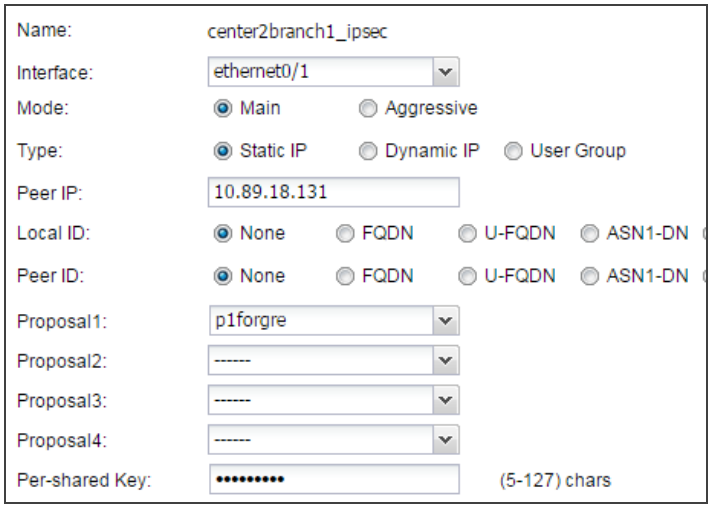


Step 1: Configuring IPSec VPN for device A

Configure a VPN peer.

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

In the Basic tab, configure the following settings:



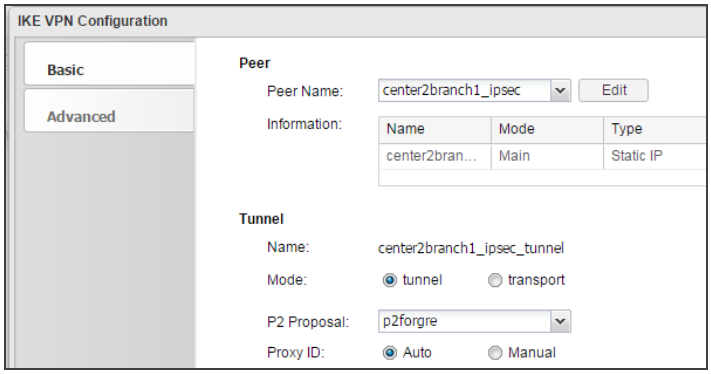
- Name: center2branch1_ipsec
- Interface: ethernet0/1
- Mode: Main
- Type: Static IP
- Peer IP: 10.89.18.131
- Proposal1: p1forgre
- Pre-shared Key: hillstone
- Keep the default of other parameters

Step 1: Configuring IPSec VPN for device A

Configure IKE VPN.

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the following settings:



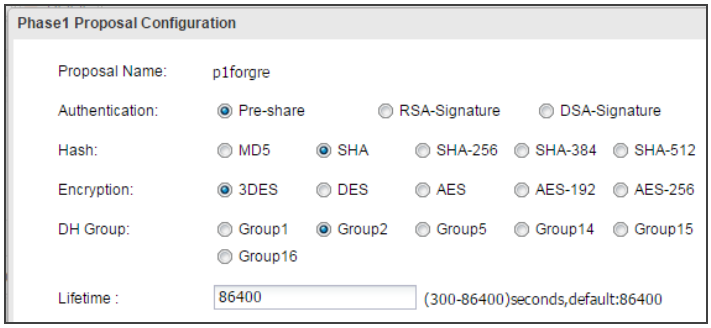
- Peer
  - Peer Name: center2branch1_ipsec
- Tunnel
  - Name: center2branch1_ipsec_tunnel
  - Mode: tunnel
  - P2 proposal: p2forgre
- Keep the default of other parameters

Step 2: Configuring IPSec VPN for device B

Create a P1 proposal and a P2 proposal.

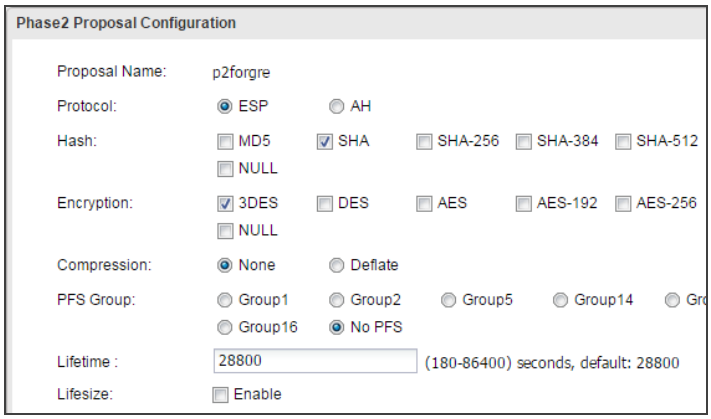
Click **Network > VPN > IPSec VPN**. In the P1 Proposal tab, click **New**.

- Proposal Name: p1forgre
- Authentication: Pre-share
- Hash: SHA
- Encryption: 3DES
- DH Group: Group2
- Lifetime: 86400



In the P2 Proposal tab, click **New**.

- Proposal Name: p2forgre
- Protocol: ESP
- HASH: SHA
- Encryption: 3DES
- Compression: None
- PFS Group: No PFS
- Lifetime: 28800

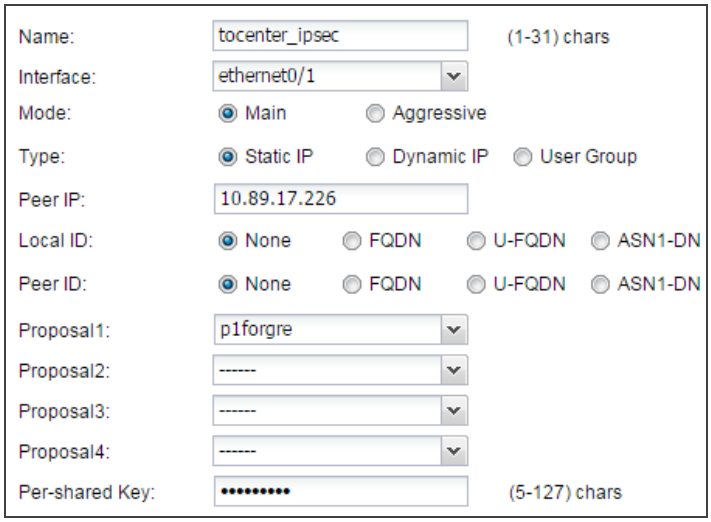


Step 2: Configuring IPSec VPN for device B

Configure a VPN peer.

Click **Network > VPN > IPSec VPN**. In the VPN Peer List tab, click **New**.

In the Basic tab, configure the following settings:



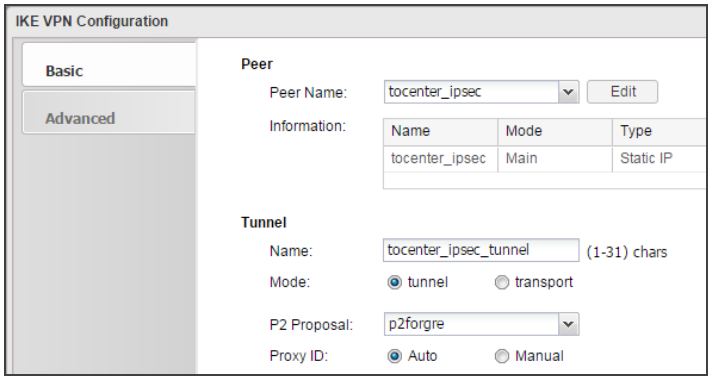
- Name: tocenter_ipsec
- Interface: ethernet0/1
- Mode: Main
- Type: Static IP
- Peer IP: 10.89.17.226
- Proposal1: p1forgre
- Pre-shared Key: hillstone
- Keep the default of other parameters

Step 2: Configuring IPSec VPN for device B

Configure IKE VPN.

Click **Network > VPN > IPSec VPN**. In the IKE VPN List tab, click **New**.

In the Basic tab, configure the following settings:



- Peer
  - Peer Name: tocenter_ipsec
- Tunnel
  - Name: tocenter_ipsec_tunnel
  - Mode: tunnel
  - P2 proposal: p2forgre
- Keep the default of other parameters

Configuring GRE VPN

GRE VPN configurations are not supported by WebUI. You need to use CLI to complete the following GRE VPN configurations.

Step 1: Configuring GRE VPN for device A

Create a GRE tunnel.

```
Device-A(config)# tunnel gre center2branch1
Device-A(config-tunnel-gre)# source 10.89.17.226
Device-A(config-tunnel-gre)# destination 10.89.18.131
Device-A(config-tunnel-gre)# interface eth0/1
Device-A(config-tunnel-gre)# next-tunnel ipsec center2branch1_ipsec_tunnel
```

1. In the global configuration mode, create a GRE tunnel:
   tunnel gre center2branch1
2. Specify the source IP address of the tunnel:
   source 10.89.17.226
3. Specify the destination IP address of the tunnel:
   destination 10.89.18.131
4. Specify the egress interface of the tunnel:
   interface ethernet0/1
5. Specify the IPSec VPN tunnel:
   next-tunnel ipsec center2branch1_ipsec_tunnel

Bind the GRE tunnl to the tunnel interface.

```
Device-A(config)# int tunnel1
Device-A(config-if-tun1)# tunnel gre center2branch1
```

1. Enter the interface configuration mode of tunnel1:
   int tunnel1
2. Bind the GRE tunnel:
   tunnel gre center2branch1

Step 2: Configuring GRE VPN for device B

Create a GRE tunnel.

1. In the global configuration mode, create a GRE tunnel:
   tunnel gre branch1
2. Specify the source IP address of the tunnel:
   source 10.89.18.131
3. Specify the destination IP address of the tunnel:
   destination 10.89.17.226
4. Specify the egress interface of the tunnel:
   interface ethernet0/1
5. Specify the IPSec VPN tunnel:
   next-tunnel ipsecto_center_tunnel

```
Device-B(config)# tunnel gre branch1
Device-B(config-tunnel-gre)# source 10.89.18.131
Device-B(config-tunnel-gre)# destination 10.89.17.226
Device-B(config-tunnel-gre)# interface eth0/1
Device-B(config-tunnel-gre)# next-tunnel ipsec to_center_tunnel
```

Bind the GRE tunnl to the tunnel interface.

1. Enter the interface configuration mode of tunnel1: int tunnel1
2. Bind the GRE tunnel: tunnel gre branch1

```
Device-B(config)# int tunnel1
Device-B(config-if-tun1)# tunnel gre branch1
```

Configuring Route and Policies

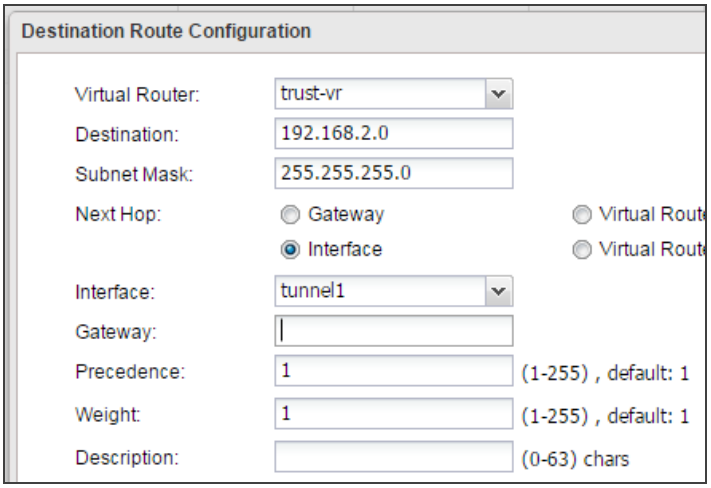
Step 1: Configuring route and policies for device A

Configure routes.

Select **Network > Routing > Destination Route**.

Click **New**.

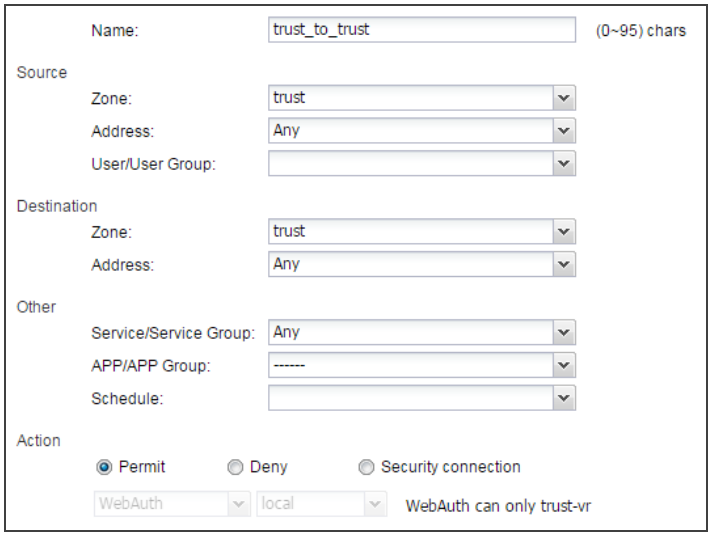
- Destination: 192.168.2.0
- Subnet Mask: 255.255.255.0
- Next Hop: Interface
- Interface: tunnel1
- Keep the default of other parameters



Step 1: Configuring route and policies for device A

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the Trust zone where the internal server locates.

Select **Policy > Security Policy**. Click **New**.



- Name: trust_to_trust
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

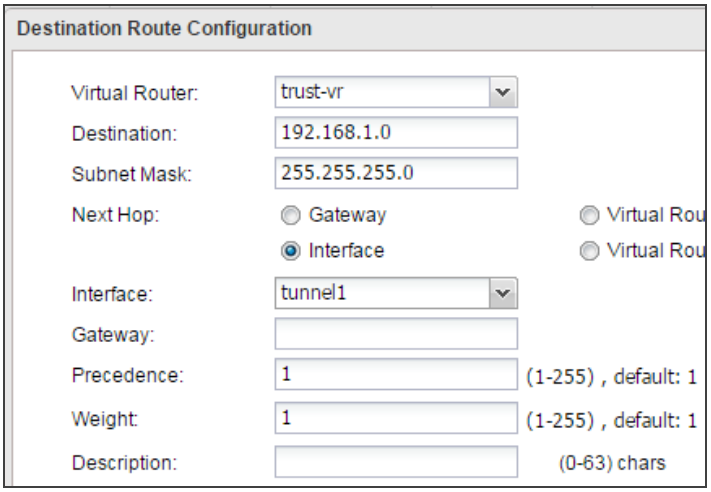
Step 2: Configuring route and policies for device B

Configure routes.

Select Network > Routing > Destination Route.

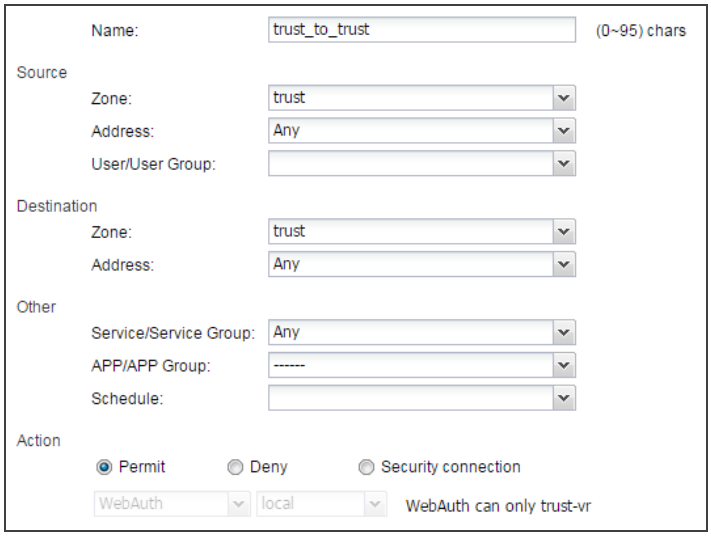
Click **New**.

- Destination: 192.168.1.0
- Subnet Mask: 255.255.255.0
- Next Hop: Interface
- Interface: tunnel1
- Keep the default of other parameters



Step 2: Configuring route and policies for device B

Configure a security policy that allows the traffic to flow from the Trust zone where the tunnel interface locates to the Trust zone where the internal server locates.



Select **Policy > Security Policy > New**.

- Name: trust_to_trust
- Source
  - Zone: trust
  - Address: Any
- Destination
  - Zone: trust
  - Address: Any
- Other
  - Service/Service Group: Any
- Action: Permit

Step 3: Verifying the connection between two private networks

After completing the above steps, the headquarters and branch can visit each other.

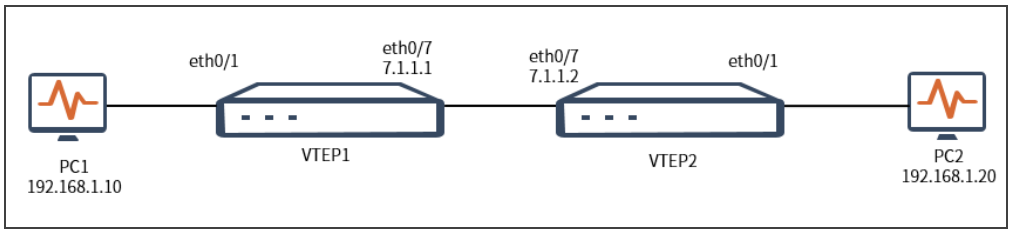
```
C:\Users\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

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.

Zero Trust Network Access (ZTNA)

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. Hillstone ZTNA solutions adopts a dynamic authorization method with user identity being the focus and persistently evaluates the creditability based on user identity and terminal device environment to achieve granular management of user, terminal device and application and realize precise and secure service access control.

- Creditable identity: Identity evaluation is not restricted to account and password authentication but incorporates more identity factors to provide enterprises with fine-grained user access control for profound access security.
- Creditable terminal device: Verified terminal state does not mean permanent access authorization. ZTNA persistently evaluates the terminal environment and dynamically adjust the authorization scope to enure that the connected terminal is always under security control.
- Creditable access: The old security concept that internal network is secure is broken. Any implicit creditability is eliminated. Access to resources will be granted only when the user and the access device satisfy specific requirements so as to effectively mitigate internal network security risks.

This chapter contains the following recipe:

- "Windows User Accessing Internal Server by Using Internal Network Access via ZTNA" on Page 298
- "Windows User Remotely Accessing Internal Server Through ZTNA" on Page 314
- " Android User Remotely Accessing Internal Server Through ZTNA" on Page 335

Windows User Accessing Internal Server by Using Internal Network Access via ZTNA

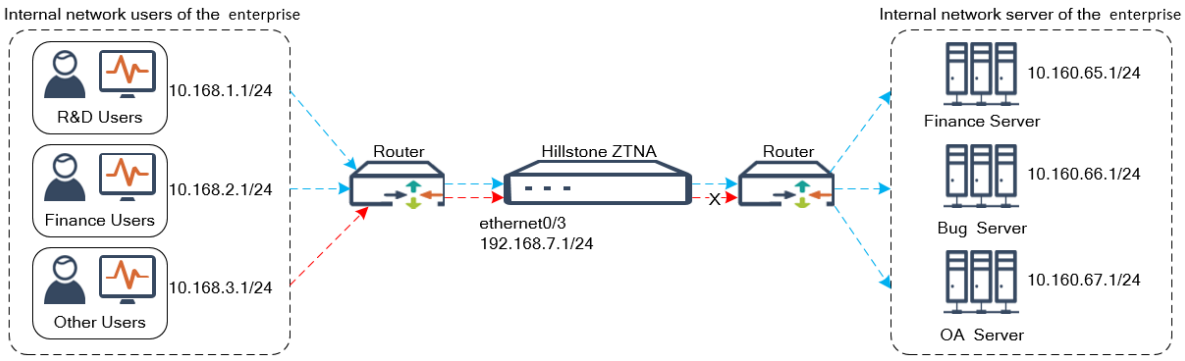
This example shows how to configure the internal network access function via ZTNA to enable Windows users to securely access local servers of the enterprise.

Networking Scenario

The R&D department and finance department of an enterprise are located in different network segments. The R&D department needs to use the intranet application resources including the bug system and OA system; The finance department needs to use the intranet application resources including the finance system and OA system. These three systems are located in different network segments within the enterprise. To improve the internal network security, the enterprise hopes that the employees of these two departments use endpoints that comply with the network security regulations of the company so that they can access the corresponding system resources as expected. Therefore, the enterprise deploys ZTNA internal network access and formulates the following access control policies based on user identity and security requirements for access endpoints:

1. R&D employees are allowed to access the Bug management system and OA system.
2. Finance employees are allowed to access the Finance and OA systems.
3. The access device used for intranet access must meet these requirements: McAfee is run. If McAfee is not run, the employee is allowed only to access the OA system.
4. A user that does not meet any one of the previous requirements will be denied from accessing any resources.

The networking diagram is shown as follows.



Configuration Roadmap

1. Create user group "rd-group" for R&D employees and add R&D employee accounts to it.
2. Create user group "fin-group" for Finance employees and add Finance employee accounts to it.
3. Configure ZTNA server parameters for establishing secure connections from the client to the device and to the application resources:
    a. ZTNA server name: name of the ZTNA service that users will access
    b. Egress interface and service port: address and port number of the ZTNA service
    c. Allow download client from browser: allow users to download ZTNA client by accessing the ZTNA service address in the browser
    d. Forced Timeout: configure the user's online duration after successfully connecting to ZTNA. When the user's online duration reaches the configured time, the system forces the user to go offline.
    e. Multiple login: allow the same user account to log in on multiple clients at the same time
4. Create application resources "Bug System", "Finance System" and "OA System", which correspond with the Bug management system, Finance system and OA system respectively, and set their URL addresses. After a user logs in on the client, the user can view the names and URL addresses of the application resources that are granted and currently not granted access. Application resources that you have permission to access are displayed in blue on the ZTNA Portal page, and application resources that you do not have permission to access are displayed in gray.

5. Configure endpoint tags. For users whose device status fully complies with the network security regulations of the company, set two endpoint tags tag1 and tag2, i.e., tag1 requires the device to be a Windows 10 operating system and to select the corresponding running process of McAfee; tag2 requires the device to be a Windows 10 operating system.

6. Configure and enable ZTNA policies. When a user's group and tag match the ZTNA policy with action Permit, the user is granted access to specific application resources.

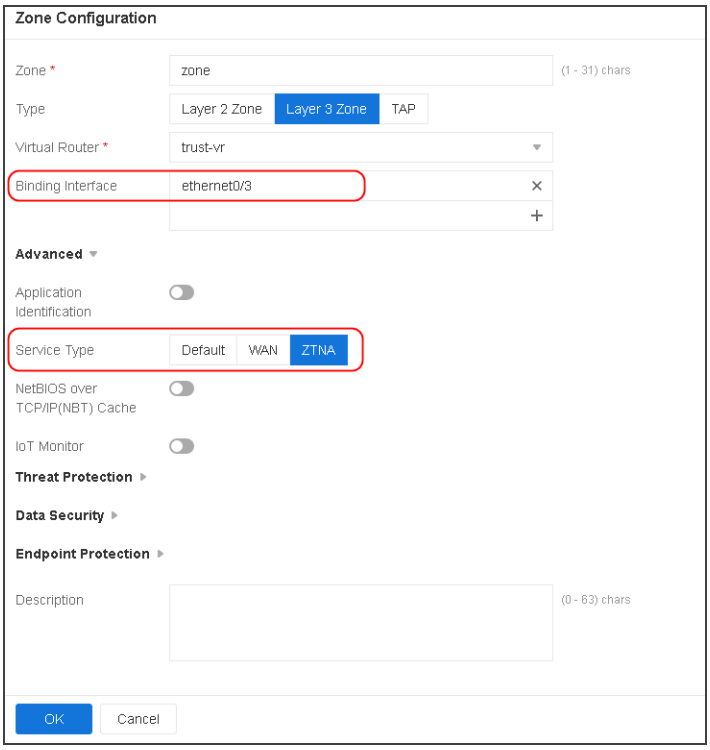
7. Configure the default action as being Deny, so that a user that do not match any ZTNA policy will be denied from accessing any application resources.

Preparations

Please follow the steps below to configure the ZTNA security domain "zone" in advance and bind it to the Egress interface "ethernet0/3". For more information, refer to *StoneOS WebUI User Guide*.

1. Select **Network** > **Zone**.

2. Click **New**, configure the security domain "zone" with "Service Type" as "ZTNA", and bind the security domain to the Egress interface "ethernet0/3".

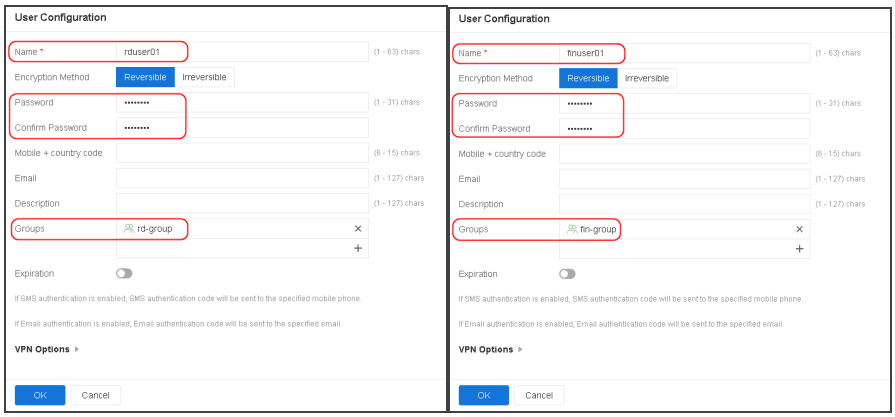


Configuration Steps

Step 1: Creating local users and user groups

Select **ZTNA** > **User** > **Local User**. Click **New** > **User** to create user "rduser01" and set the password, add it to user group "rd-group"

Then, follow the same step to create user "finuser01" and add it to user group "fin-group".



Step 2: Configuring ZTNA

Select **ZTNA** > **Gateway**, and Click **New** > **Intranet Access**, In the Name/Access User tab:

- Server Name: ZTNA-intranet
- Type: IPv4
- Assigned Users: Click **New**, and select "local" for the AAA Server dropdown list

Note: In the **Assigned Users** section, you can configure at most 10 AAA servers. When multiple servers are configured, you need to configure the Domain parameter.

Step 2: Configuring ZTNA



In the Access Interface tab:

- Egress Interfaces: ethernet0/3
- Service port: 8890

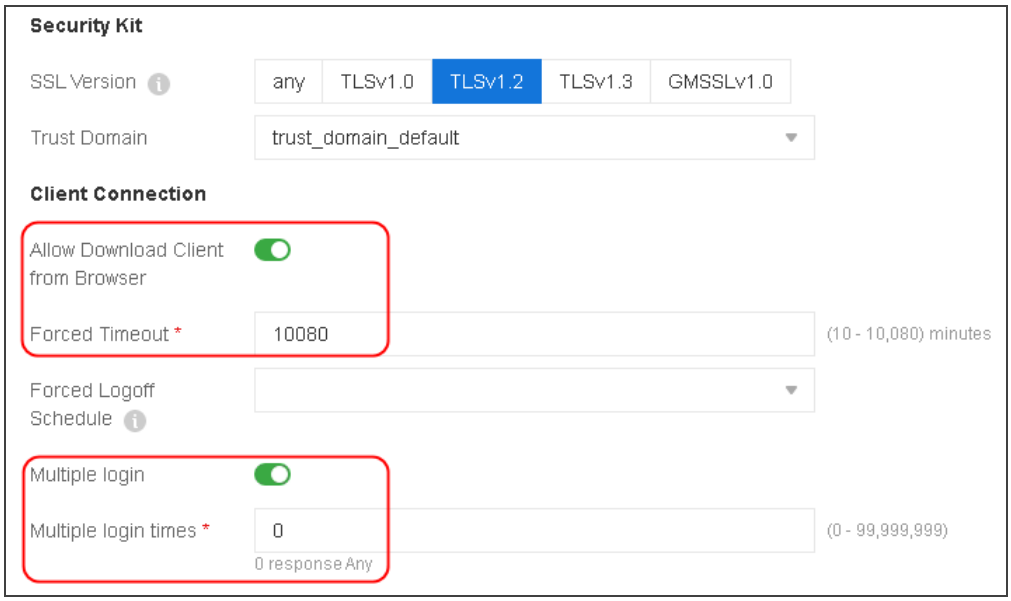
Note: The Egress interface is bound to a security domain with a service type of ZTNA.



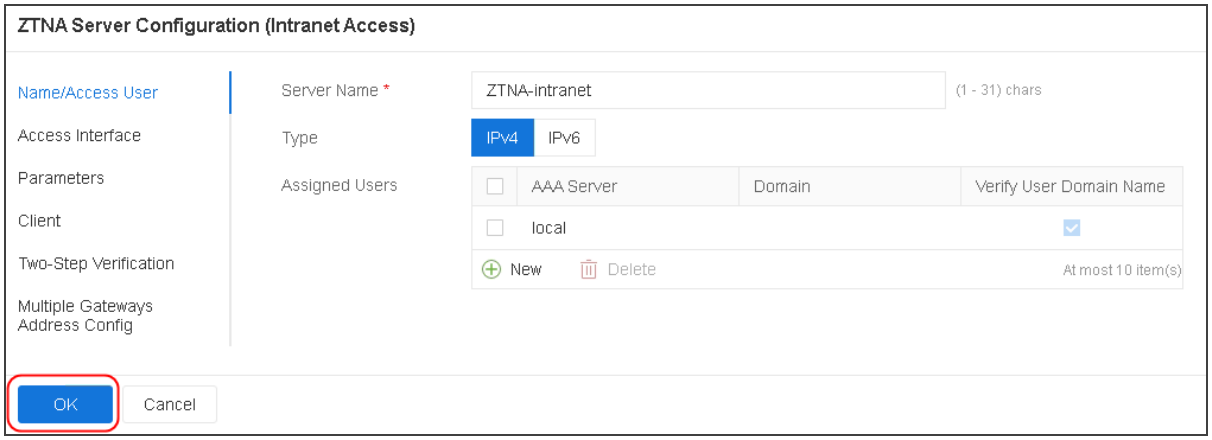
Step 2: Configuring ZTNA

In the Parameters tab, enable the **Allow Download Client from Browser** and **Multiple login** functions and set the **Multiple login times** option to 0. And set the **Forced Timeout** time to 10080.

Note: Use the default values for other parameters.



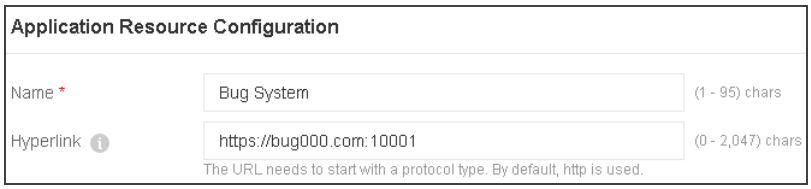
After the ZTNA is completed, click **OK**.

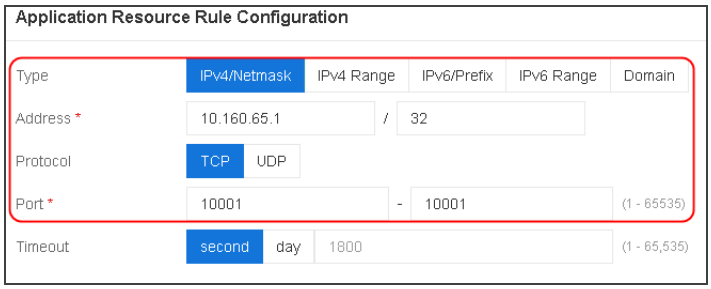


Step 3: Creating application resources

Select **ZTNA > Application Resource Book > Application Resource** and click **New**. In the Application Resource Configuration tab, click **New** to create application resource "Bug System".

- Name: Bug System (Name of the Bug management system displayed on ZTNA portal page)
- Hyperlink: https://bug000.com:10001 (URL address of the Bug management system)
- Address Type: IPv4/Netmask
- Address: 10.160.65.1/32
- Protocol: TCP
- Port: 10001 - 10001





Step 3: Creating application resources

Repeat the previous operation to create application resource "Finance System".

- Name: Finance System (Name of the finance system displayed on ZTNA portal page)
- Hyperlink: https://finance111.com:20001(URL address of the finance system)
- Address Type: IPv4/Netmask
- Address: 10.160.66.1/32
- Protocol: TCP
- Port: 20001 - 20001

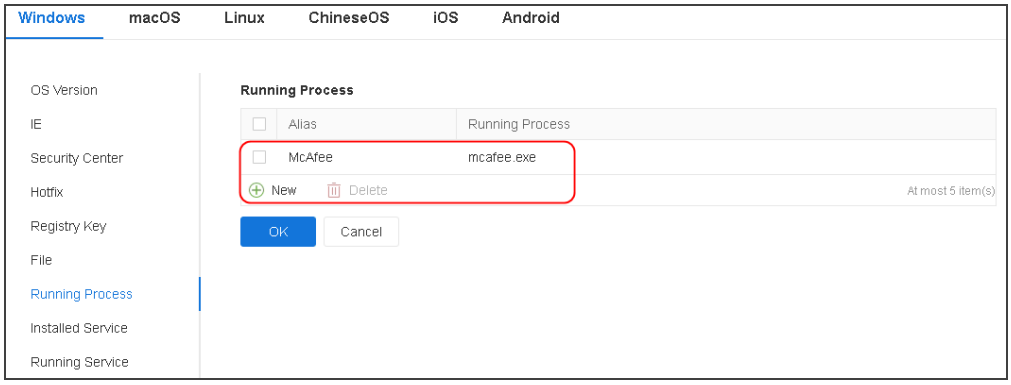
Repeat the previous operation to create application resource "OA System".

- Name: OA System (Name of the OA system displayed on ZTNA portal page)
- Hyperlink: https://oa333.com:30001 (URL address of the OA system)
- Address Type: IPv4/Netmask
- Address: 10.160.67.1/32
- Protocol: TCP
- Port: 30001 - 30001

Step 4: Creating endpoint tags

Select **ZTNA** > **Endpoint** > **Information**. In the **Windows** > **Running Process** tab, click New to add the following running process.

- Alias: McAfee
- Running Process: mcafee.exe (enter the name of the process corresponding to McAfee)



Step 4: Creating endpoint tags

Select **ZTNA** > **Endpoint** > **Tag** and click **New**. In the Tag Configuration tab:

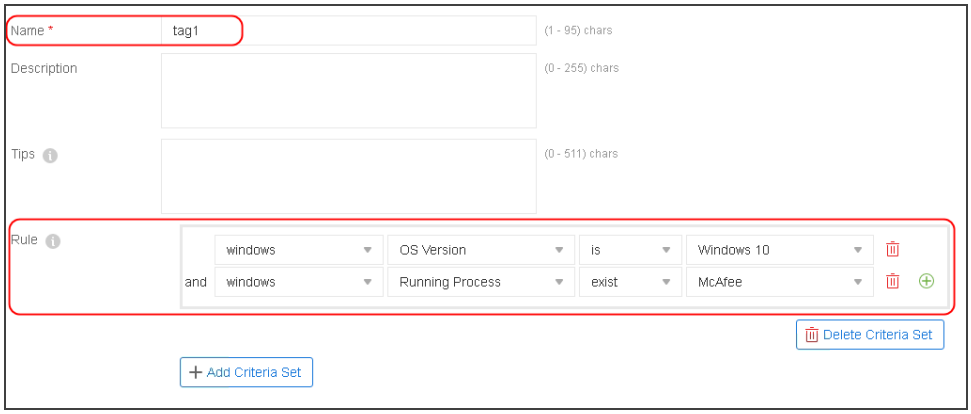
- Name: tag1

Click **Add Criteria Set**:

- Operating System: windows
- Endpoint Info Type: Select **OS Version**. Continue to select **is** and **Windows10**.

Click **+** button to create the following condition:

- Operating System: windows
- Endpoint Info Type: Select **Running Process**. Continue to select **exist** and then **McAfee**.



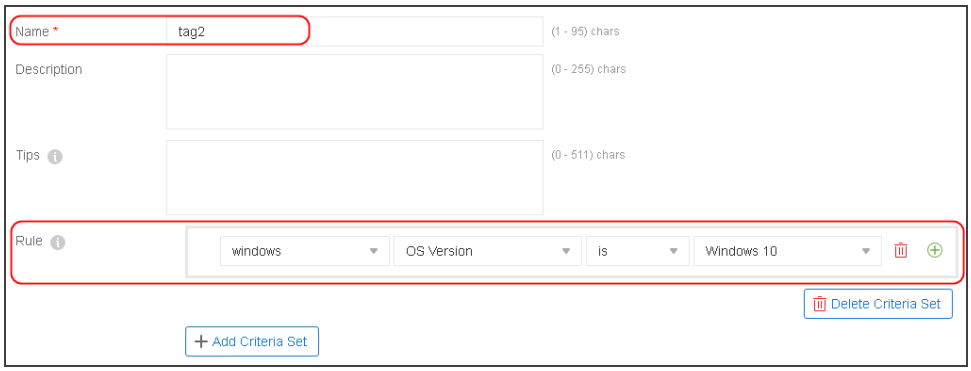
Step 4: Creating endpoint tags

Repeat the previous operation to create "tag2".

- Name: tag2

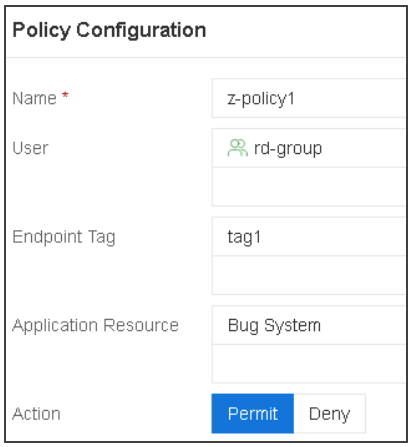
Click **Add Criteria Set**:

- Operating System: windows
- Endpoint Info Type: Select **OS Version**. Continue to select **is** and **Windows10**.



Step 5: Configuring ZTNA policies

Select **ZTNA** > **Policy** and click **New**. In the Policy Configuration tab:

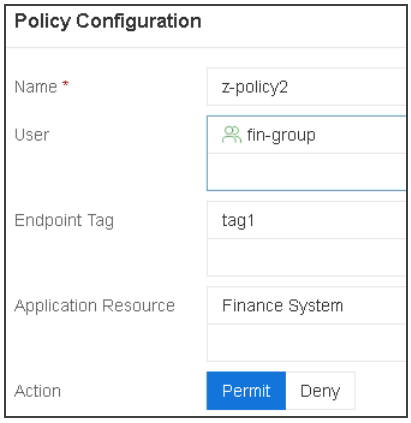


- Name: z-policy1
- User: rd-group
- Endpoint tag: tag1
- Application Resource: Bug System
- Action: Permit

Step 5: Configuring ZTNA policies

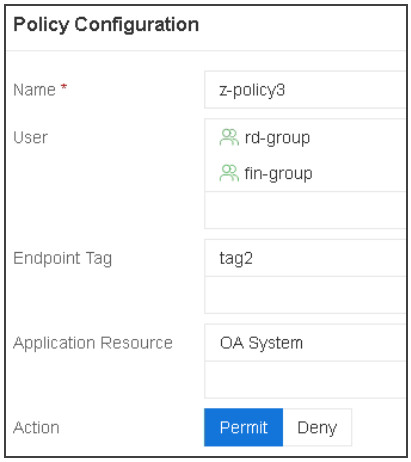
Repeat the previous operation to create "z-policy2":

- Name: z-policy2
- User: fin-group
- Application Resource: Finance System
- Endpoint tag: tag1
- Action: Permit



Repeat the previous operation to create "z-policy3":

- Name: z-policy3
- User: rd-group、fin-group
- Application Resource: OA System
- Endpoint tag: tag2
- Action: Permit



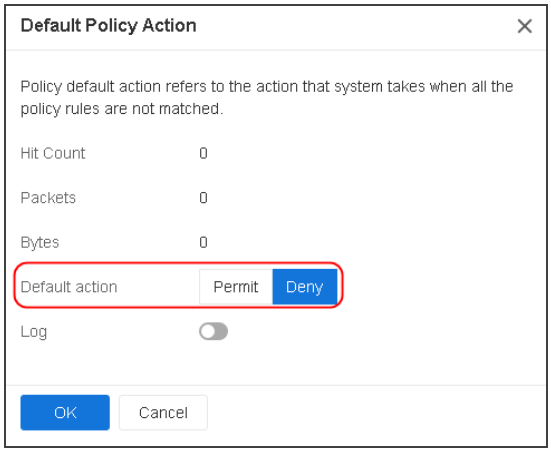
Step 6: Check that ZTNA policies are enabled

Select **ZTNA** > **Policy** and check whether these ZTNA policies are enabled. If not, select "z-policy1", "z-policy2", and "z-policy3", click ⋮ and then select **Enable**.



Step 7: Configuring the default action

Select **ZTNA** > **Policy**, click ⋮ and select **Default Policy Action**. In the **Default Policy Action** dialog box, specify the default action to **Deny**.



Step 8: Results

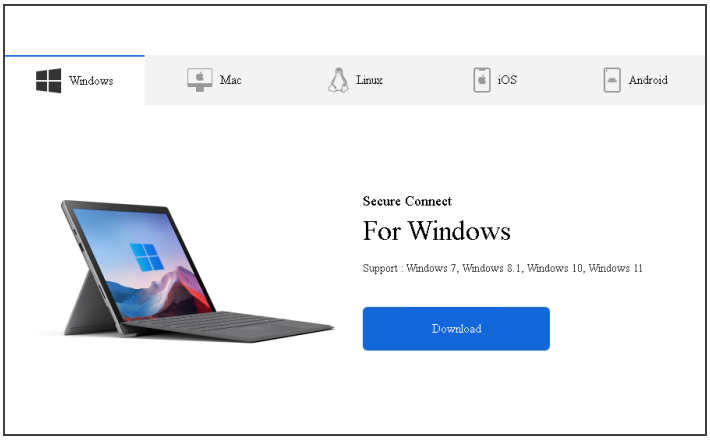
Verification Method:

1. Download Secure Connect Client. On PC1 and PC2, access https://192.168.7.1:8890 to download Secure Connect Windows client. The IP address and port number are the ones configured in the Access Interface tab.
2. Log in the client on PC1 and PC2 to check whether the access privilege for each application is correct in the ZTNA portal page.
3. Click an application resource with access privilege to check whether the user will be directed to the resource page.

Note: The operating systems of PC1 and PC2 are both Windows 10, and PC1 is running **McAfee**, while PC2 is not running **McAfee**.

Verification Steps:

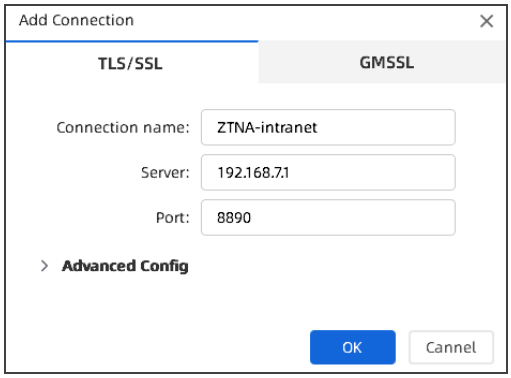
Enter the address "https://192.168.7.1:8890" in the browser on PC1 and PC2. In the pop-up page, select Windows tab and click **Download**. Then, follow the steps to install the client.



Step 8: Results

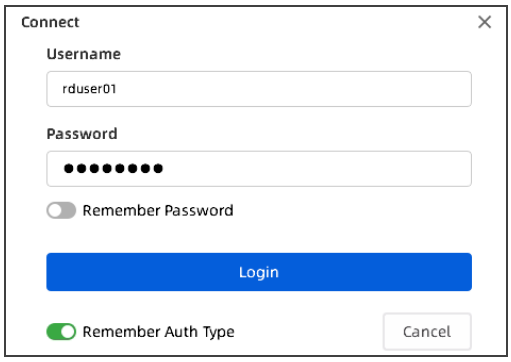
In the client on PC1 and PC2, **click Add Connection**, add a session with the connection name "ZTNA intalnet":

- Connection name: ZTNA-intranet
- Server: 192.168.7.1
- Port: 8890



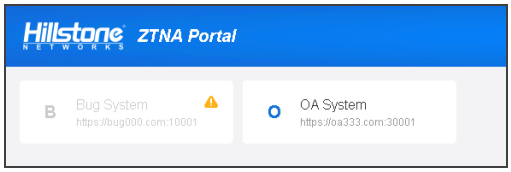
In the client, click **Connection**, use the R&D account to log in:

- Username: rduser01
- Password: password for rduser01



After successful login:

- In the ZTNA portal page displayed on PC1, Bug System and OA System are in the accessible state. Clicking the Bug System icon, the user is redirected to the Bug management page.
- In the ZTNA portal page displayed on PC2, Bug System is grayed out, OA System is displayed in blue. Clicking the Bug System icon, the user is prompted with a message indicating that the user is not granted access.



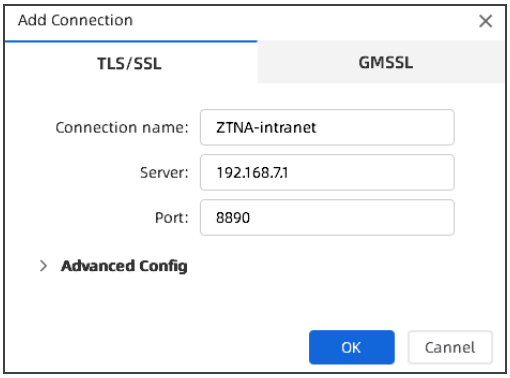
Step 8: Results

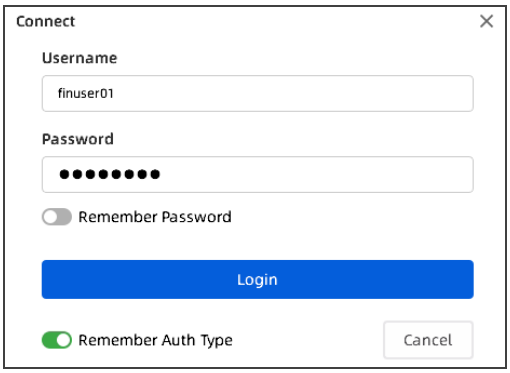
Log out rduser01 from the client on PC1 and PC2. Repeat the previous steps to log in with Finance user account finuser01.

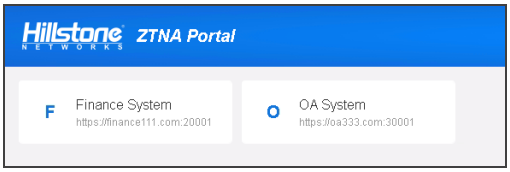
- Connection name: ZTNA-intranet
- Server: 192.168.7.1
- Port: 8890
- Username: finuser01
- Password: password for finuser01

After successful login:

- In the ZTNA portal page displayed on PC1, Finance System and OA System are in the accessible state. Clicking the Finance System icon, the user is redirected to the Finance system page.
- In the ZTNA portal page displayed on PC2, Finance System is grayed out, OA System is displayed in blue . Clicking the Finance System icon, the user is prompted with a message indicating that the user is not granted access.







Windows User Remotely Accessing Internal Server Through ZTNA

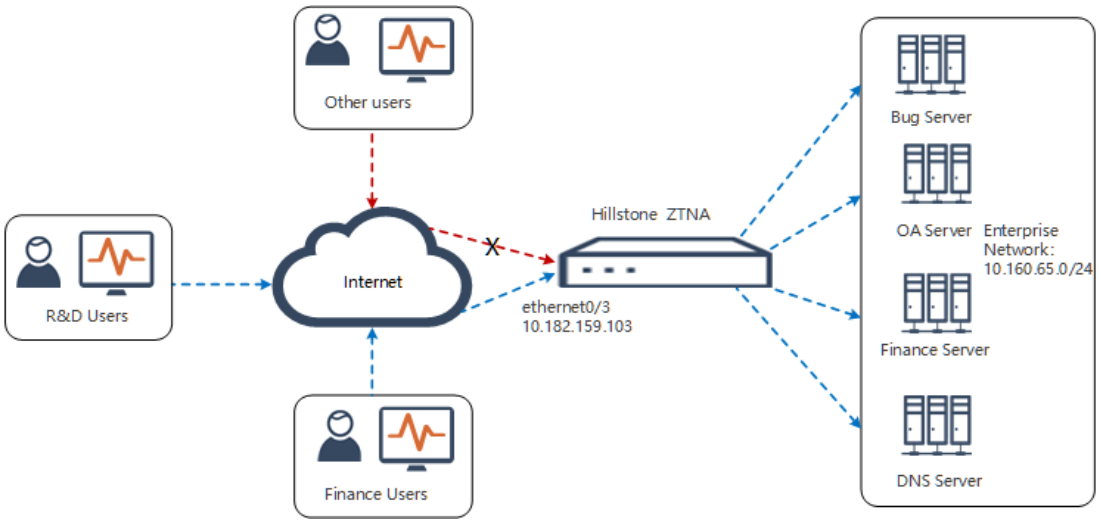
This example introduces how to configure ZTNA to enable Windows users to remotely access enterprise servers on the internal network.

Networking Scenario

An enterprise has R&D and Finance departments. The R&D department need to access enterprise application resources including the Bug management system and OA system on the enterprise network. The Finance department needs to access enterprise application resources including the Finance system and OA system on the enterprise network. Now, the enterprise hopes that employees in these two departments can access these systems when they are on a business trip. Meantime, the employes are expected to access the system using terminal devices that meet the enterprise's network security requirements. Therefore, the enterprise deploys ZTNA and formulates the following control policies based on user identity and security requirements on access terminal devices:

- R&D employees are allowed to access the Bug management system and OA system.
- Finance employees are allowed to access the Finance and OA systems.
- The access device used for remote access must meet these requirements: OS is Windows 10; McAfee is run. If McAfee is not run, the employee is allowed only to access the OA system.
- A user that does not meet any one of the previous requirements will be denied from accessing any resources.

The networking diagram is shown as follows.



Configuration Roadmap

1. Create user group "rd-group" for R&D employees and add R&D employee accounts to it.
2. Create user group "fin-group" for Finance employees and add Finance employee accounts to it
3. Configure ZTNA server parameters for establishing secure connections from the client to the device and to the application resources:
    a. ZTNA server name: name of the ZTNA service that users will access
    b. Egress interface and service port: address and port number of the ZTNA service
    c. Address pool: used for allocating private addresses to connect the internal network
    d. Tunnel interface and tunnel route: used to establish the dedicated tunnel between the user and the application resources
    e. Allow download client from browser: allow users to download ZTNA client by accessing the ZTNA service address in the browser
    f. Multiple login: allow the same user account to log in on multiple clients at the same time
    g. Two-step verification: configure the user to pass SMS code verification after logging in with user account and password
4. Create application resources "Bug System", "Finance System" and "OA System", which correspond with the Bug management system, Finance system and OA system respectively, and set their URL addresses. After a user logs in on the client, the user can

view the names and URL addresses of the application resources that are granted and currently not granted access. Application resources that you have permission to access are displayed in blue on the ZTNA Portal page, and application resources that you do not have permission to access are displayed in gray. In addition, configure application resource "Inter-DNS" for the DNS server on the enterprise network to provide domain name resolution for user traffic.

5. Configure endpoint tags. For users whose device status fully complies with the network security regulations of the company, set two endpoint tags tag1 and tag2, i.e., tag1 requires the device to be a Windows 10 operating system and to select the corresponding running process of McAfee; tag2 requires the device to be a Windows 10 operating system.

6. Configure and enable ZTNA policies. When a user's group and tag match the ZTNA policy with action Permit, the user is granted access to specific application resources. In addition, configure a ZTNA policy to allow user traffic flowing to the internal DNS server "Inter-DNS" for domain name resolution and place the policy at the beginning of all ZTNA policies.

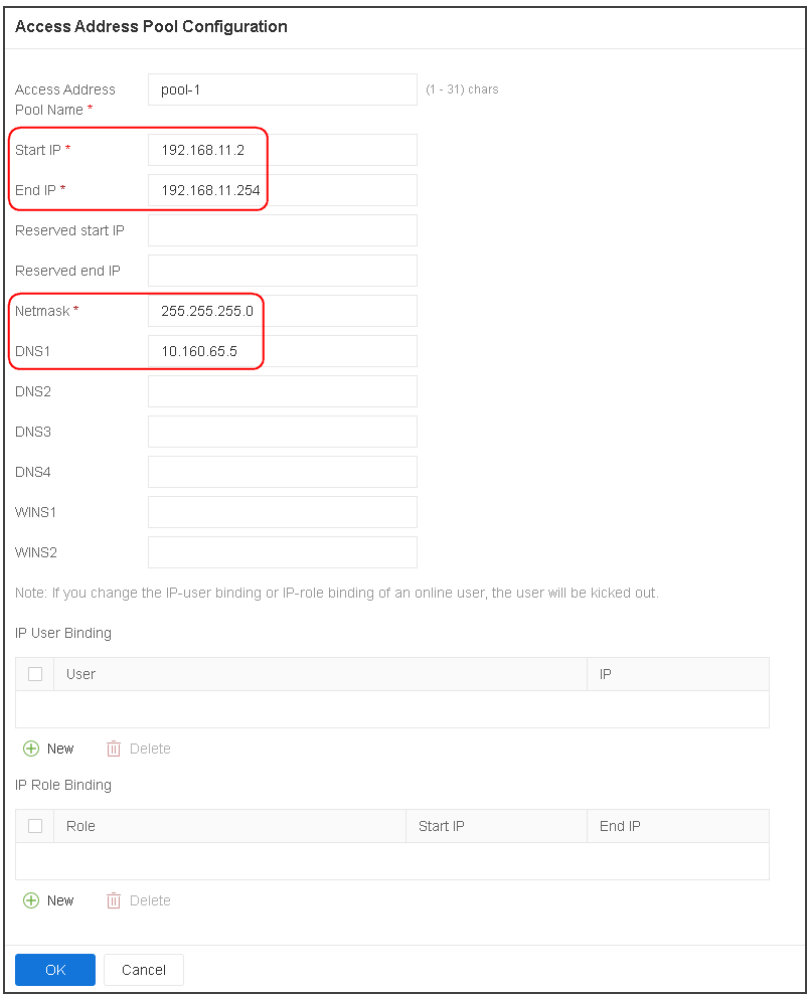
7. Configure the default action as being Deny, so that a user that do not match any ZTNA policy will be denied from accessing any application resources.

Preparations

Configure the address pool "pool-1", tunnel interface "tunnel23", and SMS gateway "hillstone" in advance. For more information, refer to *StoneOS WebUI User Guide*.

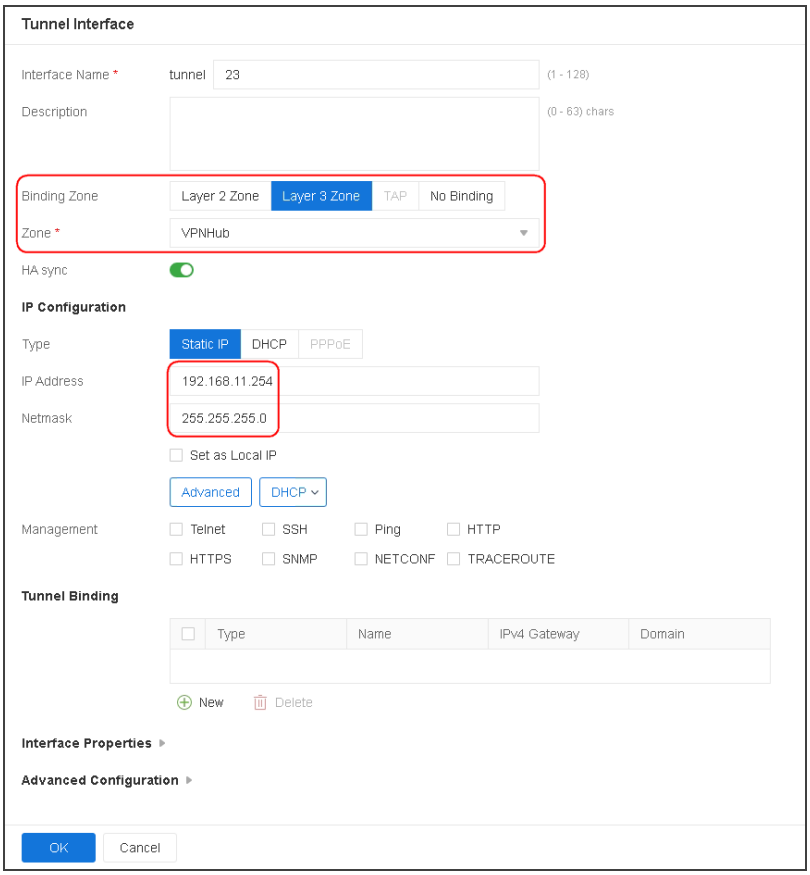
Note: The IP address of the tunnel interface and the address pool "pool-1" needs to fall into the same CIDR block, and cannot conflict with other internal endpoint that is in use.

- Select **Object** > **Access Address Pool**. On the **Access Address Pool** page, configure the address pool "pool-1".

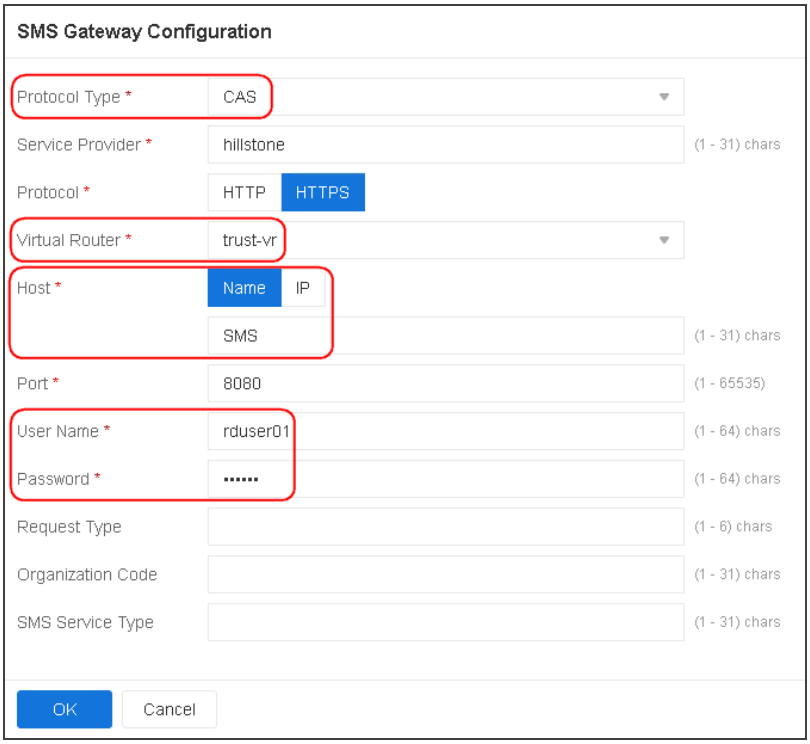


Note: When you configure ZTNA, if you need to access application resources of internal networks by using domain, you need to configure the DNS parameter.

- Select **Network** > **Interface**. On the Interface page, click **New**, select **Tunnel Interface** from the drop-down list, and then configure the tunnel interface "tunnel23".



- Select **System** > **SMS Parameters** > **SMS Gateway**. On the **SMS Gateway** page, configure the SMS gateway "hillstone".

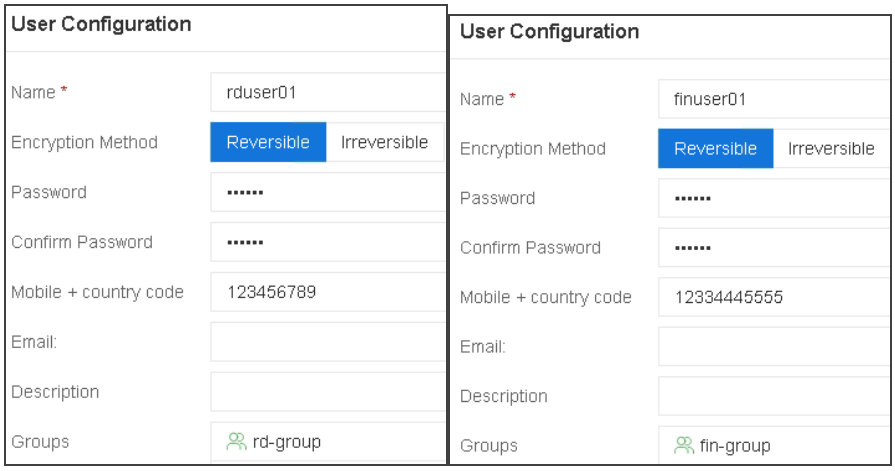


Configuration Steps

Step 1: Creating local users and user groups

Select **ZTNA** > **User** > **Local User**. Click **New** > **User** to create user "rduser01", add it to user group "rd-group" and set the password and phone number for two-step verification.

Then, follow the same step to create user "finuser01" and add it to user group "fin-group".

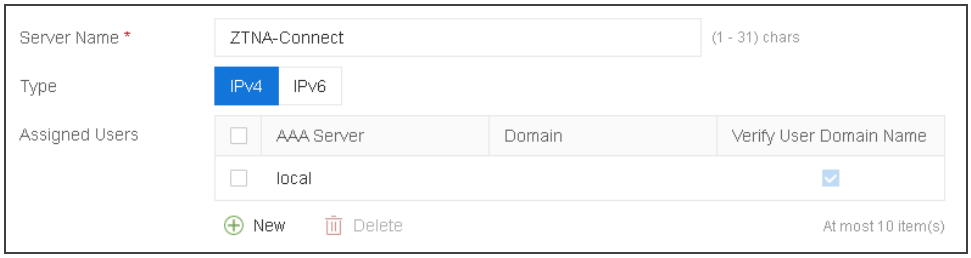


Step 2: Configuring ZTNA

Select **ZTNA** > **Gateway**, and Click **New** > **Remote Access**. In the Name/Access User tab:

- Server Name: ZTNA-Connect
- Type: IPv4
- Assigned Users: Click **New**, and select "local" for the AAA Server dropdown list

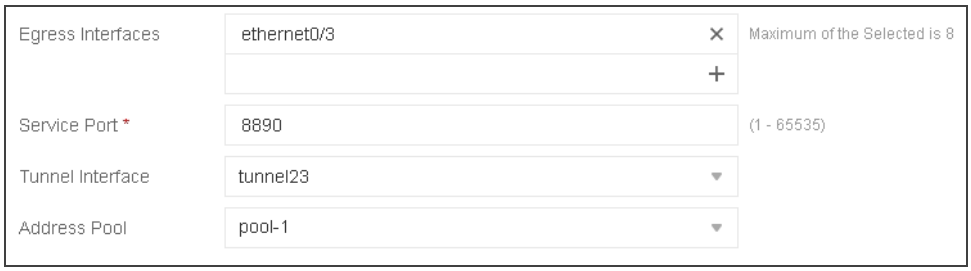
Note: In the **Assigned Users** section, you can configure at most 10 AAA servers. When multiple servers are configured, you need to configure the Domain parameter.



In the Interface tab:

- Egress Interfaces: ethernet0/3
- Service port: 8890
- Tunnel Interface: tunnel23
- Address Pool: pool-1

Note: You need to configure the tunnel interface "tunnel23" and address pool "pool-1" in advance. The IP address of the tunnel interface and the address pool need to fall into the same CIDR block.

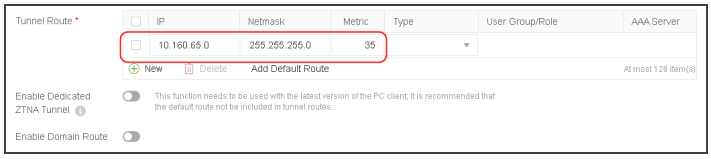


Step 2: Configuring ZTNA

In the Tunnel Route tab, click **New**:

- IP: 10.160.65.0
- Netmask: 255.255.255.0
- Metric: 35

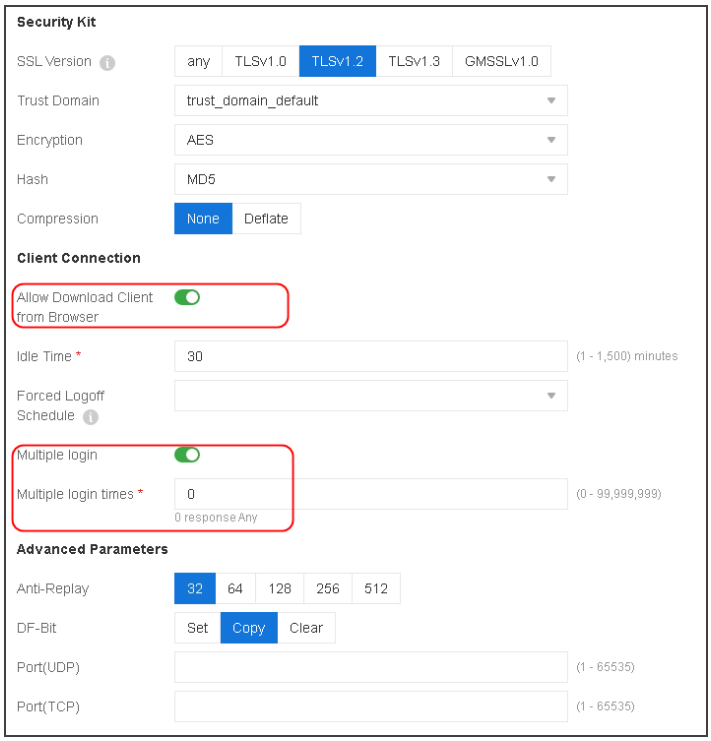
Note: When you specify the tunnel route, the IP address of the tunnel route and the IP address of the internal network server need to fall into the same CIDR block.



Step 2: Configuring ZTNA

In the Parameters tab, enable the **Allow Download Client from Browser** and **Multiple login** functions and set the **Multiple login times** option to 0.

Note: Use the default values for other parameters.

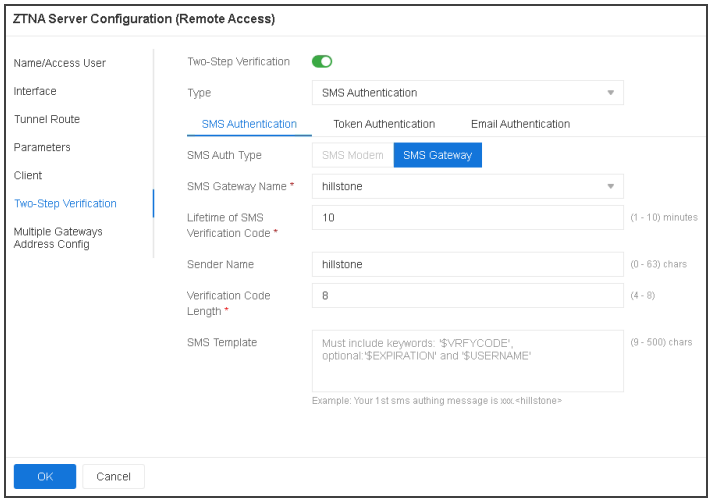


Step 2: Configuring ZTNA

In the Two-Step Verification tab:

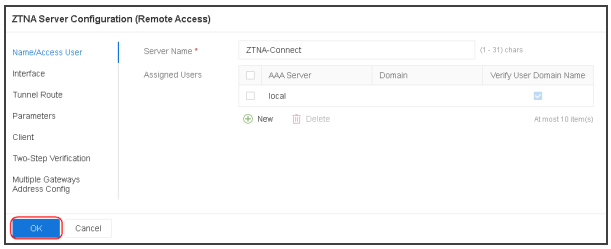
- Two-Step Verification: Click the **Enable** button
- Type: SMS Authentication
- SMS Auth Type: SMS Gateway
- SMS Gateway Name: hillstone
- Lifetime of SMS Verification Code: 10
- Sender Name: hillstone
- Verification Code Length: 8
- SMS Template (optional)

Note: You need to configure the SMS gateway "hillstone" in advance.



Step 2: Configuring ZTNA

After the ZTNA is completed, click **OK**.

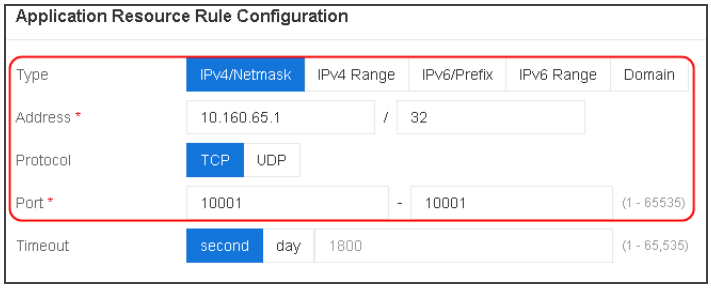


Step 3: Creating application resources

Select **ZTNA > Application Resource Book > Application Resource** and click **New**. In the Application Resource Configuration tab, click **New** to create application resource "Bug System".

- Name: Bug System (Name of the Bug management system displayed on ZTNA portal page)
- Hyperlink: https://bug000.com:10001 (URL address of the Bug management system)
- Address Type: IPv4/Netmask
- Address: 10.160.65.1/32
- Protocol: TCP
- Port: 10001 - 10001





Step 3: Creating application resources

Repeat the previous operation to create application resource "Finance System".

- Name: Finance System (Name of the finance system displayed on ZTNA portal page)
- Hyperlink: https://finance111.com:20001 (URL address of the finance system)
- Address Type: IPv4/Netmask
- Address: 10.160.65.2/32
- Protocol: TCP
- Port: 20001 - 20001

Repeat the previous operation to create application resource "OA System".

- Name: OA System (Name of the OA system displayed on ZTNA portal page)
- Hyperlink: https://oa333.com:30001 (URL address of the OA system)
- Address Type: IPv4/Netmask
- Address: 10.160.65.3/32
- Protocol: TCP
- Port: 30001 - 30001

Step 3: Creating application resources

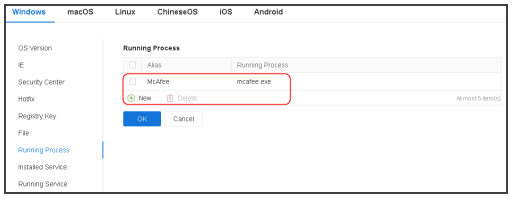
Repeat the previous operation to create application resource "Inter-DNS" for domain name resolution.

- Name: Inter-DNS
- Hyperlink: empty
- Address Type: IPv4/Netmask
- Address: 10.160.65.5/32
- Protocol: UDP
- Port: 53 - 53

Step 4: Creating endpoint tags

Select **ZTNA** > **Endpoint** > **Information**. In the **Windows** > **Running Process** tab, click New to add the following running process.

- Alias: McAfee
- Running Process: mcafee.exe (enter the name of the process corresponding to McAfee)



Step 4: Creating endpoint tags

Select **ZTNA** > **Endpoint** > **Tag** and click **New**. In the Tag Configuration tab:

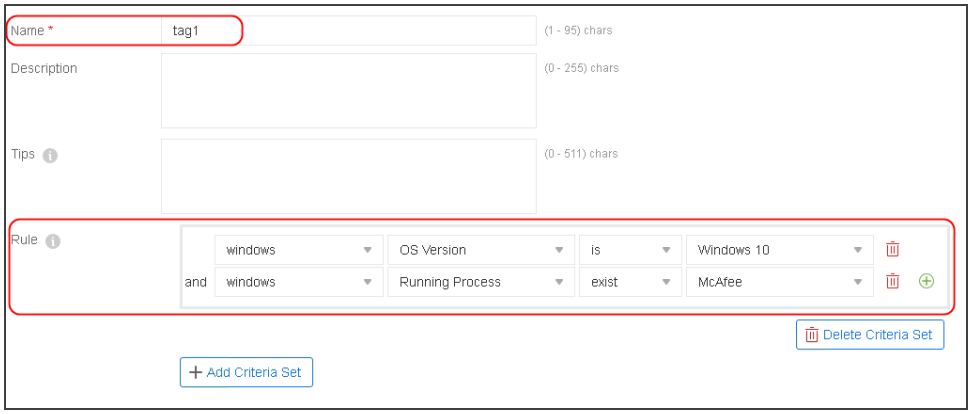
- Name: tag1

Click **Add Criteria Set**:

- Operating System: windows
- Endpoint Info Type: Select **OS Version**. Continue to select **is** and **Windows10**.

Click **+** button to create the following condition:

- Operating System: windows
- Endpoint Info Type: Select **Running Process**. Continue to select **exist** and then **McAfee**.



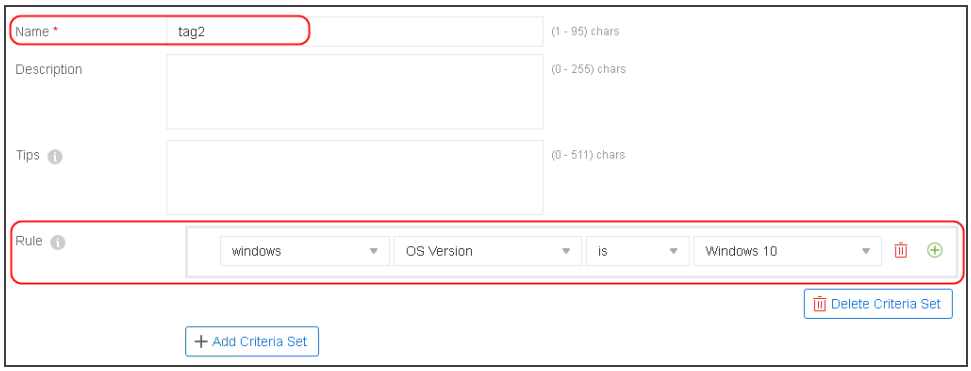
Step 4: Creating endpoint tags

Repeat the previous operation to create "tag2".

- Name: tag2

Click **Add Criteria Set**:

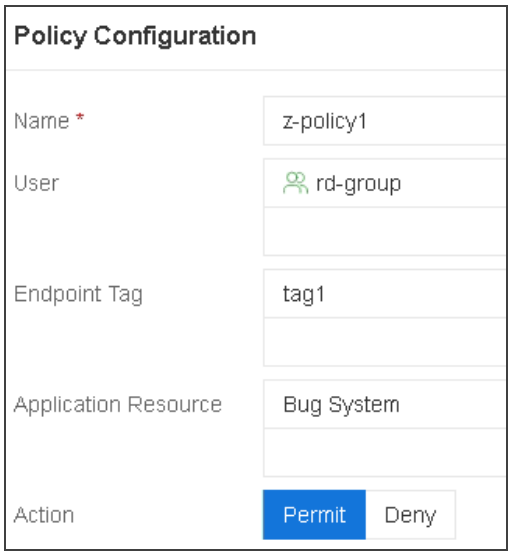
- Operating System: windows
- Endpoint Info Type: Select **OS Version**. Continue to select **is** and **Windows10**.



Step 5: Configuring ZTNA policies

Select **ZTNA** > **Policy** and click **New**. In the Policy Configuration tab:

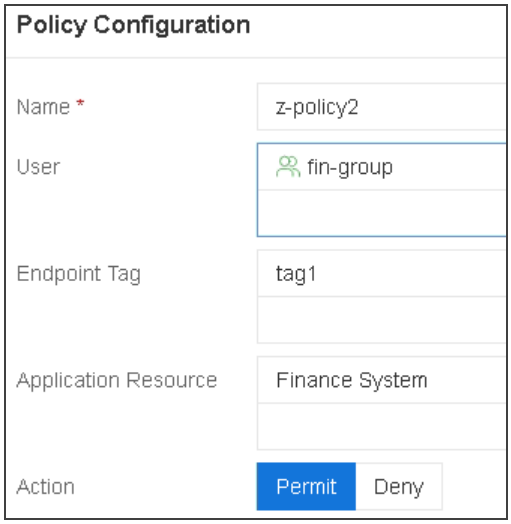
- Name: z-policy1
- User: rd-group
- Application Resource: Bug System
- Endpoint tag: tag1
- Action: Permit



Step 5: Configuring ZTNA policies

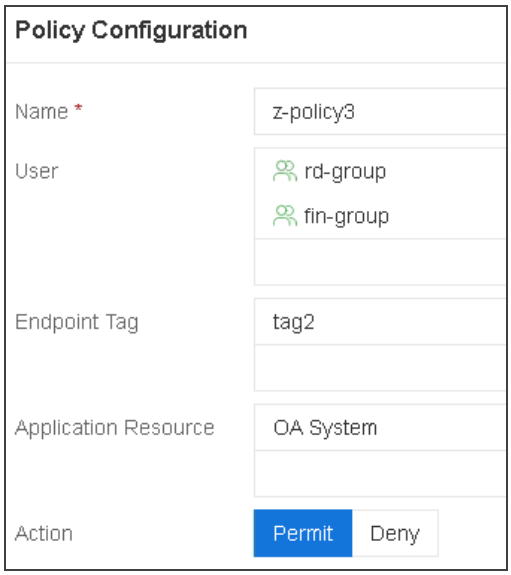
Repeat the previous operation to create "z-policy2":

- Name: z-policy2
- User: fin-group
- Application Resource: Finance System
- Endpoint tag: tag1
- Action: Permit



Repeat the previous operation to create "z-policy3":

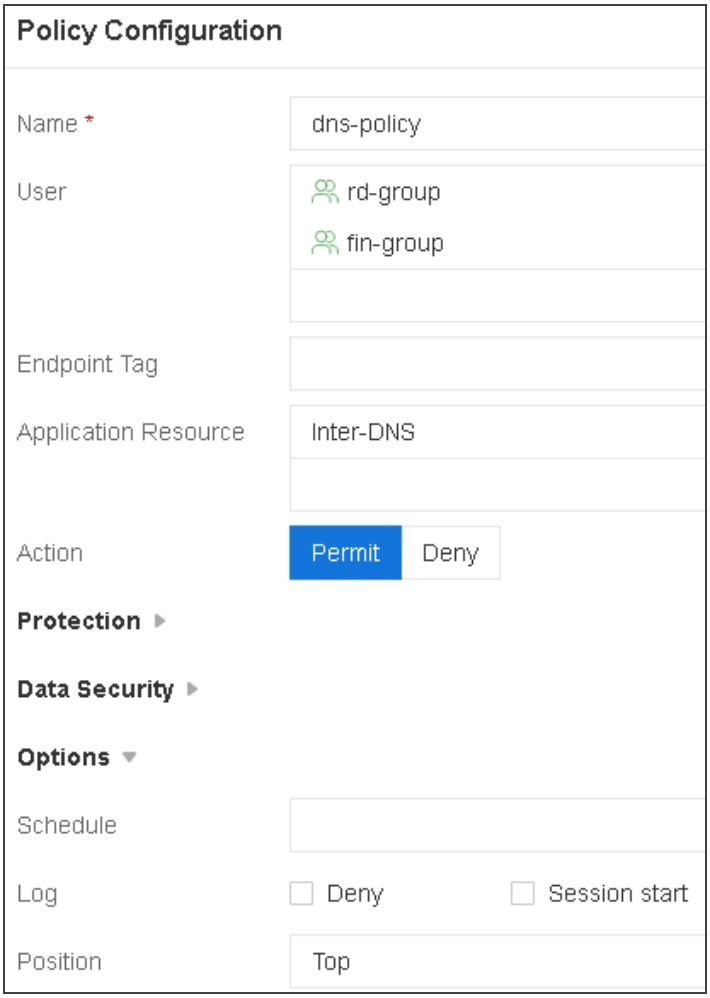
- Name: z-policy3
- User: rd-group, fin-group
- Application Resource: OA System
- Endpoint tag: tag1
- Action: Permit



Step 5: Configuring ZTNA policies

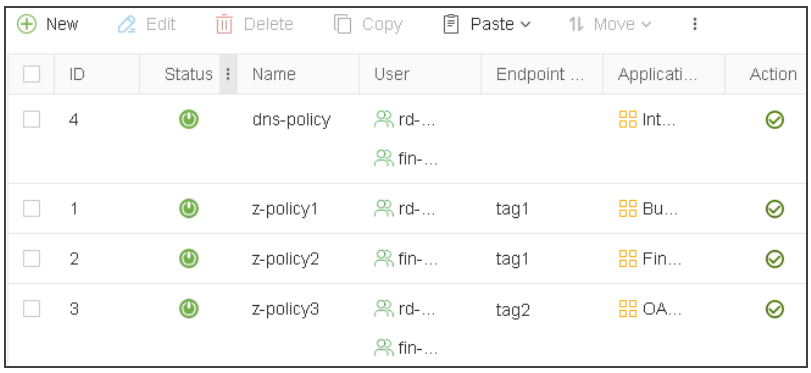
Repeat the previous operation to create "dns-policy" for user traffic domain name resolution on the internal DNS server:

- Name: dns-policy
- User: rd-group, fin-group
- Application Resource: Inter-DNS
- Endpoint tag: empty
- Action: Permit



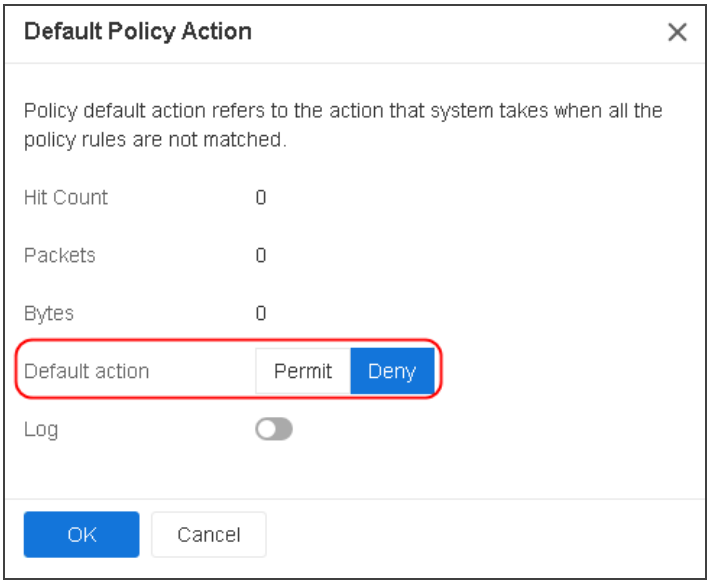
Step 6: Check that ZTNA policies are enabled

Select **ZTNA** > **Policy** and check whether these ZTNA policies are enabled. If not, select "z-policy1", "z-policy2", "z-policy3" and "dns-policy", click ⋮ and then select **Enable**.



Step 7: Configuring the default action

Select **ZTNA** > **Policy**, click ⋮ and select **Default Policy Action**. In the **Default Policy Action** dialog box, specify the default action to **Deny**.



Step 8: Results

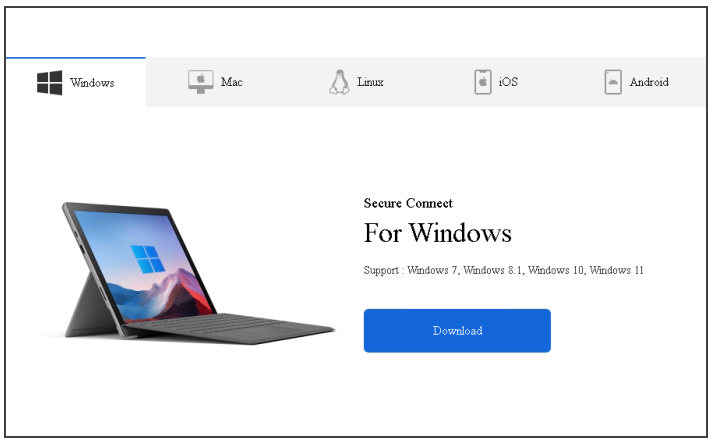
Verification Method:

1. Download Secure Connect Client. On PC1 and PC2, access https://10.182.159.103:8890 to download Secure Connect Windows client. The IP address and port number are the ones configured in the Interface tab.
2. Log in the client on PC1 and PC2 to check whether the access privilege for each application is correct in the ZTNA portal page.
3. Click an application resource with access privilege to check whether the user will be directed to the resource page.

Note: The operating systems of PC1 and PC2 are both Windows 10, and PC1 is running **McAfee**, while PC2 is not running **McAfee**.

Verification Steps:

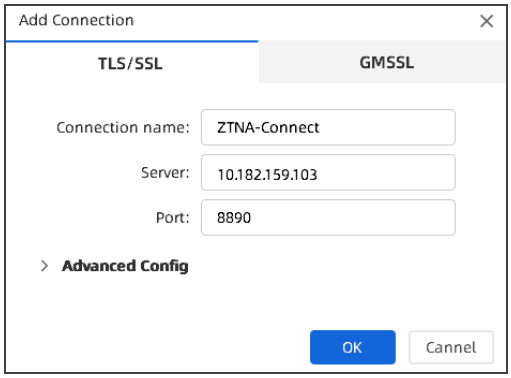
Enter the address "https://10.182.159.103:8890" in the browser on PC1 and PC2. In the pop-up page, select Windows tab and click **Download**. Then, follow the steps to install the client.



Step 8: Results

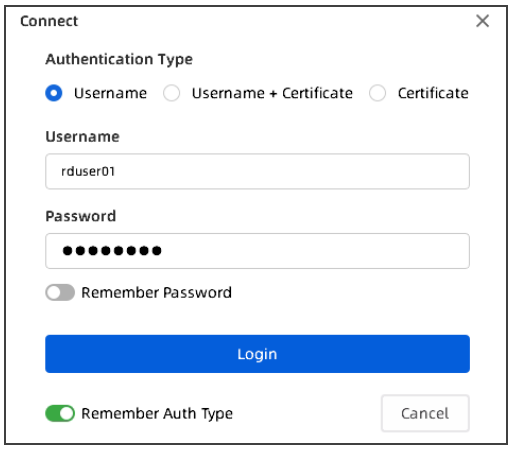
In the client on PC1 and PC2, **click Add Connection**, add a session with the connection name "ZTNA-Connect":

- Connection name: ZTNA-Connect
- Server: 10.182.159.103
- Port: 8890



In the client, click **Connection**, use the R&D account to log in:

- Username: rduser01
- Password: password for rduser01



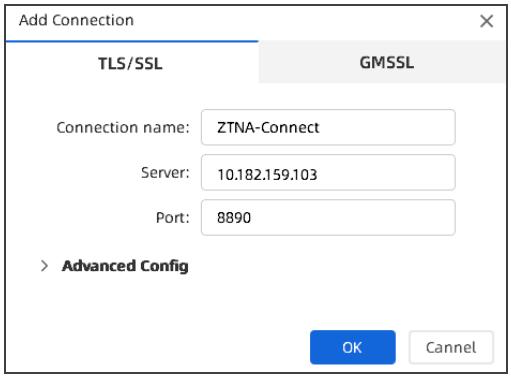
After passing the SMS code verification:

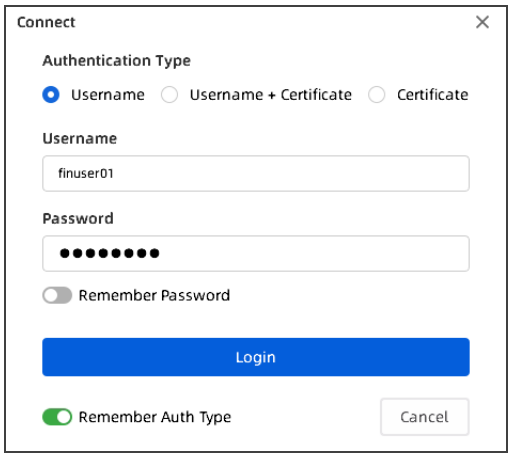
- In the ZTNA portal page displayed on PC1, Bug System and OA System are in the accessible state. Clicking the Bug System icon, the user is redirected to the Bug management page.
- In the ZTNA portal page displayed on PC2, Bug System is grayed out, OA System is displayed in blue. Clicking the Bug System icon, the user is prompted with a message indicating that the user is not granted access.

Step 8: Results

Log out rduser01 from the client on PC1 and PC2. Repeat the previous steps to log in with Finance user account finuser01.

- Server: 10.182.159.103
- Port: 8890
- Username: finuser01
- Password: password for finuser01





After passing SMS code verification:

- In the ZTNA portal page displayed on PC1, Finance System and OA System are in the accessible state. Clicking the Finance System icon, the user is redirected to the Finance system page.
- In the ZTNA portal page displayed on PC2, Finance System is grayed out, OA System is displayed in blue. Clicking the Finance System icon, the user is prompted with a message indicating that the user is not granted access.

Android User Remotely Accessing Internal Server Through ZTNA

This example introduces how to configure ZTNA to enable Android users to remotely access bank service system on the internal network.

Networking Scenario

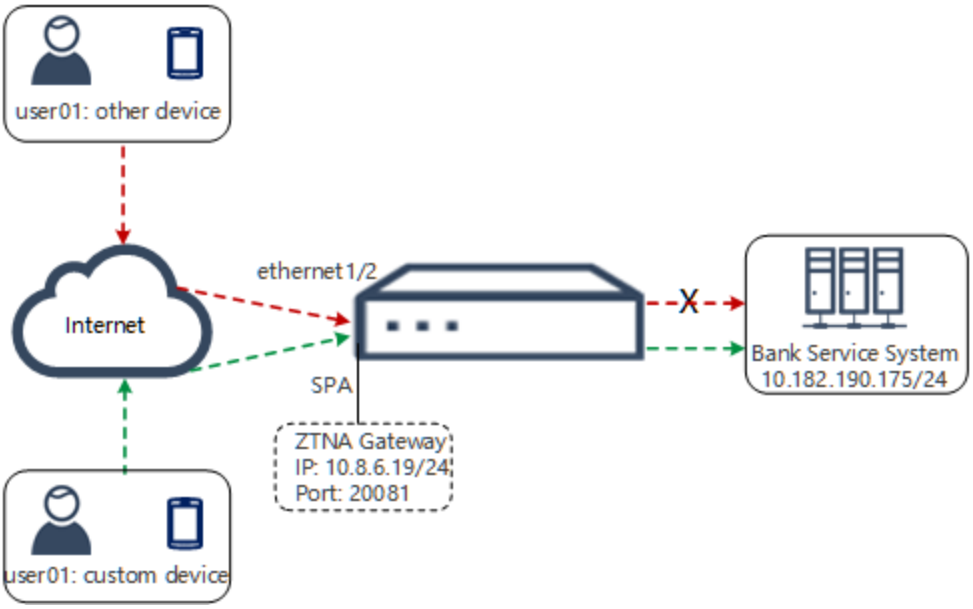
A bank needs the staff to handle services for customers on the go by accessing the bank service system via hand-held terminals. To ensure access security, the bank wants to deploy ZTNA and requires that the staff use the Android device with customized device model number designated by the bank, to access ZTNA and the system version of the device be updated to Android 13.

Specific privilege setting and requirements are as follows:

- The bank staff can log in the ZTNA gateway with the specified account and password when using the designated Android device, and can switch to the bank service system via the ZTNA Portal page after login.
- The bank staff can log in the ZTNA gateway with the specified account and password when using other Android devices or using the designated device whose system version is not Android 13, but cannot access the bank service system. When clicking the bank service system displayed on the ZTNA Portal, the staff will see a tip indicating "Please use designated device and update system version to Android 13!".
- Except the specified account, other account cannot log in the ZTNA gateway.

In addition, the bank hopes that the ZTNA service port be closed by default so as to make it and the bank service system invisible on the network and not be scanned. For users needing to access the ZTNA service, the service port will be particularly open to the user only after the user has passed the verification of the ZTNA service by sending single packet authorization (SPA) packets to knock the ZTNA service port.

The networking diagram is shown as follows.



Configuration Roadmap

1. Create a local user "user01" for the bank work to log in the ZTNA gateway.
2. Configure ZTNA server parameters for establishing secure connects from the client to the device and to the application resources.
    a. ZTNA service: name of the ZTNA service that users will access
    b. Egress interface and service port: address and port number of the ZTNA service
    c. Address pool: used for allocating private addresses to connecting the internal network
    d. Tunnel interface and tunnel route: used to establish the dedicated tunnel between the user and the application resources
3. Configure Single Packet Authorization (SPA) to hide the ZTNA service IP and port number. The ZTNA service port will be open to the user who accesses through the Hillstone Secure Connect client and passes SPA.
4. Configure the bank service system as application resource "Bank System" and specify a hyperlink for it so that the user can switch to the bank service system via the ZTNA Portal after login.
5. Configure the designated Android device's model number A-bank-2256 as a custom endpoint item "m-device".

6. Create endpoint tag "m-device-tag" for the designated Android device whose device model number is "m-device" and system version is Android 13 and configure the tip "Please use designated device and update system version to Android 13!", which will be displayed when the user is not granted access to the bank service system because the endpoint tag is not matched.
7. Configure and enable ZTNA policy "m-policy", allowing the bank staff to access the bank service system via the designated Android device.
8. Configure the default action as being Deny, so that a user that do not match "m-policy" will be denied from accessing the bank service system.

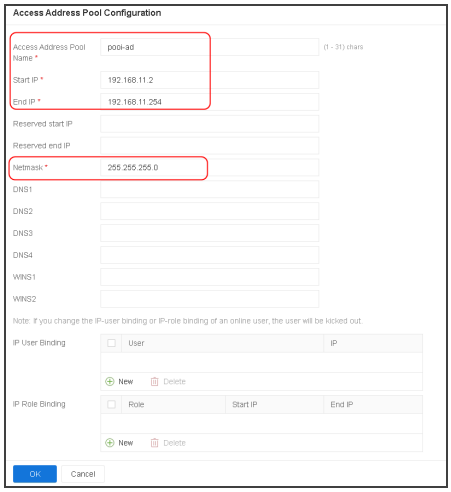
Preparations

Configure the address pool "pool-ad", and tunnel interface "tunnel2". For more information, refer to *StoneOS WebUI User Guide*.

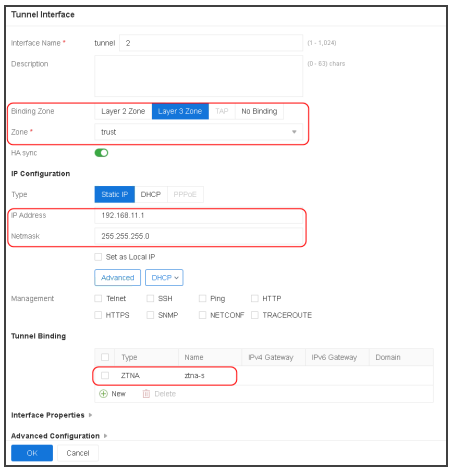
Note: The IP address of the tunnel interface and the address pool "pool-ad" needs to fall into the same CIDR block, and cannot conflict with other internal endpoint that is in use.

- Select **Object** > **Access Address Pool**. On the **Access Address Pool** page, configure the address pool "pool-ad".

  Note: When you configure ZTNA, if you need to access application resources of internal networks by using domain, you need to configure the DNS parameter.



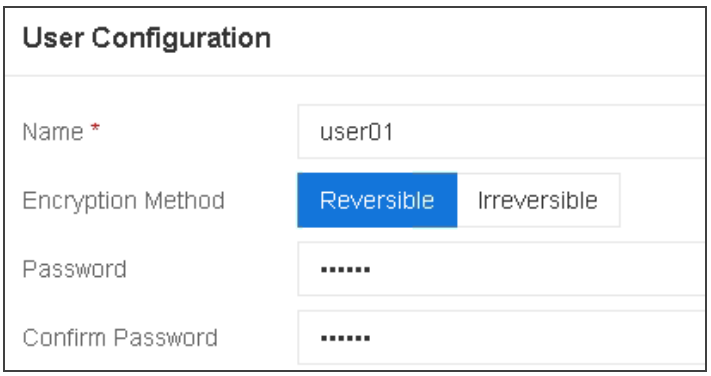
- Select **Network** > **Interface**. On the Interface page, click **New**, select **Tunnel Interface** from the drop-down list, and then configure the tunnel interface "tunnel2".



Configuration Steps

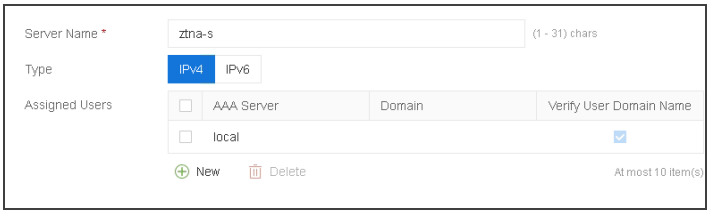
Step 1: Creating local user.

Select **ZTNA** > **User** > **Local User**. Click **New** > **User** to create user "user01" and set the password



Step 2: Configuring ZTNA

Select **ZTNA** > **Gateway**, and Click **New** > **Remote Access**. In the Name/Access User tab:



- Server Name: ztna-s
- Type: IPv4
- Assigned Users: Click **New**, and select **local** for the **AAA Server** dropdown list

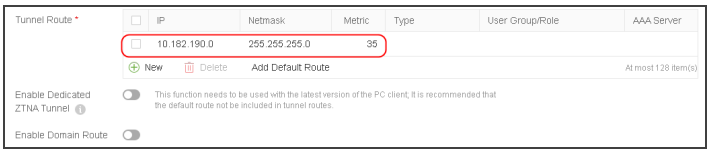
In the Interface tab:



- Egress Interfaces: ethernet1/2
- Service port: 20081
- Tunnel Interface: tunnel2
- Address Pool: pool-ad

Note: You need to configure the tunnel interface "tunnel2" and address pool "pool-ad" in advance. The IP address of the tunnel interface and the address pool need to fall into the same CIDR block.

In the Tunnel Route tab, click **New**:

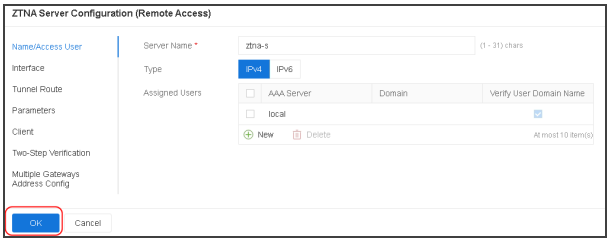


- IP: 10.182.190.0
- Netmask: 255.255.255.0
- Metric: 35

Tunnel route must be on the same network segment with the internal server.

Step 2: Configuring ZTNA

After the ZTNA is completed, click **OK**.



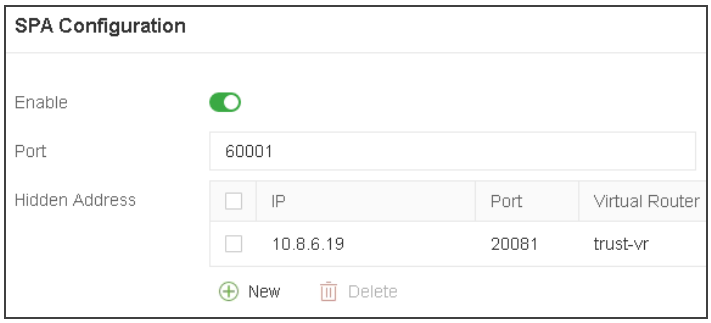
Step 3: Configure Single Packet Authorization (SPA).

Select **ZTNA > SPA > SPA Configuration** to enable SPA and set the knock port:

- Enable: click to enable SPA
- Port: 60001

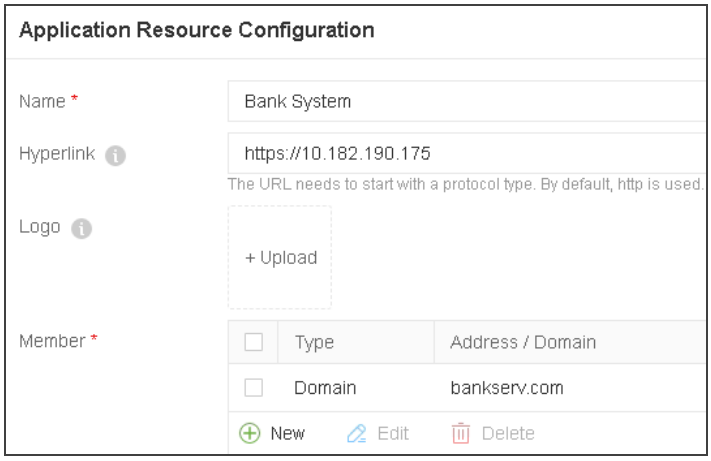
Click new to add ZTNA service address as hidden address:

- IP: 10.8.6.19
- Port: 20081
- Virtual Router: trust-vr



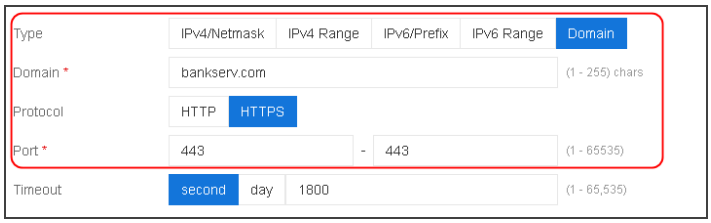
Step 4: Creating application resource

Select **ZTNA > Application Resource Book > Application Resource** and click **New**. In the Application Resource Configuration tab, click **New** to create application resource "Bank System".



- Name: Bank System (Name of the bank service system displayed on ZTNA portal page)
- Hyperlink: https://10.182.190.175 (URL address of the bank service system)

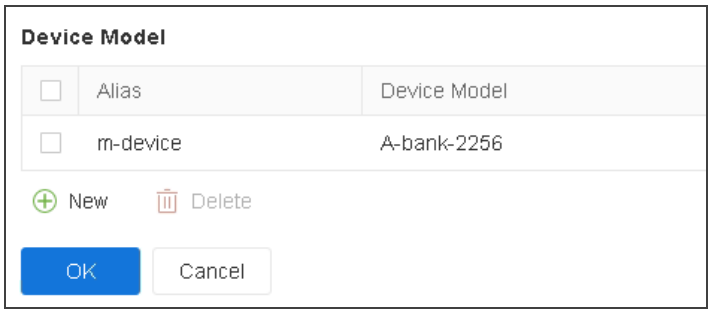
Click **New** to configure application resource rule:



- Type: Domain
- Domain: bankserv.com
- Protocol: HTTPS
- Port: 443 - 443

Step 5: Adding the designated Android device as endpoint information to be collected

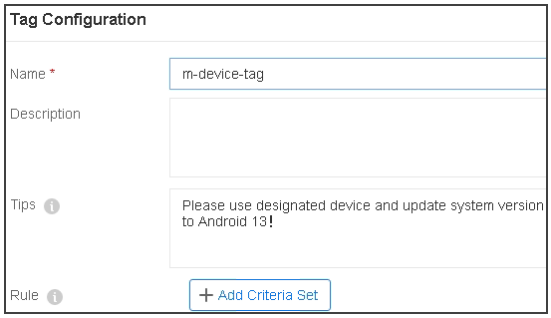
Select **ZTNA > Endpoint > Information** and click **Android**. Click **Device Model** and add the model number of the designated device:



- Alias: m-device
- Device Model: A-bank-2256

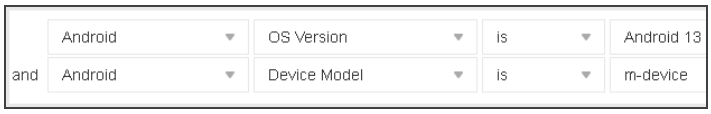
Step 6: Creating endpoint tag

Select **ZTNA > Endpoint > Tag**and click **New** to create endpoint tag in the Tag Configuration tab:



- Name: m-device-tag
- Tips: Please use designated device and update system version to Android 13!

Click **Add Criteria Set** and add the device model and system version as criteria:



- Operating System: Android
- Endpoint Info Type: Select **OS Version**. Continue to select **is** and then **Android 13**.

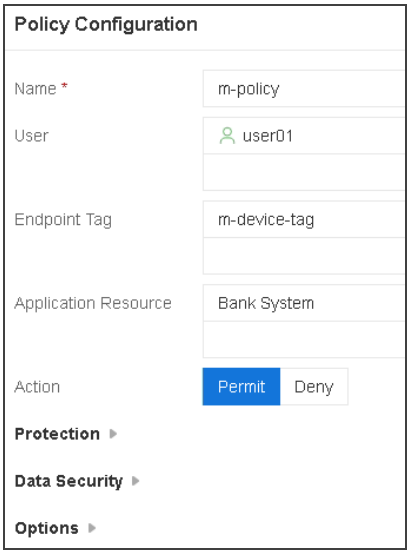
Click the + button to create the following condition:

- Operating System: Android
- Endpoint Info Type: Select **Device Model**. Continue to select **is** and then **m-device**.

Step 7: Configuring ZTNA policy

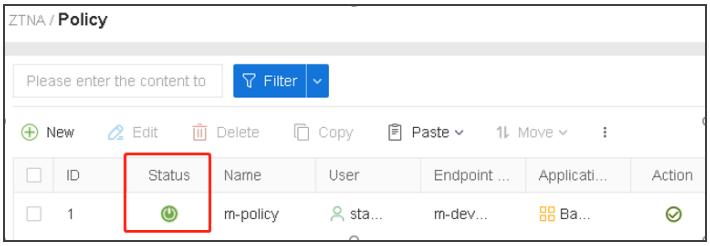
Select ZTNA > Policy and click **New**. In the Policy Configuration tab:

- Name: m-policy
- User: user01
- Application Resource: Bank System
- Endpoint Tag: m-device-tag
- Action: Permit



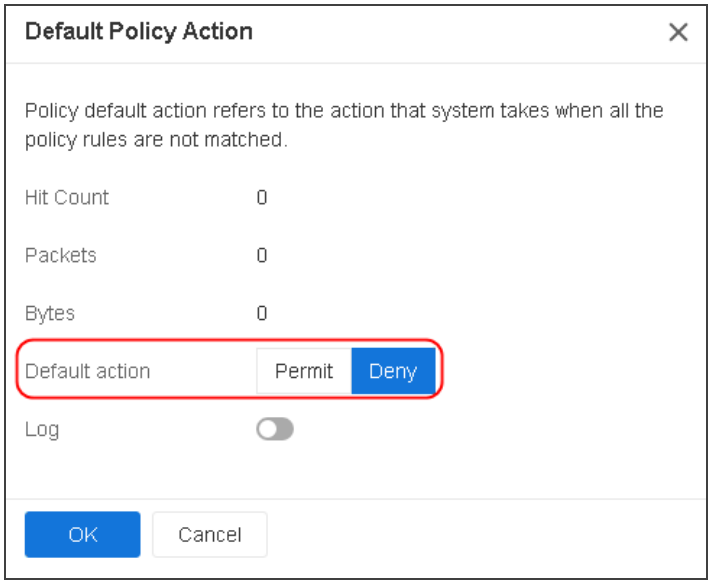
Step 8: Checking that ZTNA policy is enabled

Select **ZTNA** > **Policy** and check whether the ZTNA policy is enabled. If not, select "m-policy", click ⋮ and then select **Enable**.



Step 9: Configuring the default action

Select **ZTNA** > **Policy**, click ⋮ and select **Default Policy Action**. In the **Default Policy Action** dialog box, specify the default action to **Deny**.



Step 10: Results

Access the client download page: http://www.hillstonenet.com.cn/product/technology/VPN.html.

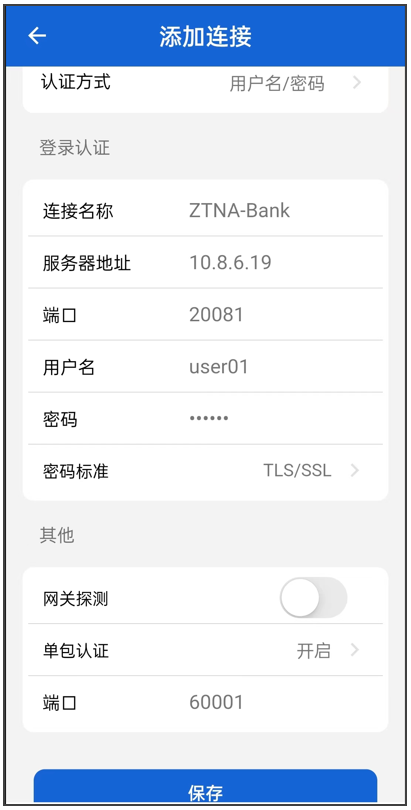
Locate the QR code for Android client and use the designated Android device to scan the code.

Download the installation file and install the Hillstone Secure Connect client.

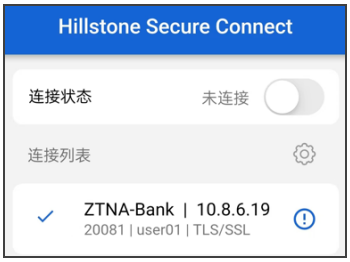
Step 10: Results

Open the client and click **Add Connection** on the upper right. In the displayed dialog box, fill the following information and then click **Add Connection** at the lower part:

- Connection Name: ZTNA-Bank
- Server: 10.8.6.19
- Port: 20081
- User: user01
- Password: password of the user "user01"
- SPA: on
- Port: 60001



Return to the Hillstone Secure Connect client and click **Connect** on the ZTNA-Bank session.



After login, the ZTNA Portal Page is displayed. Click Bank System, the user is switched to the bank service system.

High Availability

High Availability is a redundancy backup methhod. It uses two identical devices to ensure that when one fails to work, the other will immediately takes over to provide network consistency.

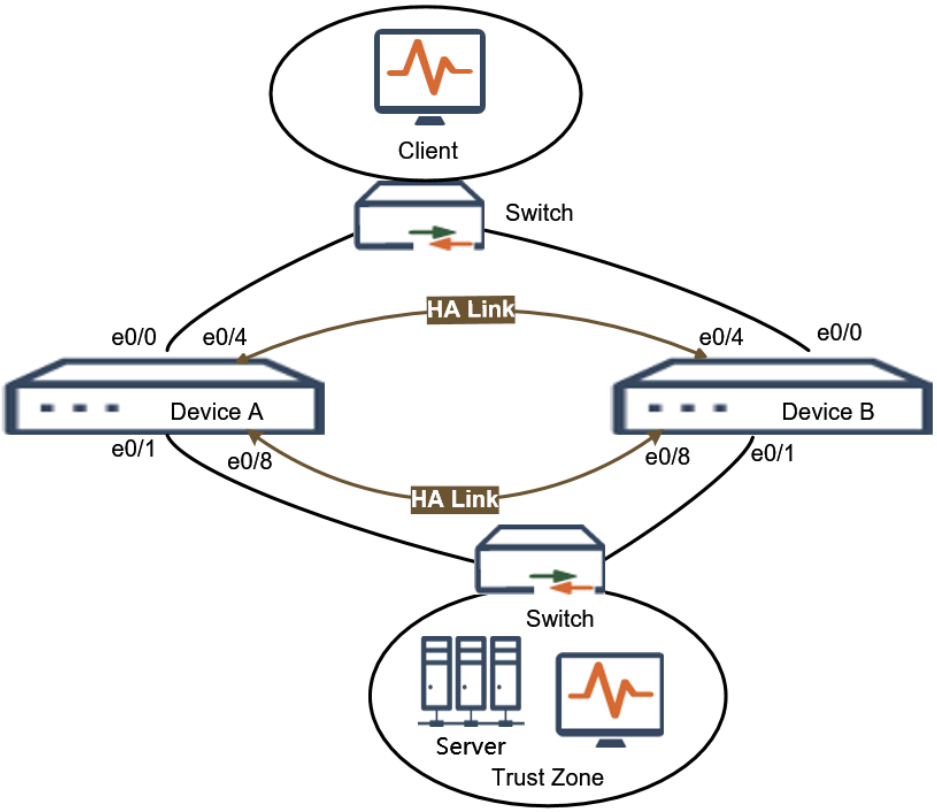
This chapter includes the following recipe:

- " Ensuring Uninterrupted Connection Using HA" on Page 347
- "Making Two Firewalls Working in Hot Standby Mode by Deploying them in HA Peer to Ensure the Continuity of Service " on Page 355
- "Using Two Devices as Gateways to Forward Business Traffic and Back Up Each Other Based on HSVRP, which Ensures Uniterrupted Business Traffic" on Page 360

Ensuring Uninterrupted Connection Using HA

This example introduces how to configure two devices working under Active-Passive mode to provide high availability for the protected network.

The topology gives a typical user scenario for HA. In the designed scenario, one (Device A)of the HA devices will be working under the active mode, while the other (Device B) is under passive mode. The active device will synchronize its data and status to the passive device. When the active one fails, the passive device will immediately switch to be active, without interrupting the network.



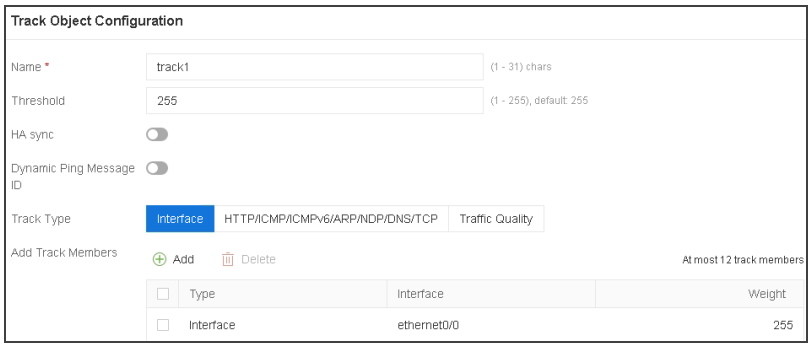
Configuration Steps

Step 1: Configuring track object. Each device monitors eth0 respectively.

Device A

Select **Object > Track Object**, and click **New**.

- Name: track1
- Threshold: 255
- HA sync: Disable
- Track Type: Select **Interface**, and click **Add**. In the prompt, select ethernet0/0, and weight as 255.



Device B

Select **Object > Track Object**, and click **New**.

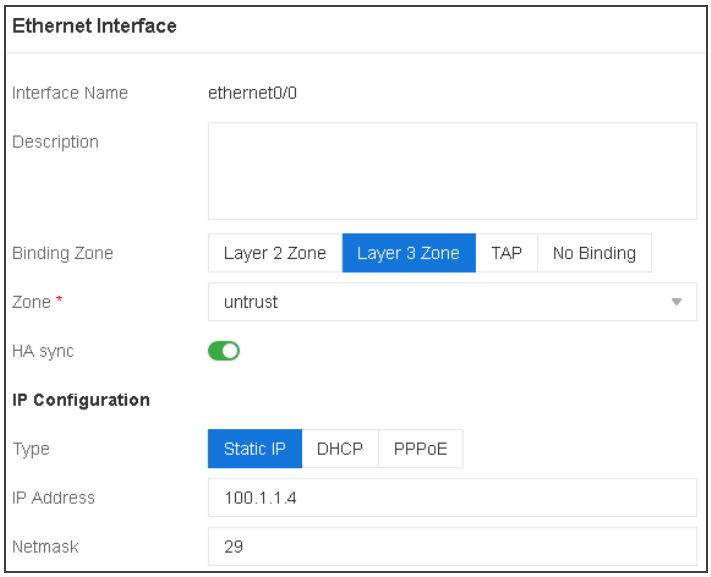
- Name: track1
- Threshold: 255
- HA sync: Disable
- Track Type: Select **Interface**, and click **Add**. In the prompt, select ethernet0/0, and weight as 255.



Step 2: Configuring Device A's interface and policy

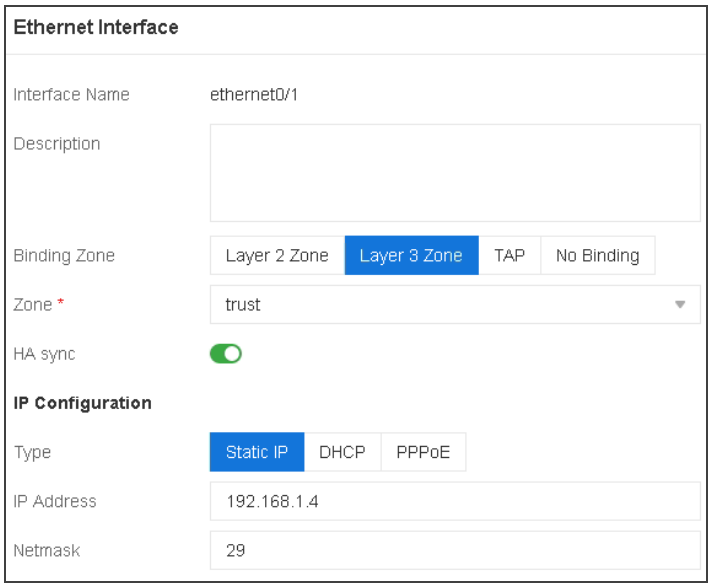
Select **Network > Interface**, and double click ethernet0/0.

- Binding Zone: Layer 3 Zone
- Zone: untrust
- HA sync: Enable
- Type: Static IP
- IP Address: 100.1.1.4
- Netmask: 29



Select **Network > Interface**, and double click ethernet0/1.

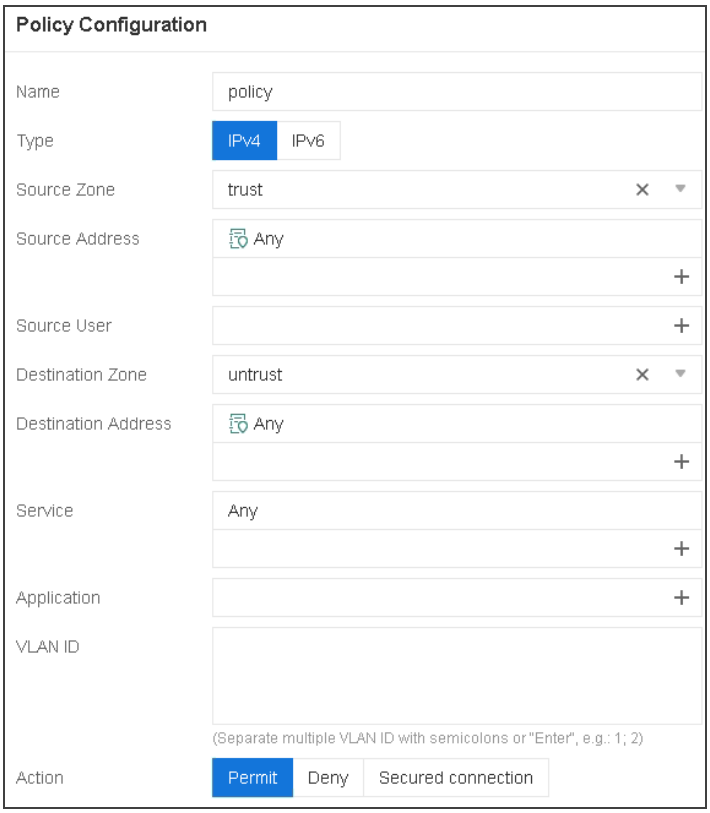
- Binding Zone: Layer 3 Zone
- Zone: trust
- HA sync: Enable
- Type: Static IP
- IP Address: 192.168.1.4
- Netmask: 29



Step 2: Configuring Device A's interface and policy

Select **Policy > Security Policy > Policy**, and click **New**.

- Name: policy
- Source Zone: trust
- Source Address: Any
- Destination Zone: untrust
- Destination Address: Any
- Service: Any
- Action: Permit

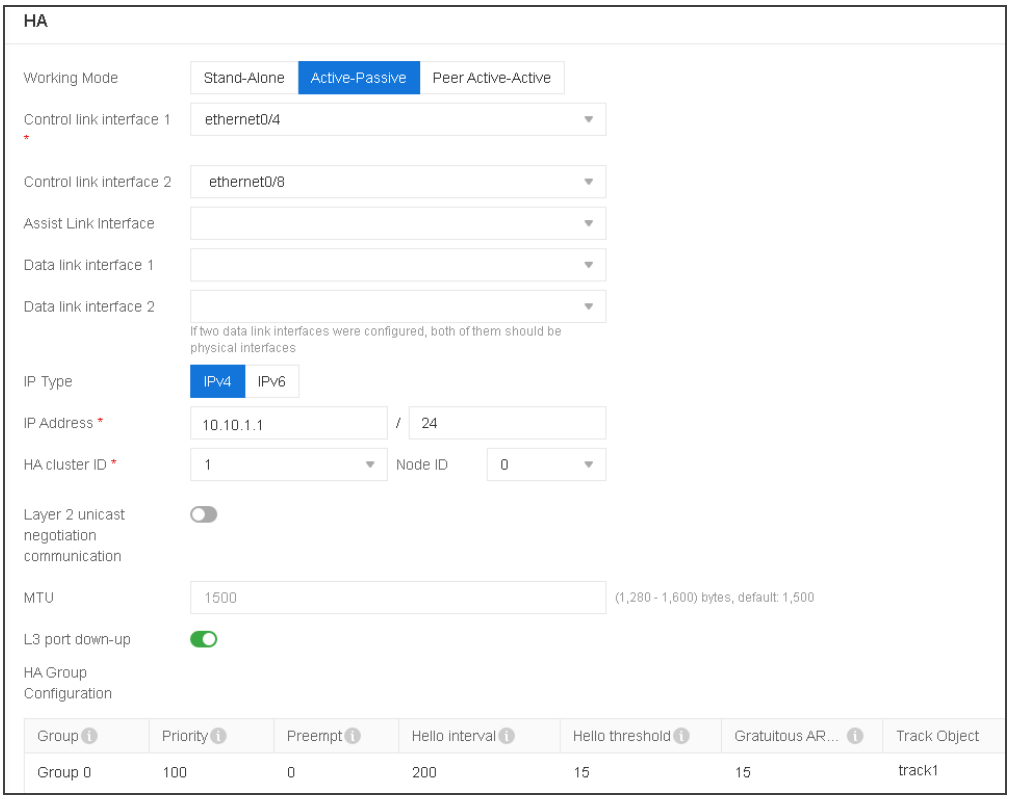


Step 3: Configuring HA function

Device A

Select **System > HA**.

- Working Mode: Active-Passive
- Control link interface 1: ethernet0/4
- Control link interface 2: ethernet0/8
- IP Address: 10.10.1.1/24
- HA cluster ID: 1
- Node ID: 0
- HA Group Configuration: Enter 10 for "Priority" and select track1 for "Track Object".

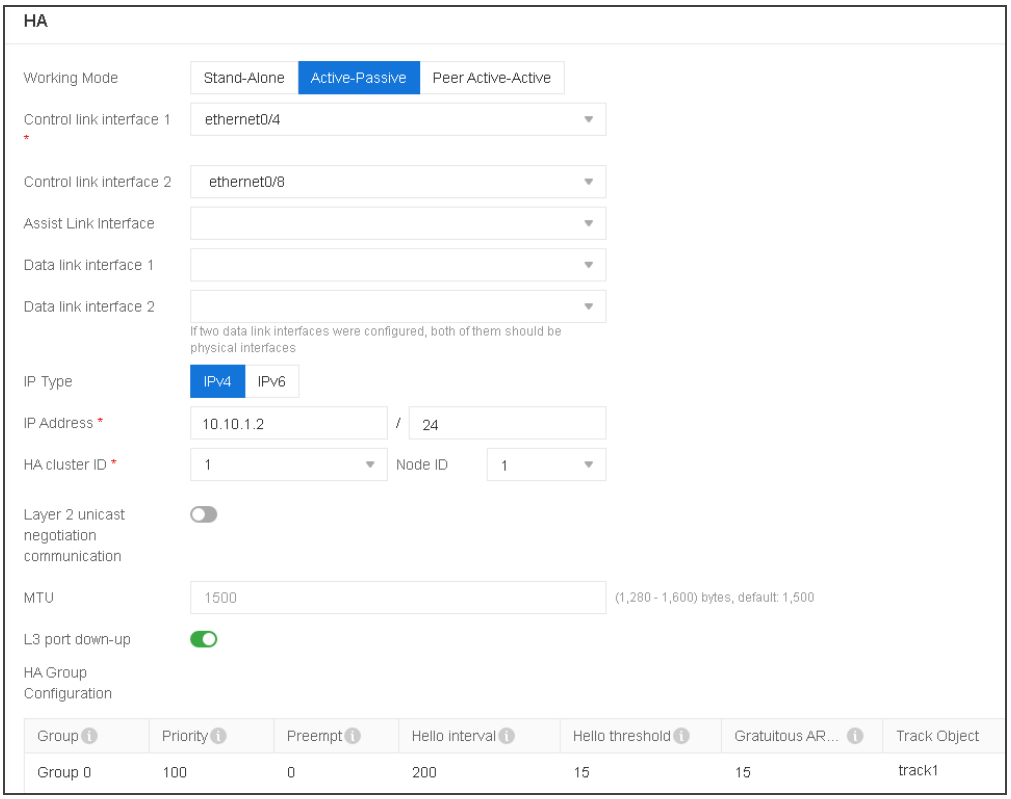


Step 3: Configuring HA function

Device B

Select **System > HA**.

- Working Mode: Active-Passive
- Control link interface 1: ethernet0/4
- Control link interface 2: ethernet0/8
- IP Address: 10.10.1.2/24
- HA cluster ID: 1
- Node ID: 1
- HA Group Configuration: Enter 100 for "Priority" and select track1 for "Track Object".

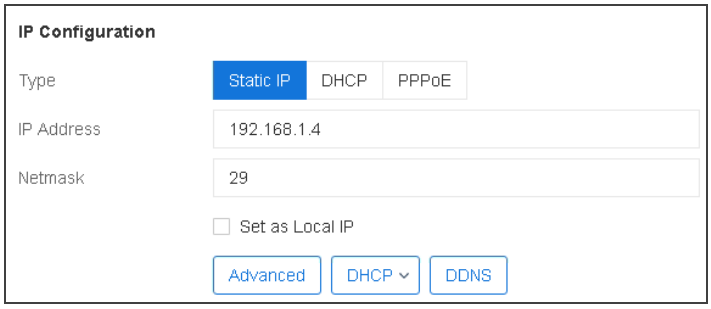


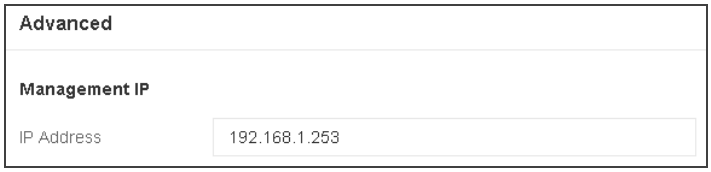
Step 4: Configuring management IP of active and passive devices after synchronization

Device A

Select **Network > Interface**, and double click ethernet0/1. Under IP Configuration, click **Advanced**.

- Management IP
  - IP Address: 192.168.1.253

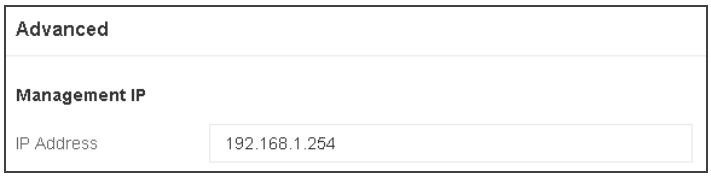




Device B

Select **Network > Interface**, and double click ethernet0/1. Under IP Configuration, click **Advanced**.

- Management IP
  - IP Address: 192.168.1.254



Step 5: Results

After configuration, select **System > System and Signature Database**. Under System Information, the "HA State" item shows the device's HA status.

Device A

- HA State: Master

Device B

- HA State: Backup

Device A :



Device B :



When Device A fails to forward traffic or its eth0/0 is disconnected, Device B will turn to Active and starts forwarding without interrupting protected network.

Select **System > System and Signature Database**. Under System Information, the "HA State" item shows the device's HA status.

Device A

- HA State: Monitor Failed

Device B

- HA State: Master

Device A :



Device B :



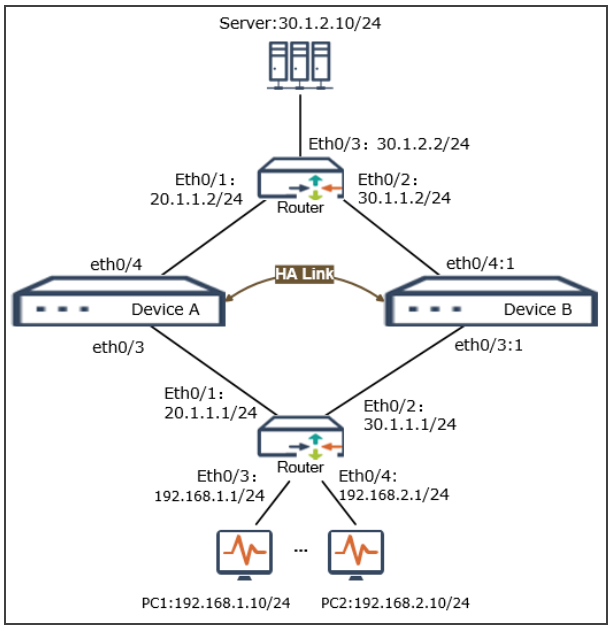
Making Two Firewalls Working in Hot Standby Mode by Deploying them in HA Peer to Ensure the Continuity of Service

This example introduces how to configure two firewalls to work in the HA Peer Active-Active(A/A) mode. They will backup each other while processing their own work in order that network communication will not be interrupted.

As shown in the figure below, without affecting the original network architecture, the two Hillstone firewalls Device A and Device B are connected transparently to the upstream and downstream devices.

The eth0/3 and eth0/4 interfaces of Device A are used to connected to the upstream and downstream routers. The eth0/3:1 and eth-0/4:1 interfaces of Device B are used to connected to the upstream and downstream routers. Also, Device A and Device B use the eth0/1 and eth0/2 interfaces as HA link interfaces.

Normally, both Device A and Device B forward the traffic from PC to the Server. When one of them fails, the other one takes over all the traffic.



Configuration Steps

Step 1: Configuring HA Peer

Device A

```
hostname(config)# ha link interface ethernet0/1
hostname(config)# ha link data interface ethernet0/2
hostname(config)# ha link ip 10.10.1.2/24
hostname(config)# ha cluster 1 peer-mode node 0
hostname(config)# ha group 0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# exit
hostname(config)# ha traffic enable
hostname(config)#
```

Device B

```
hostname(config)# ha link interface ethernet0/1
hostname(config)# ha link data interface ethernet0/2
hostname(config)# ha link ip 10.10.1.3/24
hostname(config)# ha cluster 1 peer-mode node 1
hostname(config)# ha group 0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# exit
hostname(config)# ha traffic enable
hostname(config)#
```

Step 2: Configuring the interfaces.

Device A

```
hostname(M0D1)(config)# interface ethernet0/4
hostname(M0D1)(config-if-eth0/4)# zone l2-untrust
hostname(M0D1)(config-if-eth0/4)# exit
hostname(M0D1)(config)# interface ethernet0/3
hostname(M0D1)(config-if-eth0/3)# zone l2-trust
hostname(M0D1)(config-if-eth0/3)# exit
hostname(M0D1)(config)# interface ethernet0/4:1
hostname(M0D1)(config-if-eth0/4:1)# zone l2-untrust
hostname(M0D1)(config-if-eth0/4:1)# exit
hostname(M0D1)(config)# interface ethernet0/3:1
hostname(M0D1)(config-if-eth0/3:1)# zone l2-trust
hostname(M0D1)(config-if-eth0/3:1)# exit
hostname(M0D1)(config)#
```

Step 3: Configuring track objects and binding them to HA groups.

Device A

```
hostname(M0D1)(config)# track track1 local
hostname(M0D1)(config-trackip)# interface ethernet0/3
hostname(M0D1)(config-trackip)# interface ethernet0/4
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
hostname(M0D1)(config)#
```

Device B

hostname(D0M1)(config)# **track track2 local**

hostname(D0M1)(config-trackip)# **interface ethernet0/3:1**

hostname(D0M1)(config-trackip)# **interface ethernet0/4:1**

hostname(D0M1)(config-trackip)# **exit**

hostname(D0M1)(config)# **ha group 1**

hostname(D0M1)(config-ha-group)# **monitor track track2**

hostname(D0M1)(config-ha-group)# **exit**

hostname(D0M1)(config)#

Step 4: Configuring an security policy.

hostname(M0D1)(config)# **policy-global**

hostname(M0D1)(config-policy)# **rule id 1**

Rule id 1 is created

hostname(M0D1)(config-policy-rule)# **src-zone trust**

hostname(M0D1)(config-policy-rule)# **dst-zone untrust**

hostname(M0D1)(config-policy-rule)# **service Any**

hostname(M0D1)(config-policy-rule)# **action permit**

hostname(M0D1)(config-policy-rule)# **exit**

hostname(M0D1)(config)#

Verification

Device A and Device B Working Normally

When Device A and Device B work normally, both of them forward traffic from PC to Server(IP： 30.1.2.10/24).

As shown below, you can use **trace 30.1.2.10** command to view the path information of the traffic on PC.

- Traffic forwarded by Device A:

```
VPCS> trace 30.1.2.10
trace to 30.1.2.10, 8 hops max, press Ctrl+C to stop
 1   192.168.2.1   3.474 ms  0.192 ms  0.177 ms
 2   20.1.1.2   4.373 ms  1.186 ms  1.469 ms
 3   *30.1.2.10   10.576 ms (ICMP type:3, code:3, Destination port unreachable)
```

- Traffic forwarded by Device B:

```
VPCS> trace 30.1.2.10
trace to 30.1.2.10, 8 hops max, press Ctrl+C to stop
 1   192.168.1.1   0.785 ms  0.234 ms  0.197 ms
 2   30.1.1.2   2.461 ms  1.020 ms  1.070 ms
 3   *30.1.2.10   2.150 ms (ICMP type:3, code:3, Destination port unreachable)
```

Device B Failing and Device A Working Normally

When Device B fails and Device A works normally, Device A takes over all the traffic from PC to server.

In this case, the status of Device A is still `(M0D1)`. The status of Device B changes from `(D0M1)` to `(D0F1)`. You can use **ping** command on the PC to test if PC can still connect to Server successfully.

```
VPCS> ping 30.1.2.10

84 bytes from 30.1.2.10 icmp_seq=1 ttl=62 time=3.603 ms
84 bytes from 30.1.2.10 icmp_seq=2 ttl=62 time=2.186 ms
84 bytes from 30.1.2.10 icmp_seq=3 ttl=62 time=2.529 ms
84 bytes from 30.1.2.10 icmp_seq=4 ttl=62 time=2.456 ms
84 bytes from 30.1.2.10 icmp_seq=5 ttl=62 time=2.351 ms
```

Using Two Devices as Gateways to Forward Business Traffic and Back Up Each Other Based on HSVRP, which Ensures Uniterrupted Business Traffic

This example introduces how to configure the HSVRP function when the firewall devices are deployed in the HA Peer A/A and work as gateways. So that, when one of the firewalls goes faulty, the original IP of its gateway can still be reached.

As shown in the figure below, the two Hillstone devices M0D1 and D0M1 are deployed in the Peer A/A mode. The connection of the interfaces on the two firewalls is as follows:

- M0D1:
  - The xethernet1/10 is used as the HA control link interface and xethernet2/10 is used as the HA data link interface.
  - The xethernet1/14 is directly connected to the upstream switch and its IP address is 20.1.1.11/24. The xethernet2/15 is directly connected to the downstream switch and its IP address is 30.1.1.11/16.
- D0M1:
  - The xethernet1/10 is used as the HA control link interface and xethernet2/10 is used as the HA data link interface.
  - The xethernet1/14:1 is directly connected to the upstream switch and its IP address is 20.1.1.12/24. The xethernet2/15:1 is directly connected to the downstream switch and its IP address is 30.1.1.12/16.

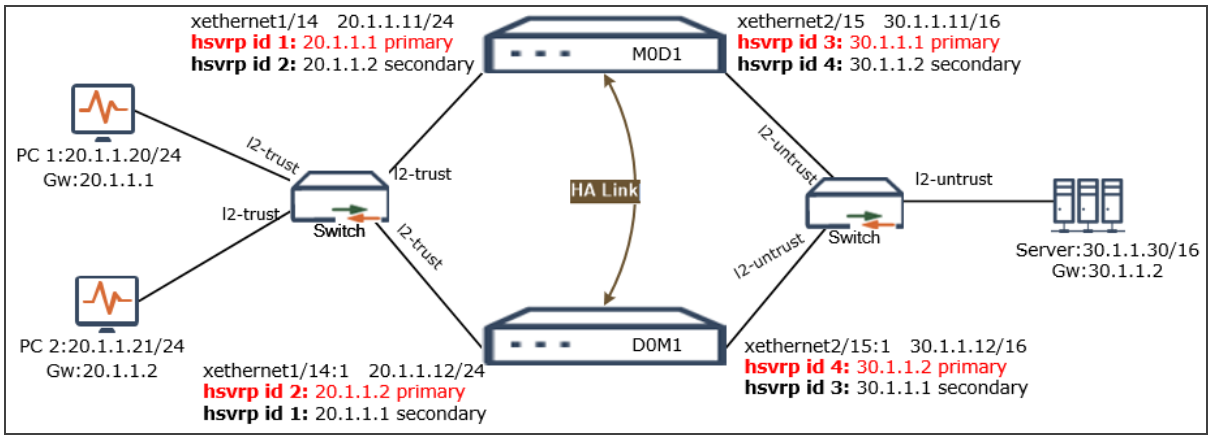
Four HSVRP groups are configured: hsvrp 1, hsvrp 2, hsvrp 3 and hsvrp 4. Their virtual IP address are different from each other.

Take hsvrp 1 and hsvrp 2 as example, the xethernet1/14 interface is used as the primary interface of hsvrp 1 and the xethernet1/14:1 interface is used as the secondary interface of hsvrp 1. The xethernet1/14:1 interface is used as the primary interface of hsvrp 2 and the xethernet1/14 interface is used as the secondary interface of hsvrp 2.

If D0M1 fails, the virtual IP address of hsvrp 1 will still take effect on the xethernet1/14 interface. And the virtual IP address of hsvrp 2 will take effect on the xethernet1/14 interface too.

The virtual IP address of hsvrp 1 is configured as the gateway of the host PC1. The virtual IP address of hsvrp 2 is configured as the gateway of the host PC2. The virtual IP address of hsvrp 4 is configured as the gateway of the server.

- If M0D1 and D0M1 work normally, M0D1 forwards the traffic from PC1 to Server and D0M1 forwards the traffic from PC2 to Server.
- If D0M1 fails and the gateways of PC2 and Server are not changed, M0D1 will forward all the traffic from PC1 and PC2. This ensures that network communication is not interrupted.



Configuration Steps

Step 1: Configuring HA Peer.

M0D1 Device

hostname(config)# **ha link interface xethernet1/10**

hostname(config)# **ha link data interface xethernet2/10**

hostname(config)# **ha link ip 172.16.1.1/24**

hostname(config)# **ha cluster 5 peer-mode node 0**

hostname(config)# **ha group 0**

hostname(config-ha-group)# **exit**

hostname(config)# **ha group 1**

hostname(config-ha-group)# **exit**

hostname(config)# **ha traffic enable**

hostname(config)# **exit**

D0M1 Device

hostname(config)# **ha link interface xethernet1/10**

hostname(config)# **ha link data interface xethernet2/10**

hostname(config)# **ha link ip 172.16.1.2/24**

hostname(config)# **ha cluster 5 peer-mode node 1**

hostname(config)# **ha group 0**

hostname(config-ha-group)# **exit**

hostname(config)# **ha group 1**

hostname(config-ha-group)# **exit**

hostname(config)# **ha traffic enable**

hostname(config)# **exit**

Step 2: Configuring HSVRP groups.

M0D1 Device

```
hostname(M0D1)(config)# hsvrp id 1
hostname(M0D1)(config-hsvrp)# ip address 20.1.1.1
hostname(M0D1)(config-hsvrp)# exit
hostname(M0D1)(config)# hsvrp id 2
hostname(M0D1)(config-hsvrp)# ip address 20.1.1.2
hostname(M0D1)(config-hsvrp)# exit
hostname(M0D1)(config)# hsvrp id 3
hostname(M0D1)(config-hsvrp)# ip address 30.1.1.1
hostname(M0D1)(config-hsvrp)# exit
hostname(M0D1)(config)# hsvrp id 4
hostname(M0D1)(config-hsvrp)# ip address 30.1.1.2
hostname(M0D1)(config-hsvrp)# exit
```

Step 3: Configuring interfaces and referencing the HSVRP group for the interfaces.

```
hostname(M0D1)(config)# interface xethernet1/14
hostname(M0D1)(config-if-xe1/14)# zone trust
hostname(M0D1)(config-if-xe1/14)# ip address 20.1.1.11/24
hostname(M0D1)(config-if-xe1/14)# hsvrp id 1 primary
hostname(M0D1)(config-if-xe1/14)# hsvrp id 2 secondary
hostname(M0D1)(config-if-xe1/14)# exit
```

```
hostname(M0D1)(config)# interface xethernet1/14:1
hostname(M0D1)(config-if-xe1/14:1)# zone trust
hostname(M0D1)(config-if-xe1/14:1)# ip address 20.1.1.12/24
hostname(M0D1)(config-if-xe1/14:1)# hsvrp id 2 primary
hostname(M0D1)(config-if-xe1/14:1)# hsvrp id 1 secondary
hostname(M0D1)(config-if-xe1/14:1)# exit
```

```
hostname(M0D1)(config)# interface xethernet2/15
hostname(M0D1)(config-if-xe2/15)# zone untrust
hostname(M0D1)(config-if-xe2/15)# ip address 30.1.1.11/16
hostname(M0D1)(config-if-xe2/15)# hsvrp id 3 primary
hostname(M0D1)(config-if-xe2/15)# hsvrp id 4 secondary
hostname(M0D1)(config-if-xe2/15)# exit
```

```
hostname(M0D1)(config)# interface xethernet2/15:1
hostname(M0D1)(config-if-xe2/15:1)# zone untrust
hostname(M0D1)(config-if-xe2/15:1)# ip address 30.1.1.12/16
hostname(M0D1)(config-if-xe2/15:1)# hsvrp id 4 primary
hostname(M0D1)(config-if-xe2/15:1)# hsvrp id 3 secondary
hostname(M0D1)(config-if-xe2/15:1)# exit
```

Step 4: Checking the configuration of the HSVRP groups.

M0D1 Device

```
hostname(M0D1)(config)# show hsvrp
==================================================
ID:                          1
Virtual IP:                  20.1.1.1  255.255.255.0
Virtual MAC:                 0000.5e00.0101
Primary bind interface:      xethernet1/14
Secondary bind interface:    xethernet1/14:1
Status:                      active(xethernet1/14)
==================================================
ID:                          2
Virtual IP:                  20.1.1.2  255.255.255.0
Virtual MAC:                 0000.5e00.0102
Primary bind interface:      xethernet1/14:1
Secondary bind interface:    xethernet1/14
Status:                      inactive
==================================================
ID:                          3
Virtual IP:                  30.1.1.1  255.255.255.0
Virtual MAC:                 0000.5e00.0103
Primary bind interface:      xethernet2/15
Secondary bind interface:    xethernet2/15:1
Status:                      active(xethernet2/15)
==================================================
```

```
ID:                          4
Virtual IP:                  30.1.1.2  255.255.255.0
Virtual MAC:                 0000.5e00.0104
Primary bind interface:      xethernet2/15:1
Secondary bind interface:    xethernet2/15
Status:                      inactive
==================================================
```

Step 5: Configuring an security policy.

```
hostname(M0D1)(config)# policy-global
hostname(M0D1)(config-policy)# rule id 1
Rule id 1 is created
hostname(M0D1)(config-policy-rule)# src-zone trust
hostname(M0D1)(config-policy-rule)# dst-zone untrust
hostname(M0D1)(config-policy-rule)# service Any
hostname(M0D1)(config-policy-rule)# action permit
hostname(M0D1)(config-policy-rule)# exit
hostname(M0D1)(config)#
```

Verification

M0D1 and D0M1 Working Normally

When M0D1 and D0M1 work normally, M0D1 forwards the traffic from PC1 to Server and D0M1 forwards the traffic from PC2 to Server.

As shown below, on the M0D1 device, in any configuration mode, you can use **show flow0-interface xethernet1/14** command to view the information of corresponding sessions.

```
SG-6000[DBG](M0D1)(config)# show session flow0-interface xethernet1/14
cpu1/1(6), session: id 6291455, proto 6, flag 104000, flag1 1020000, flag2 0, flag3 0, created 104245, life 1736, policy
 type 0, policy 1, app 4(FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0
  flow0(48(xethernet1/14)/40300b10): 20.1.1.20:45604→30.1.1.30:21
  flow1(75(xethernet2/15)/300b10): 30.1.1.30:21→20.1.1.20:45604

cpu2/1(10), session: id 6094847, proto 6, flag 204000, flag1 1010000, flag2 0, flag3 0, created 104293, life 1784, polic
y type 0, policy 1, app 4(FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0
  flow0(48(xethernet1/14)/40200910): 20.1.1.21:33532→30.1.1.30:21
  flow1(75(xethernet2/15)/200910): 30.1.1.30:21→20.1.1.21:33532
```

- The value "flag 104000" represents that this session is processed by M0D1 so it tests that M0D1 forwards the traffic from PC1 to Server.
- The value "flag 204000" represents that this session is processed by the peer device D0M1 so it tests that D0M1 forwards the traffic from PC2 to Server.

D0M1 Failing and M0D1 Working Normally

When D0M1 fails and the gateways of PC2 and Server are not changed, PC1 and PC2 can still connect to Server successfully. M0D1 forwards all the traffic from PC1 and PC2.

As shown below, on the M0D1 device, in any configuration mode, you can use **show flow0-interface xethernet1/14** command to view the information of corresponding sessions.

```
SG-6000[DBG](M0D1)(config)# show session flow0-interface xethernet1/14
cpu2/0(9), session: id 5931006, proto 6, flag 104000, flag1 1020000, flag2 0, flag3 0, created 109155, life 1686, policy
 type 0, policy 1, app 4(FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0
  flow0(48(xethernet1/14)/40300b10): 20.1.1.20:45610→30.1.1.30:21
  flow1(75(xethernet2/15)/300b10): 30.1.1.30:21→20.1.1.20:45610

cpu2/0(9), session: id 5996543, proto 6, flag 104000, flag1 1020000, flag2 0, flag3 0, created 109180, life 1711, policy
 type 0, policy 1, app 4(FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0
  flow0(48(xethernet1/14)/40300b10): 20.1.1.21:33540→30.1.1.30:21
  flow1(75(xethernet2/15)/300b10): 30.1.1.30:21→20.1.1.21:33540
```

- The value "flag 104000" represents that this session is processed by M0D1. That is to say, M0D1 forwards all the traffic from PC1 and PC2.

Quality of Service (QoS)

QoS adopts the concept "pipe" to indicate traffic control method. A pipe is a bandwidth limit. The system divides bandwidth by creating pipe of different sizes.

This chapter contains the following recipe:

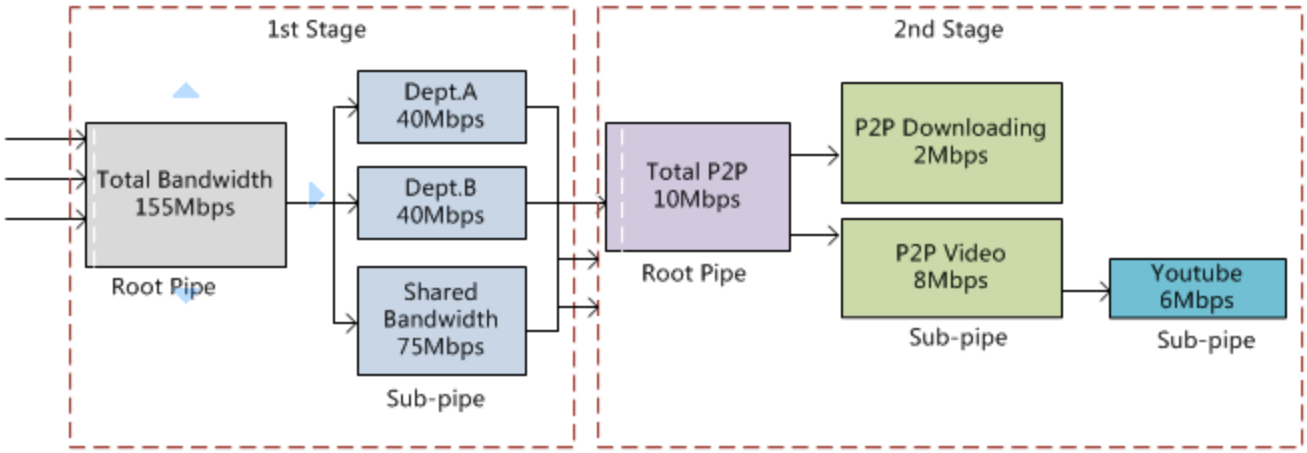
- " QoS Control" on Page 369
- "Outbound Link Load Balance" on Page 376
- "Outbound Link Load Balance with Customizable SLA Metrics" on Page 381

QoS Control

This examples shows how to control Internet bandwidth allocation to different users and applications. The key feature that applies in this situation is 2-Stage QoS flow control.

As shown in the topology below, a company of 155 MB Internet bandwidth has a 2-Stage QoS requirement:

- In 1st Stage QoS: Within the 155 Mbps bandwidth, 40 Mbps will be allocated to Department A, 40 Mbps to Department B, and the remaining 75 Mbps will be shared by all employees.
- In 2nd Stage QoS: The total P2P flow is limited to 10 Mbps, in which downloading is limited to 2 Mbps, streaming video is limited to 8 Mbps, and within the video bandwidth, Youku streaming is limited to 6 Mbps.



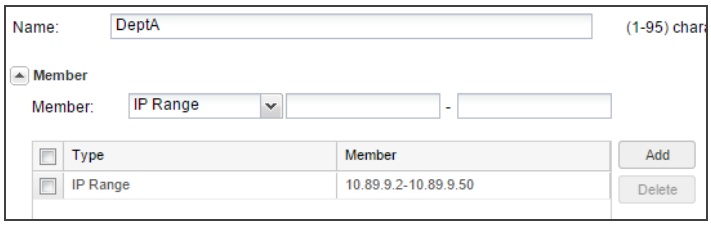


Configuration Steps

Step 1: Creating address entries for Dept. A and Dept. B

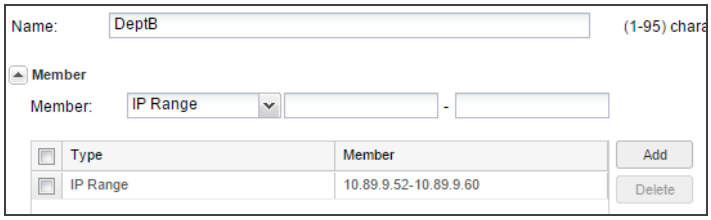
Select **Object > Address Entry**, and click **New**.

- Name: DeptA
- Member: select IP Range, and enter "10.89.9.2" and "10.89.9.50" and click **Add**.



Create another address entry:

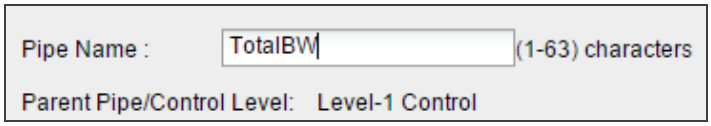
- Name: DeptB
- Member: select IP Range, and enter "10.89.9.52" and "10.89.9.60" and click **Add**.



Step 2: Create a root pipe of 155 Mbps under Level-1 Control

Select **Policy > QoS**, click **Level-1 Control**, and click **New > Pipe**.

- Pipe Name: TotalBW



Step 2: Create a root pipe of 155 Mbps under Level-1 Control

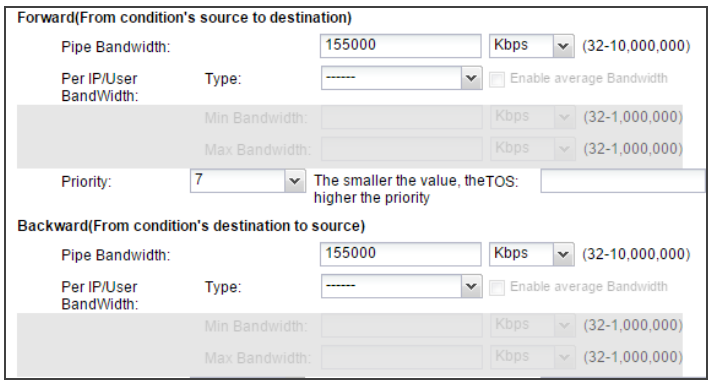
In the same tab, click **New**.

- Source Information
  - Interface: ethernet0/2



Under the Action tab:

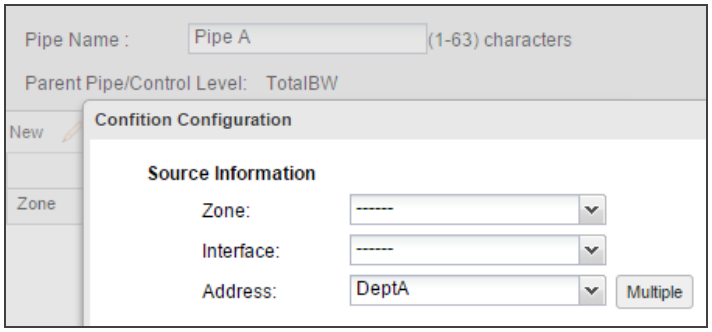
- Forward
  - Pipe Bandwidth: 155000 Kbps
- Backward
  - Pipe Bandwidth: 155000 Kbps

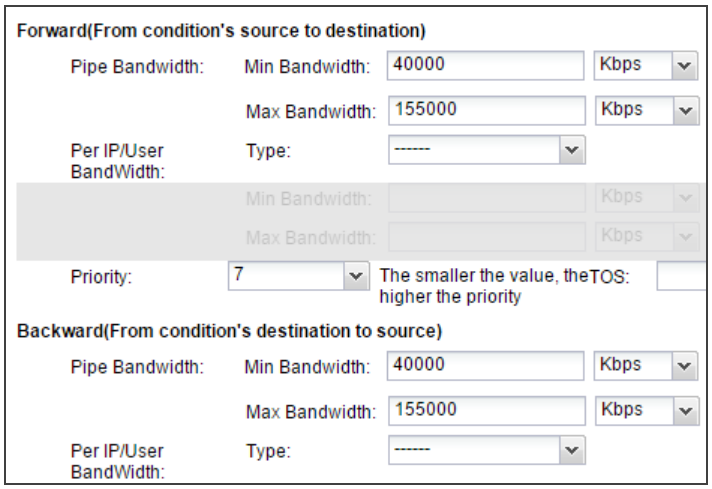


Step 3: Creating sub-pipes for two departments below root pipe

Select root pipe "TotalBW"and click **New**.

- Pipe Name: pipeA
- Click **New**, and under Source Information, select "DeptA" as Address.
- Click the Action tab:
  - Forward: Bandwidth: min: 40000 Kbps; max: 155000 Kbps
  - Backward Bandwidth: min:40000 Kbps; max: 155000 Kbps





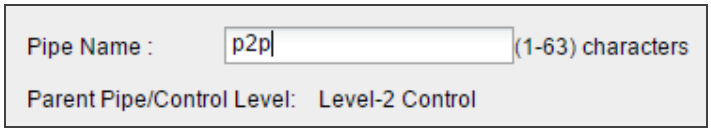
Use the same steps to create "pipe B":

- Pipe name: pipeB
- Source address: DeptB
- (Forward and Backward) min bandwidth: 40000 kbps
- (Forward and Backward) max bandwidth: 155000 kbps

Step 4: Creating root pipe "p2p" under Level-2 control to limit P2P total to 10 Mbps

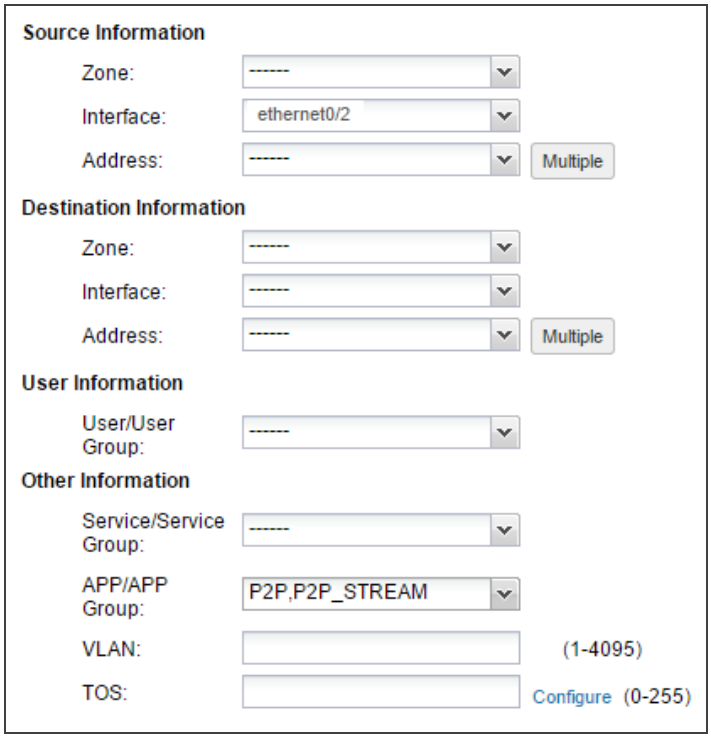
Select **Policy > QoS**, select Level-2 Control and click **New > Pipe**.

- Pipe Name: p2p



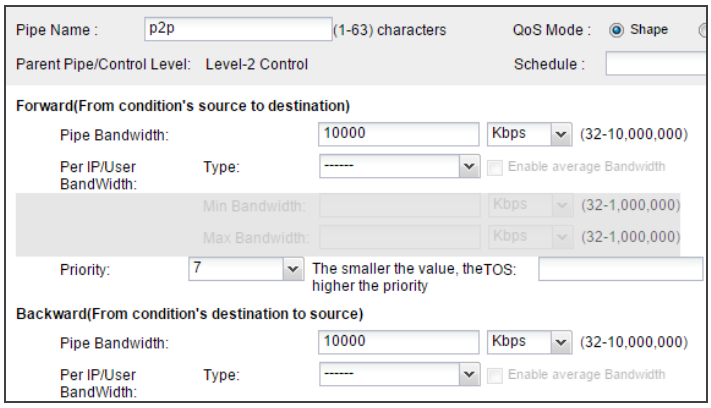
In the same tab, click **New**.

- Source Information
  - Interface: ethernet0/2
- Other
  - APP/APP Group: P2P. P2P_Stream



Under the Action tab:

- Forward
  - Bandwidth: 10000 kbps
- Backward:
  - Bandwidth: 10000 kbps

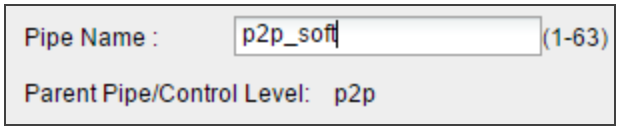


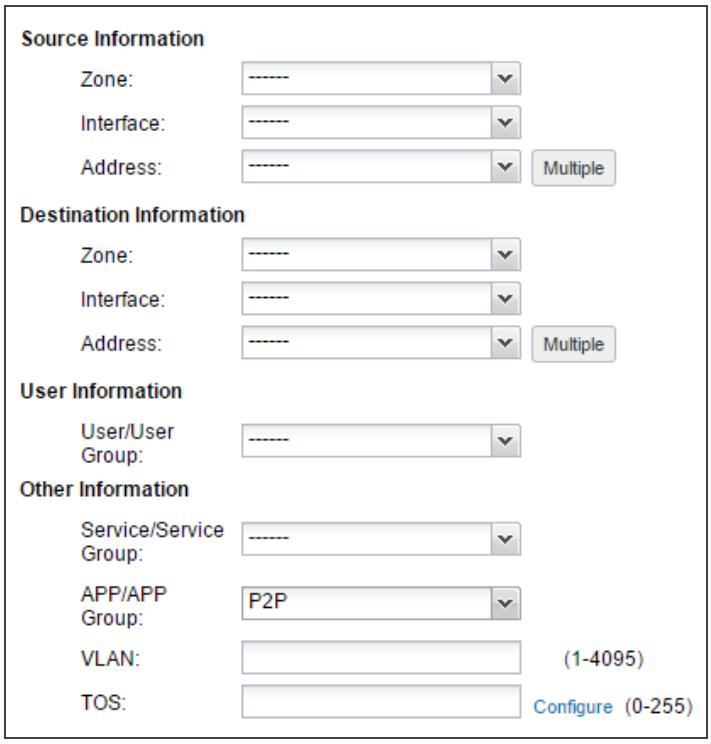
Step 5: Creating sub pipes under root pipe "p2p"

1. Creating a sub-pipe to limit p2p software

Under Level-2 Control, select root pipe "p2p", and click **New > Pipe**.

- Pipe Name: p2p_soft
- Click **New**: in the prompt, select **P2P** as APP/APP Group.
- Select the Action tab:
  - Forward bandwidth: min: 32; max 2000
  - Backward bandwidth: min: 32; max: 2000

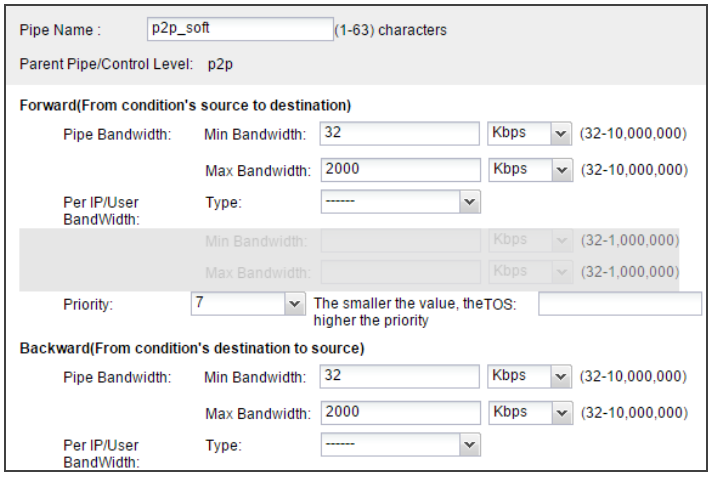




2. Creating a sub-pipe to limit p2p video streaming

Under Level-2 Control, select root pipe "p2p", and click **New > Pipe**.

- Pipe Name: p2p_stream
- Click **New**: in the prompt, select **P2P_Stream** as APP/APP Group.
- Select the Action tab:
  - Forward bandwidth: min: 32; max 8000
  - Backward bandwidth: min: 32; max: 8000



3. Creating a sub-pipe to limit p2p video streaming

Under Level-2 Control, select sub pipe "p2p_stream", and click **New > Pipe**.

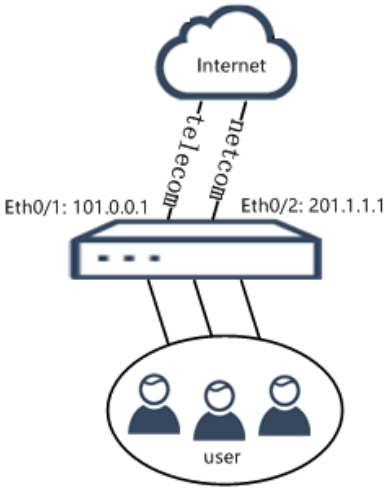
Step 5: Creating sub pipes under root pipe "p2p"

- Pipe Name: p2p_stream
- Click **New**: in the prompt, select **Youku** and **Youku_Stream** as APP/APP Group.
- Select the Action tab:
  - Forward bandwidth: min: 32; max 6000
  - Backward bandwidth: min: 32; max: 6000

Outbound Link Load Balance

This example shows how to configure outbound link load balancing. Through the configuration of efficient drainage strategy to achieve dynamic link load balancing, improve the export bandwidth utilization.

As shown in the following figure, this lab environment simulates the deployment of equipment at the second-level ISP exit scene.The second-level ISP rent Tele-com, China Netcom and other operators of the bandwidth to the user to achieve Internet access. The figure use 101.0.0.1 to connect to the Internet by Tele-com and 201.1.1.1 to connect to Netcom.

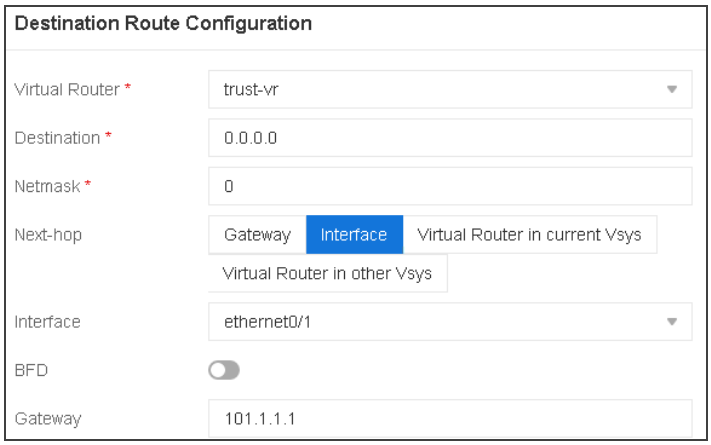


Configuration Steps

Step 1: Configure multiple equal-cost routes

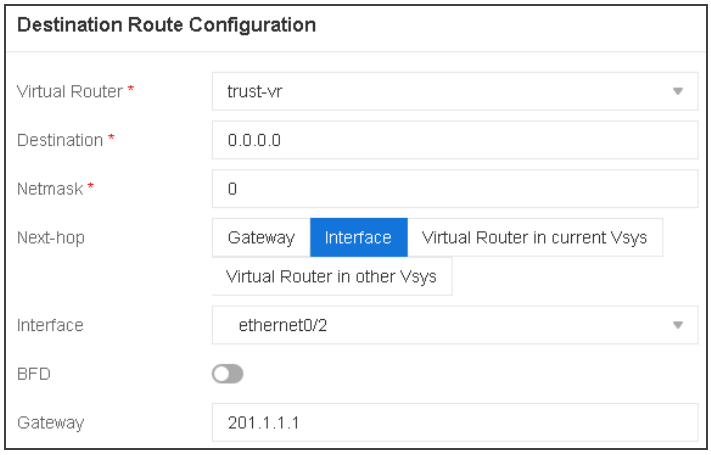
1.Select **Network > Routing >Destination Route**, and click **New**.

- Destination：0.0.0.0
- Subnet Mask：0
- Next Hop：interface
- Interface：ethernet0/1
- Gateway：101.1.1.1



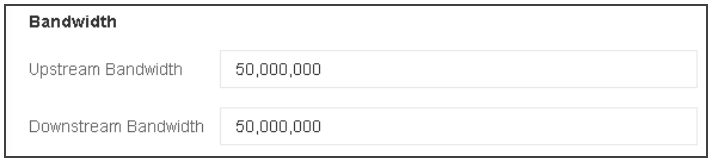
2.Select **Network > Routing >Destination Route**, and click **New**to configure another equal-cost route.

- Destination：0.0.0.0
- Subnet Mask：0
- Next Hop：interface
- Interface：ethernet0/2
- Gateway：201.1.1.1



Step 2: Configure the outbound interface bandwidth

Network > Interface, select interface ethernet0 / 1, and click **Edit** to configure the bandwidth as 50M (according to the actual situation to determine the value of the configuration bandwidth).

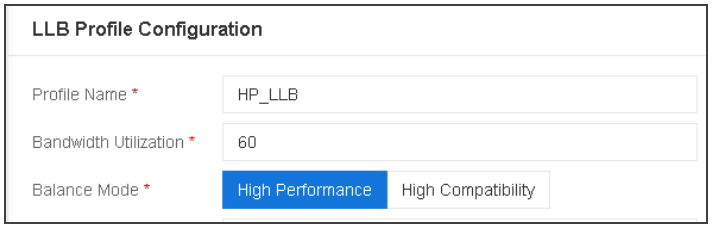


- Bandwidth
  - Up Bandwidth： 50000000bps
  - Down Bandwidth： 50000000bps

Follow the same steps to set the bandwidth of the interface ethernet0 / 2 to 50M.

Step 3: Configure the outbound load balancr profile

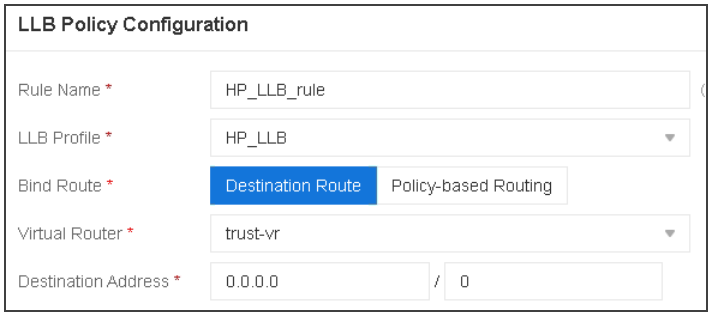
Select **Network > Outbound >Profile**, click **New**.



- Profile： HP_LLB
- Bandwidth Utillzation : 60%
- Balance Mode： High Performance

Step 4: Configure the outbound load balancr rule

Select **Network > Outbound >Rule**, click **New**.



- Rule Name: HP_LLB_rule
- LLB Profile: Select the Profile "HP_LLB"
- Bind Route: Destination Route
- Vitual Router: trust-vr
- Destination Address: 0.0.0.0/0

Step 5: Verify that outbound load balance is in effect

After completing the above steps, use the test tool to construct traffic through ethernet0/1 and ethernet0/2, respectively, and then observe the traffic on each link.By changing the size of outgoing traffic,you can find that the traffic on two links can be adjusted equitably. The system routing mechanism is as follows:

- When the bandwidth of each link does not exceed 30M (50M*60%), the system calculates the link overhead based on the link delay, jitter and packet loss rate. The link with the lower link overhead eventually allocates more traffic, while the other link has less traffic,but the two links are basically balanced.
- When the link bandwidth exceeds 30M, the system adds the bandwidth utilization factor to the calculation, that is, the system calculates the link overhead based on the delay, jitter, packet loss rate and bandwidth utilization. The link with lower link overhead eventually allocates more traffic, while the other link has less traffic, but the two links are basically balanced.

Q&A

- Q: What factors in the network affect the link load balancing routing of the system?

  A: The delay, jitter, packet loss rate and bandwidth utilization of each link are the impact factors. System can intelligently oute and dynamically adjust the traffic load of each link by monitoring the delay, jitter, packet loss rate and bandwidth utilization of each link in real-time.

- Q: Which modes do link load balancing support?

  A: Two load balancing modes are supported, namely, high performance and high compatibility modes.

  - High Performance - In this mode, system adjusts link to keep the link balance as fast as possible
  - High Compatibility - In this mode, When the link load changes, system does not switch the link frequently, but ensures that the service is as far as possible on the previous link. This mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.

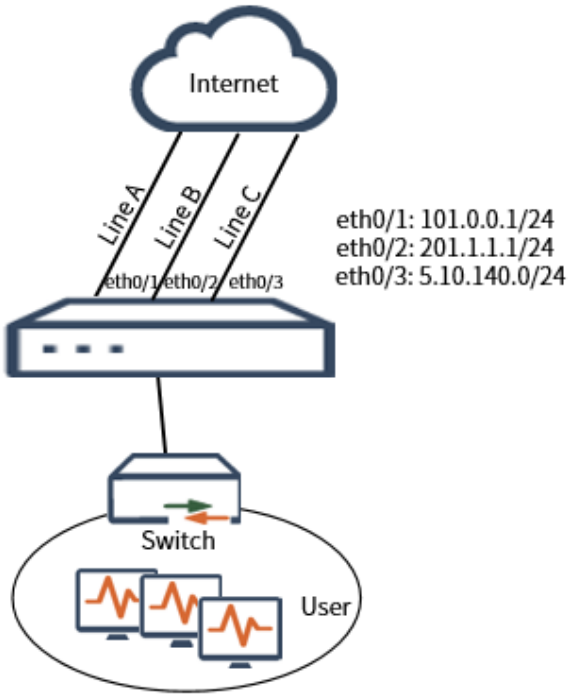
Outbound Link Load Balance with Customizable SLA Metrics

In a multi-egress Internet line deployment environment, for some mission-critical applications that are extremely sensitive to packet loss rate, this example introduces how to configure outbound line load balancing combined with customizable SLA metrics to prioritize lines with lower packet loss rates for critical business connections to the Internet.

As shown in the following figure, a company has three egress lines, A, B, and C, each connected to the Internet through different ISP dedicated lines:

- Line A: Connected to a certain ISP dedicated line via eth0/1 (IP: 101.0.0.1);
- Line B: Connected to another ISP dedicated line via eth0/2 (IP: 201.1.1.1);
- Line C: Connected to a third ISP dedicated line via eth0/3 (IP: 5.10.140.0).

The company has multiple research and development centers across the country, and efficient communication is required between them. Tencent Meeting is the company's primary communication tool. The requirement is to configure the system so that employees prefer lines with lower packet loss rates when using Tencent Meeting, thus ensuring smooth voice and video calls.



*This example is configured and verified by using 5.5R11 in a test environment. Please configure the IP address for each interface based on the actual condition.

Configuration Instructions

The SG-6000-K9180/K6580 and X-series devices do not support SLA functionality.

Configuration Roadmap

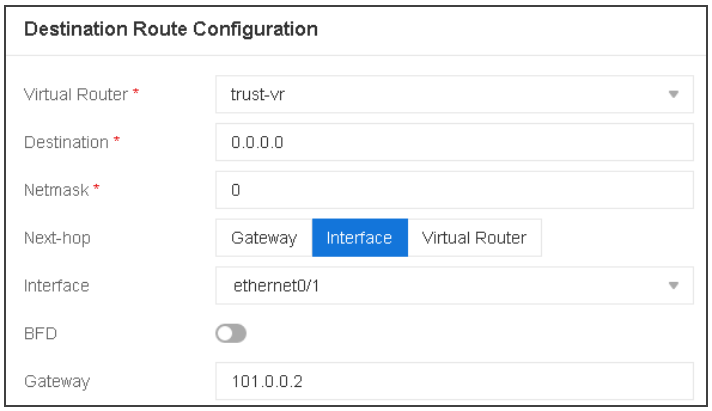
1. Configure equal-cost routes to enable load balancing and forwarding of traffic across all egress interfaces.
2. Configure policy-based routes to direct Tencent Meeting application traffic to the three egress lines.
3. Configure outbound line load balance rule based on SLA packet loss threshold values to exclude lines that do not meet the required packet loss rate, set the LLB packet loss priority factor to prefer lines with lower packet loss rates, and combine the policy-based routes with the outbound line load balance rule to achieve control and load balancing of Tencent Meeting traffic.

Configuration Steps of WebUI

Step 1: Configure multiple equal-cost routes

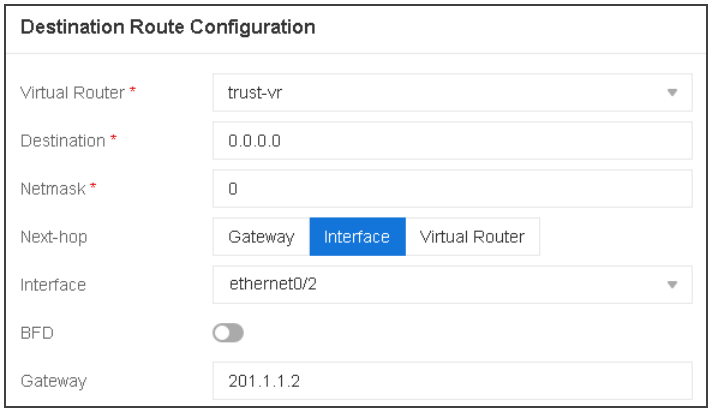
1.Select **Network > Routing > Destination Route**, and click **New**.

- Vitual Router: trust-vr
- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: interface
- Interface: ethernet0/1
- Gateway: 101.0.0.2



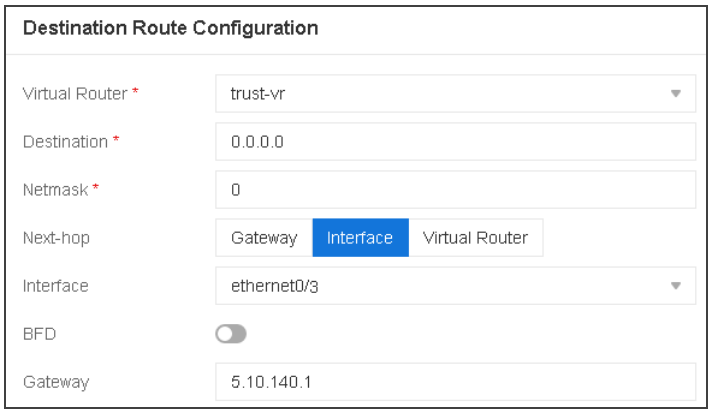
Step 1: Configure multiple equal-cost routes

2.Select **Network > Routing > Destination Route**, and click **New**to configure another equal-cost route.



- Vitual Router: trust-vr
- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: interface
- Interface: ethernet0/2
- Gateway: 201.1.1.2

3.Select **Network > Routing >Destination Route**, and click **New**to configure another equal-cost route.

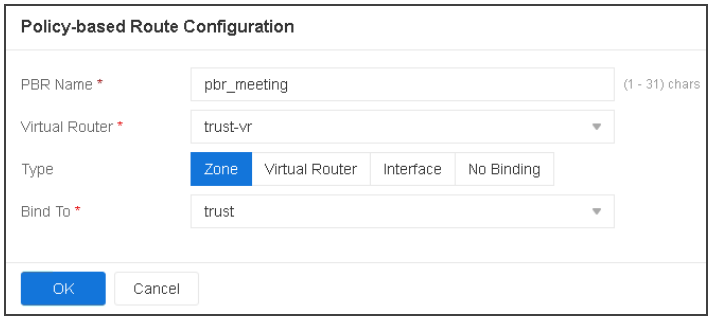


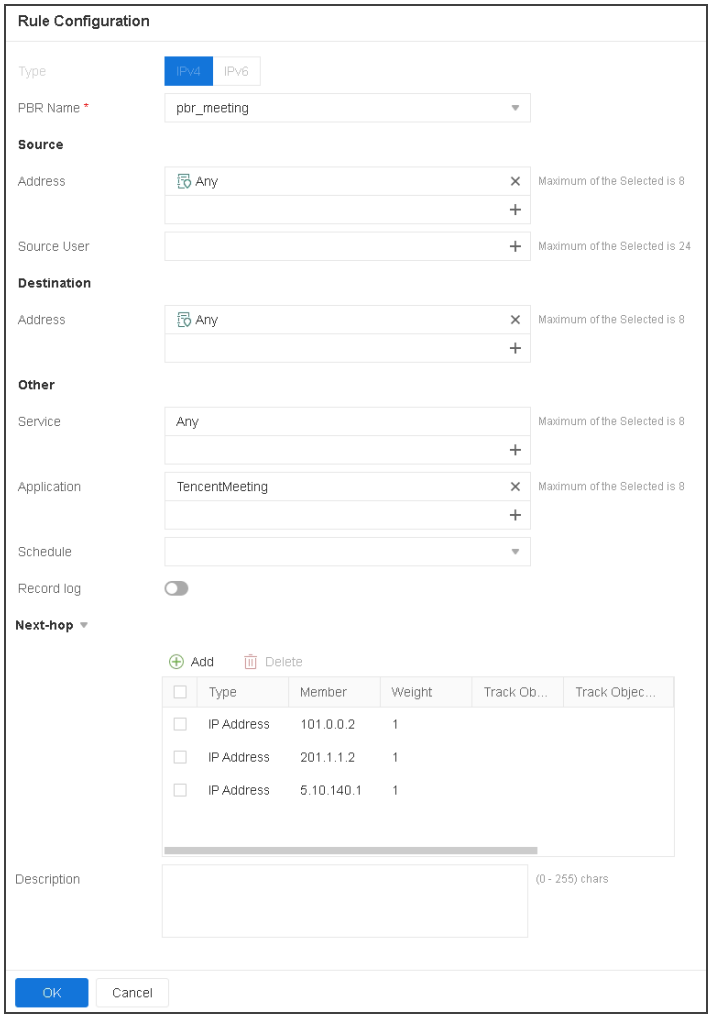
- Vitual Router: trust-vr
- Destination: 0.0.0.0
- Subnet Mask: 0
- Next Hop: interface
- Interface: ethernet0/3
- Gateway: 5.10.140.1

Step 2: Configure policy-based routes

Select **Network > Routing > Policy-based Routing**, click **New**, and select **Rule** from the drop-down list.

- PBR Name: Click ⊕ from the drop-down list.
  - PBR Name: pbr_meeting
  - Vitual Router: trust-vr
  - Type: Zone
  - Bind to: trust
- Source
  - Address: any
- Destination
  - Address: any
- Other
  - Application: TencentMeeting
- Next-hop
  - Click ⊕ to add a "IP Address" type of next hop with the member "101.0.0.2". Repeat this step to add next hops with members "201.1.1.2" and "5.10.140.1".

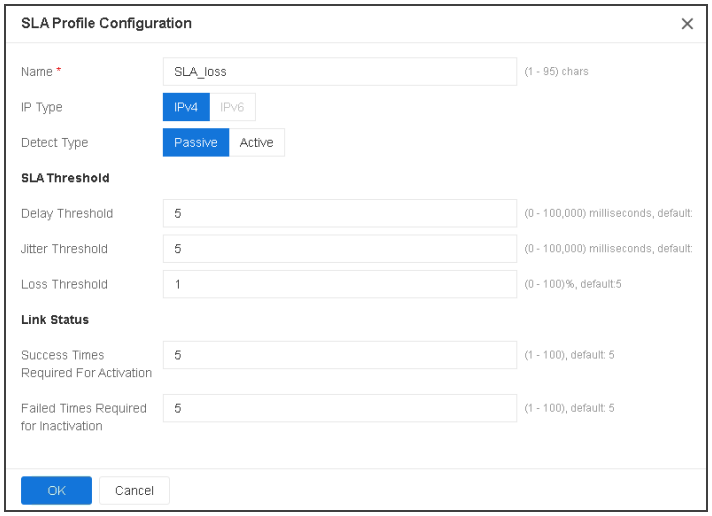


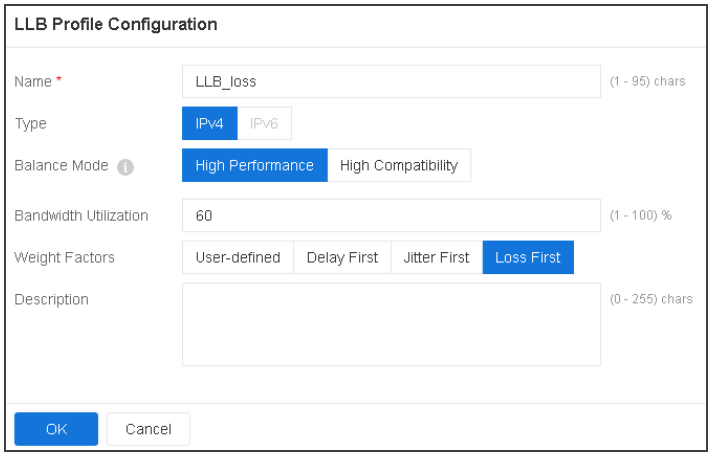


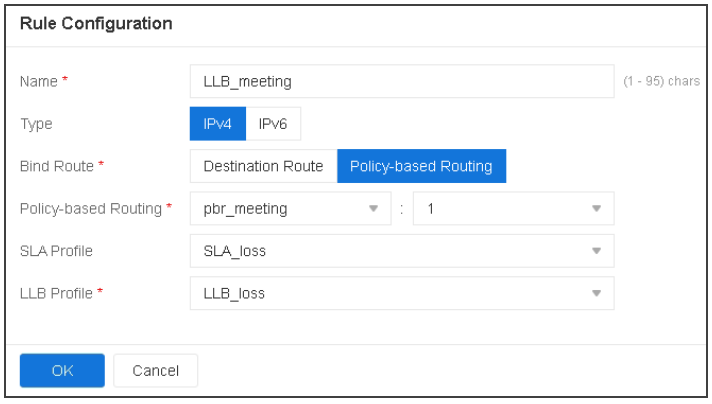
Step 3: Configure the outbound line load balance rule

Select **Network > Outbound LLB> Rule**, click **New**.

- Name: LLB_meeting
- Bind Route: Policy-based Routing
- Policy-based Routing： Select "pbr_meeting"
- SLA Profile: Click ⊕ from the drop-down.
  - Name: SLA_loss
  - Detect Type: Passive
  - Loss Threshold: 1
- LLB Profile: Click ⊕ from the drop-down.
  - Name:LLB_loss
  - Weight Factors: Select "Loss First"







Step 4: Results

After completing the above steps, when employees are using Tencent Meeting, by observing the Tencent Meeting traffic on each link, it is found that the system can basically prioritize lines with lower packet loss rates. For example, if only Line A and Line B meet the SLA criteria, while Line C does not, and Line A has a lower packet loss rate than Line B, by executing the command "**`show session application TencentMeeting`**" to check the Tencent Meeting application sessions, it can be observed that the interface ethernet0/1 of Line A has the highest Tencent Meeting sessions, the interface ethernet0/2 of Line B has a lower Tencent Meeting sessions, and the interface ethernet0/3 of Line C has no Tencent Meeting sessions.

Configuration Steps of CLI

Step 1: Configure multiple equal-cost routes

hostname(config)# `ip vrouter trust-vr` (Enter the VRouter configuration mode)

hostname(config-vrouter)# `ip route 0.0.0.0/0 ethernet0/1 101.0.0.2` (Configure the first equal-cost route)

hostname(config-vrouter)# `ip route 0.0.0.0/0 ethernet0/2 201.1.1.2` (Configure the second equal-cost route)

hostname(config-vrouter)# `ip route 0.0.0.0/0 ethernet0/3 5.10.140.1` (Configure the third equal-cost route)

hostname(config-vrouter)# `exit`

hostname(config)#

Step 2: Configure policy-based routes

hostname(config)# `pbr-policy pbr_meeting` (Create a PBR policy and enter the PBR policy configuration mode)

hostname(config-pbr)# `match top any any any TencentMeeting nexthop 101.0.0.2` (Create the first PBR policy)

Info: Match ID 1 is created

hostname(config-pbr)# `match top any any any TencentMeeting nexthop 201.1.1.2` (Create the second PBR policy)

Info: Match ID 2 is created

hostname(config-pbr)# `match top any any any TencentMeeting nexthop 5.10.140.1` (Create the third PBR policy)

Info: Match ID 3 is created

hostname(config-pbr)# `exit`

hostname(config)#

Step 3: Configure SLA Profile

hostname(config)# `sla-profile SLA_loss` (Create an SLA profile and enter the SLA profile configuration mode)

hostname(config-sla-profile)# `detect-mode passive type ipv4` (Set the detection mode to passive detection mode)

hostname(config-sla-profile)# `threshold lossrate-thres 1` (Set SLA packet loss rate threshold)

hostname(config-sla-profile)# `exit`

hostname(config)#

Step 4: Configure LLB Profile

hostname(config)# `llb profile LLB_loss` (Create an LLB profile and enter the LLB profile configuration mode)

hostname(config-llb-profile)#`detect weight-factors predefine loss-template` (Set packet loss rate as the primary influence factor for link cost)

hostname(config-llb-profile)# `exit`

hostname(config)#

Step 5: Configure the outbound line load balance rule

hostname(config)# `llb rule LLB_meeting pbr pbr_meeting id 1 profile LLB_loss SLa-profile SLA_loss` (Bind SLA profile and LLB profile to the route to form an LLB rule)

hostname(config)#

Step6: Results

After completing the above steps, when employees are using Tencent Meeting, by observing the Tencent Meeting traffic on each link, it is found that the system can basically prioritize lines with lower packet loss rates. For example, if only Line A and Line B meet the SLA criteria, while Line C does not, and Line A has a lower packet loss rate than Line B, by executing the command "**`show session application TencentMeeting`**" to check the Tencent Meeting application sessions, it can be observed that the interface ethernet0/1 of Line A has the highest Tencent Meeting sessions, the interface ethernet0/2 of Line B has a lower Tencent Meeting sessions, and the interface ethernet0/3 of Line C has no Tencent Meeting sessions.

Threat Prevention

Threat prevention, that device can detect and block network threats occur. By configuring the threat protection function, Device can defense network attacks, and reduce losses caused by internal network.

This chapter includes the following recipes:

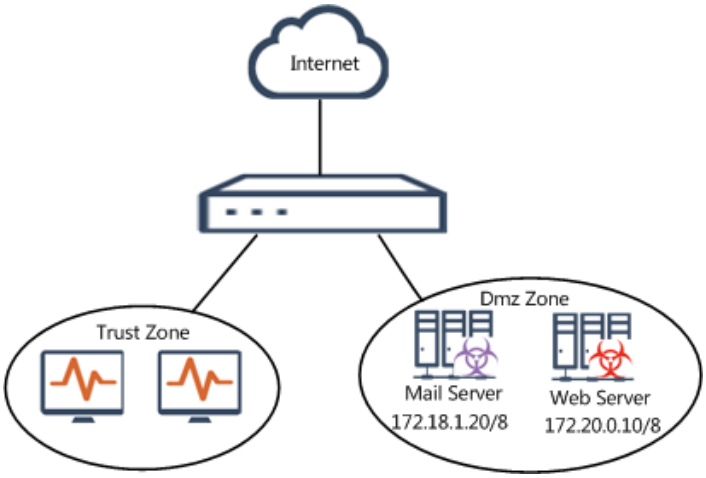
- "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 390
- "Protecting Intranet to Defend Attacks via Intrusion Prevention System" on Page 398
- "Forensic Analysis " on Page 406
- "Identifying IoT Assets to Enable Security Control of IoT by Using Built-in Docker" on Page 416
- "Identifying IoT Assets to Enable Security Control by Deploying the Asset Identifying System on the VM" on Page 431

Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection

This example introduces how to use Abnormal Behavior Detection to find attacks about servers as early as possible, and integrate with Mitigation to protect servers better.

As shown in the topology, the device is deployed in the data center exit. After enable and configure the Abnormal Behavior Detection, when a Web server is infected by SYN flood frequently, a mail server is infected by port scan attacks periodically, Trojan implanted to the intranet host, Trojan fake domain name by DGA algorithm technology, and connect external network control server, the administrator can find these attacks and protect the internal hosts and servers.

* To use Abnormal Behavior Detection, apply and install the StoneShield license.



Configuration Steps

Step 1: Enabling Abnormal Behavior Detection to defend internal hosts

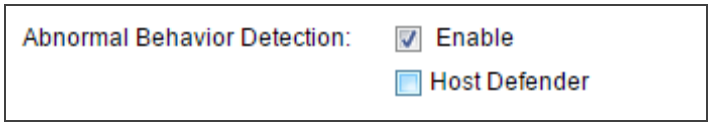
Select **Network > Zone**. Select '**trust**' zone, click **Edit**, and select the <Threat Protection>tab.



- Abnormal Behavior Detection: Select the **Enable** check box .
- Host Defender : Select the **Host Defender** check box. To enable the abnormal behavior detection of the HTTP factor, select the **Advanced Protection** check box. To enable the DDoS protection for the host, select the **DDoS Protection** check box. To capture and save the corresponding evidence that leads to the alarm of abnormal behavior, select **Forensic**.

Step 2: Configuring the critical asset object (Web Server and Mail Server)

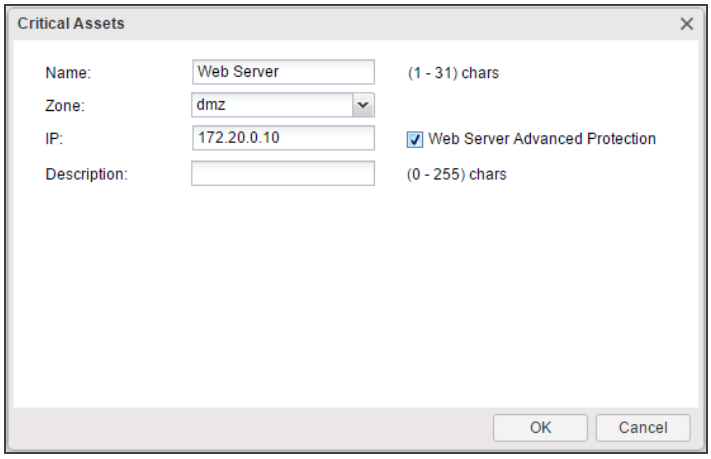
Select **Network > Zone**. Select '**dmz**' zone, click **Edit**, and select the <Threat Protection>tab.



- Abnormal Behavior Detection: Select the **Enable** check box .

Step 2: Configuring the critical asset object (Web Server and Mail Server)

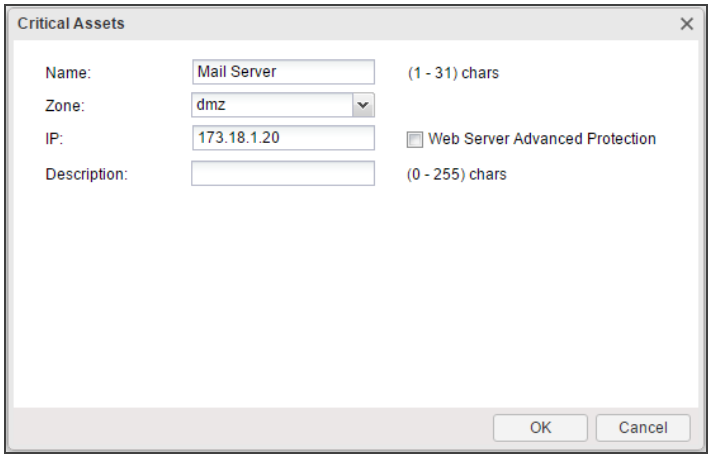
1. Configuring the Abnormal Behavior Detection object (Web Server), and enabling the web server advanced protection.



Click **Object > Critical Assets**, and click **New**.

- Name: Web Server
- Type: Server
- IP: 172.20.0.10
- Web Server Advanced Protection: Select the check box.

2. Configuring the Abnormal Behavior Detection object (Mail Server)



Click **Object > Critical Assets**, and click **New**.

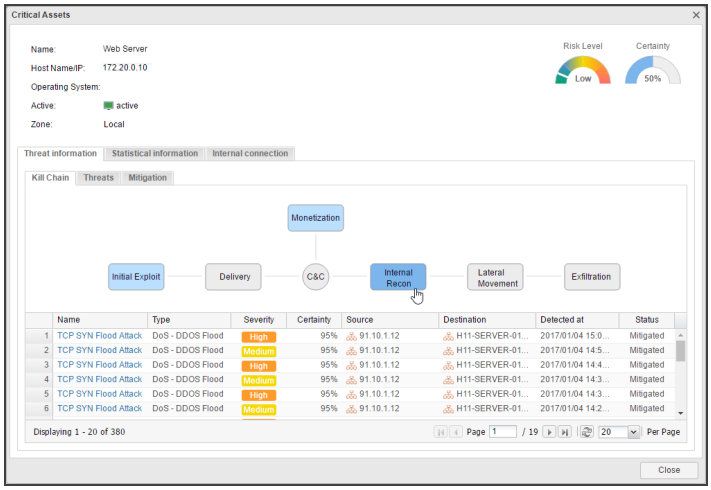
- Name: Mail Server
- Type: Server
- IP: 172.18.1.20

Step 3: Viewing the results of Abnormal Behavior Detection

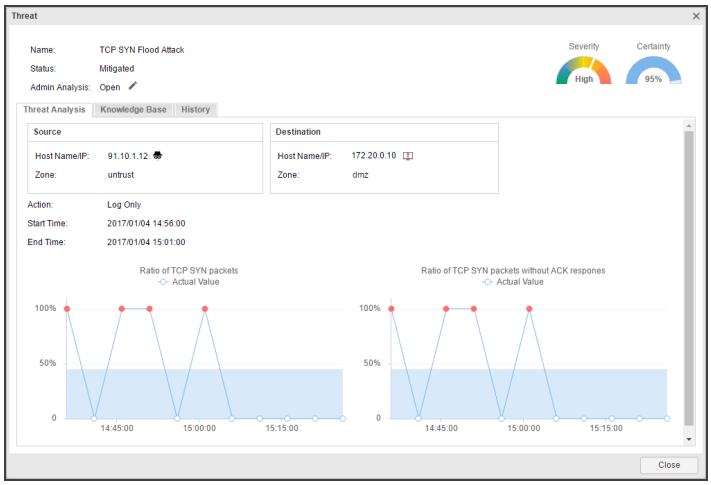
1. Viewing the results from iCenter

Results of Web Server:

- Select **iCenter>Critical Assets**, click the critical assets name **'Web Server'** link in the list, to view the information of this critical asset.



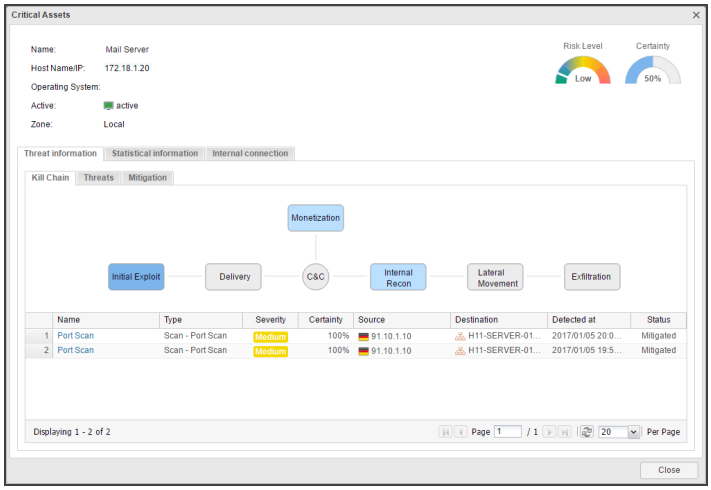
- For example, click the **Internal Recon> 'TCP SYN Flood Attack'** link in the kill chain list, to view the Abnormal Behavior Detection information and the trend chart of the actual value, predictive value of the detected object.



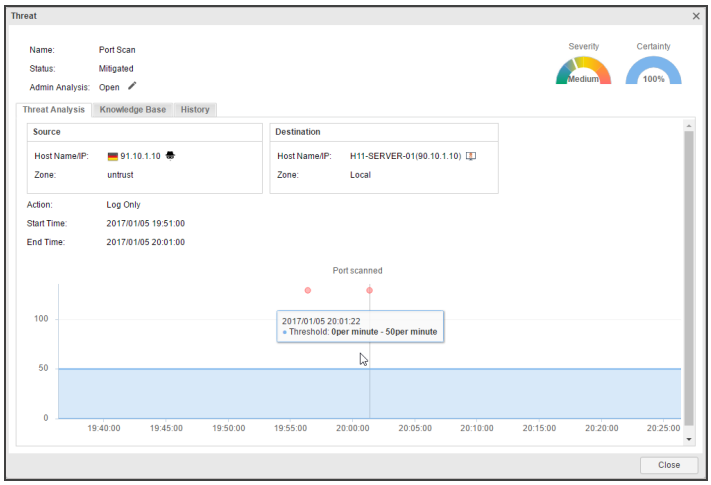
Step 3: Viewing the results of Abnormal Behavior Detection

Results of Mail Server:

- Select **iCenter>Critical Assets**, click the critical assets name **'Mail Server'** link in the list, to view the information of this critical asset.



- For example, click the **Initial Exploit> 'Port Scan'** link in the kill chain list, to view the Abnormal Behavior Detection information and the trend chart of the baseline, thresholds of the detected object.

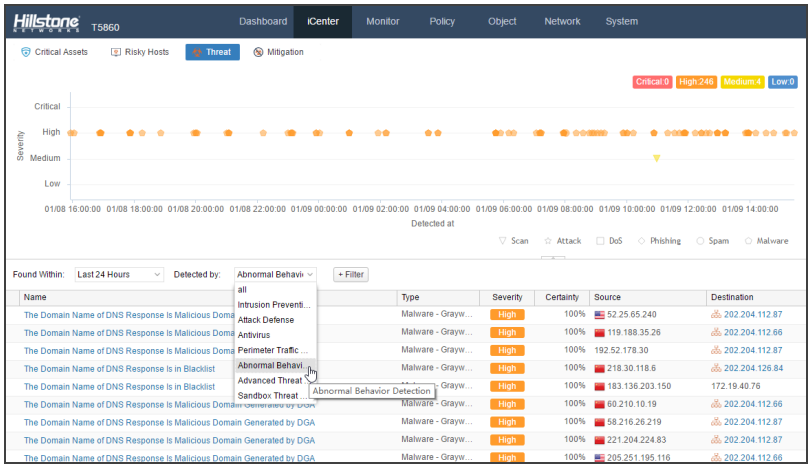


Step 3: Viewing the results of Abnormal Behavior Detection

Results of Internal Host:

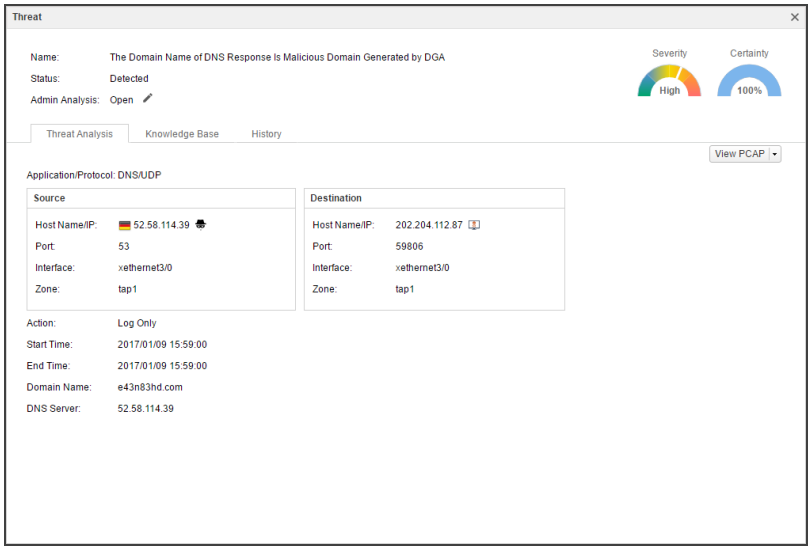
1. Click **iCenter > Threat**, and click Filter to add conditions.

- Detected by : Abnormal Behavior Detection



2. For example, click the **The Domain Name of DNS Response Is Malicious Domain Generated by DGA** link in the list, to view the malware and abnormal behavior attack details detected according the DNS mapping.

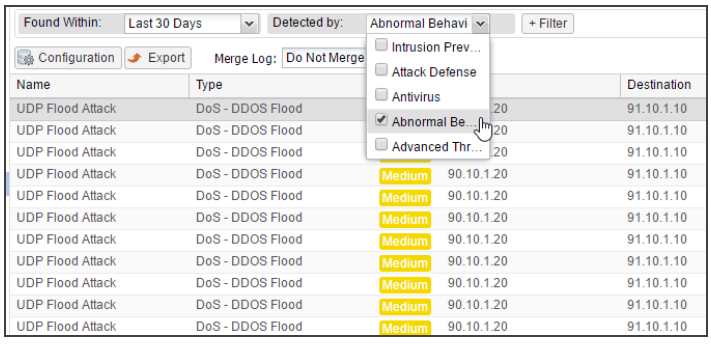
In **Threat Analysis** tab, you can view the information of host that send DGA fake domain name attack.



2. Viewing the results from threat log

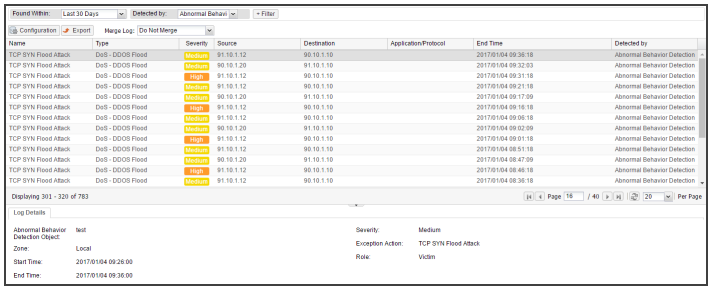
1. Select **Monitor>Log>Threat**, click Filter to add conditions to show logs that march your filter.

- Detected By: Abnormal Behavior Detection



Step 3: Viewing the results of Abnormal Behavior Detection

2. The log of Abnormal Behavior Detection will be displayed.



Step 4: Integrating with Mitigation, and configuring the mitigation rules for attacks.

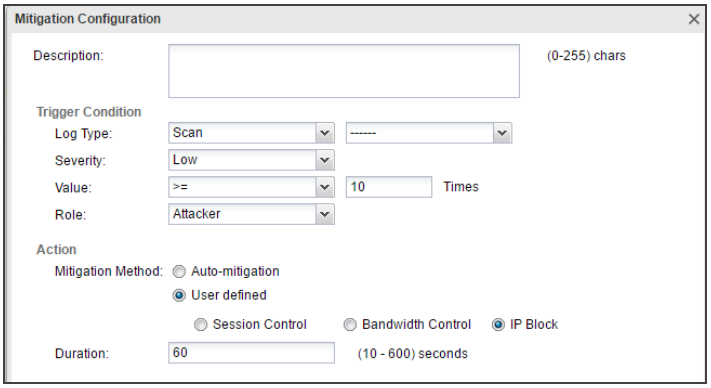
Select **iCenter> Mitigation> Mitigation Rule**, and select the **Enable Auto Mitigation** check box.



Configuring mitigation rules for Port Scan

In **Mitigation Rule**page, click **New**

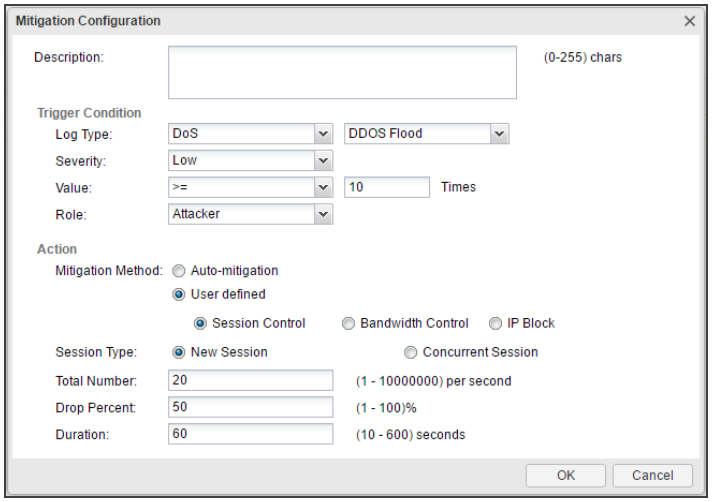
- Log Type: Scan
- Severity: Low
- Value: >= 10 Time
- Action Type: User defined > IP Block
- Duration: 60



Step 4: Integrating with Mitigation, and configuring the mitigation rules for attacks.

Configuring mitigation rules for TCP SYN Flood Attack

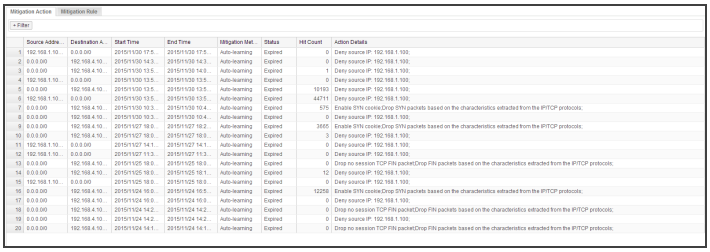
In **Mitigation Rule**page, click **New**



- Log Type: DoS> DDoS Flood
- Severity: Low
- Value: >= 10 Time
- Role: Attacker
- Action Type: User defined >Session Control
- Session Type: New Session
- Total Number: 20
- Drop Percent: 50
- Duration: 60

Step 5: Viewing the results of mitigation rules

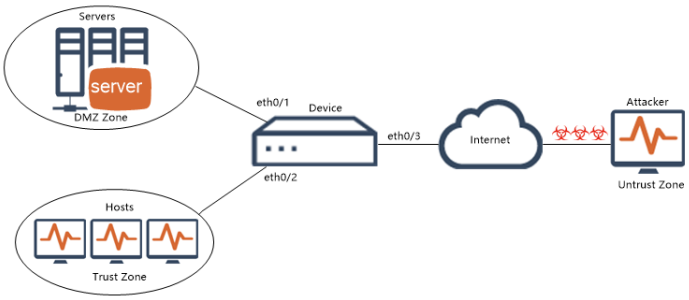
Click **iCenter > Mitigation>Mitigation Action** to view the mitigation action results details of mitigation rules



Protecting Intranet to Defend Attacks via Intrusion Prevention System

This example introduces how to use Intrusion Prevention System to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration.

As shown in the following topology, the device is deployed in the Intranet exit. After enabling and configuring the Intrusion Prevention System, the device will protect Intranet against internet attacks.



Configuration Steps

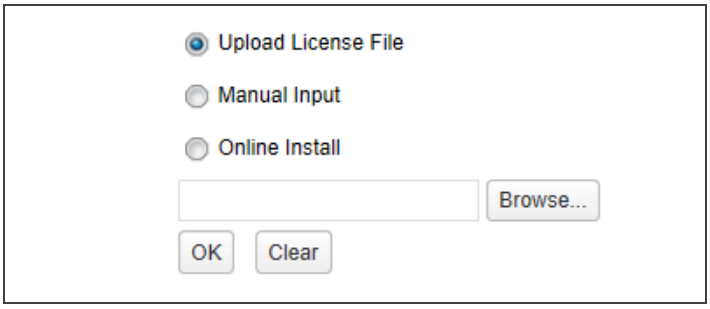
Step 1: Installing the Intrusion Prevention System license

1. Select **System> License**. Under **License Request**, input all user information. Then send the code to your sales contact. The sales person will get the license and send it back to you.



Step 1: Installing the Intrusion Prevention System license

2. Select **Upload License File**, Click **Browse** to select the Intrusion Prevention System license file, and then click **OK** to upload it.

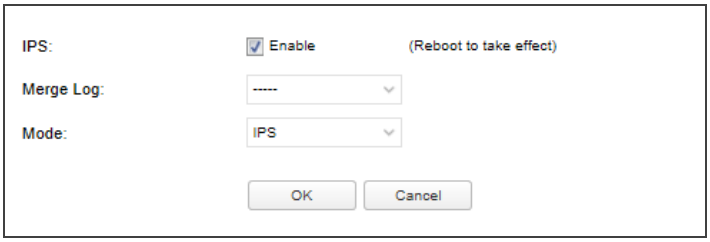


3. Select **System > Device Management>Option**, and click **Reboot**. When it starts again, the installed license will take effect.



Step 2: Enabling Intrusion Prevention System and updating Signature Database

1. Select **Object>Intrusion Prevention System>Configuration** to view the Intrusion Prevention System function status. If disabled, click **Enable** and reboot.



2. Select **System>Upgrade Management>Signature Database Update**. Under **IPS Signature Database Update**, click **Update** to update IPS Signature Database to assure its integrity and accuracy.

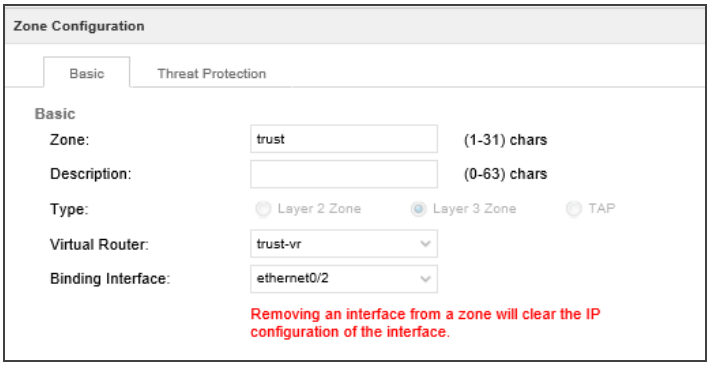


Step 3: Binding internal and external interfaces to the specified zones

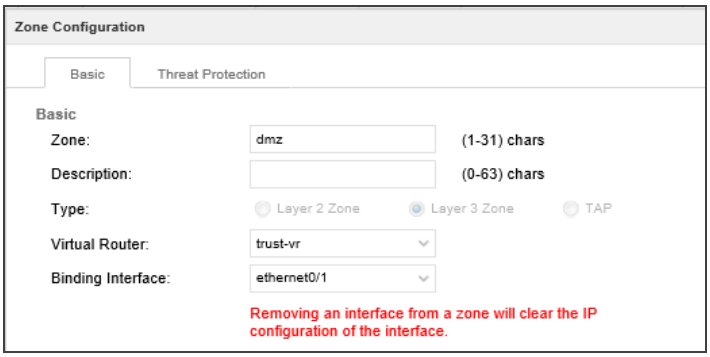
1. Binding internal interface ethernet0/2 to **trust**.

Select **Network>Zone**, select **trust** and click **Edit** to jump to the Zone Configuration dialog.

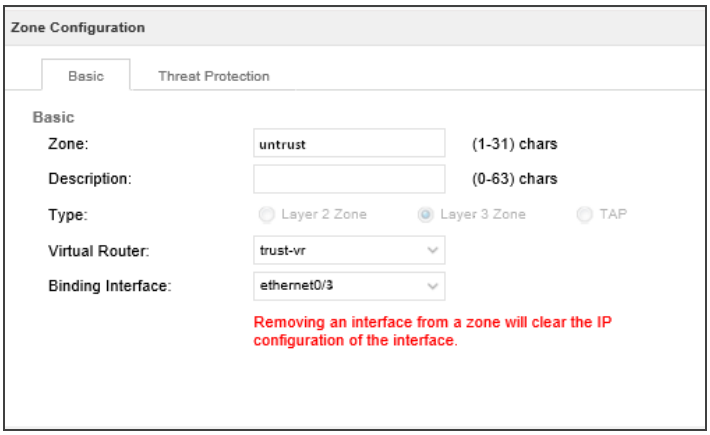
- Binding Interface: ethernet0/2



2. Binding internal interface ethernet0/1 to **dmz**, which can be configured as above.

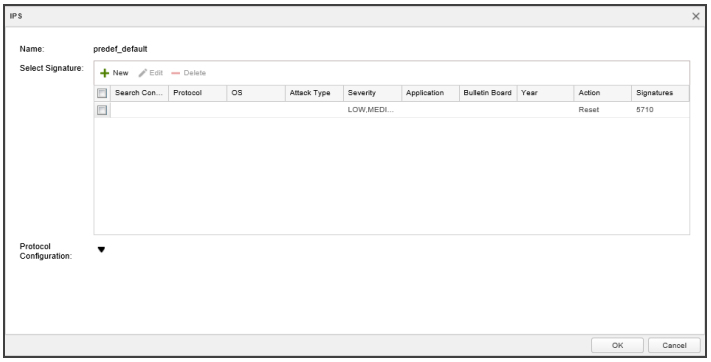


3. Binding external interface ethernet0/3 to **untrust** , which can be configured as above.



Step 4: Creating Intrusion Prevention System rules

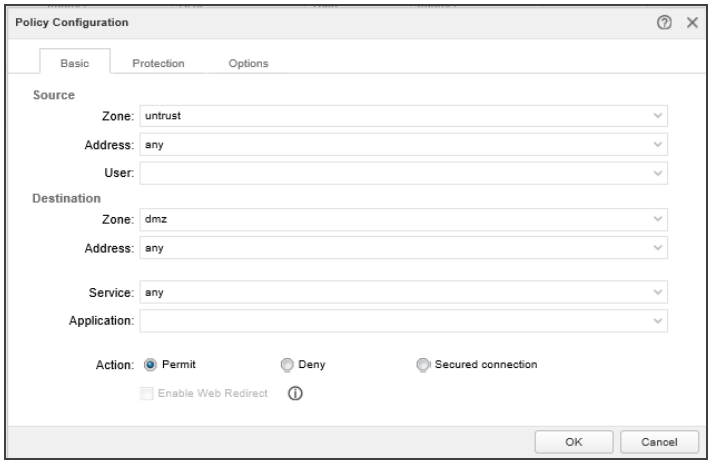
Users can use the default rule or create a new rule. Select **Object>Intrusion Prevention System>Profile**, click **New** to jump to the IPS dialog. This example uses the predef_default rule, which includes all the IPS signatures and the default action is reset.



Step 5: Creating Security Policies.

Security policy: untrust to dmz

By default, the devices will deny all traffic between security zones. This case permits internet and internal hosts to access internal servers. Take the following steps to configure the security policies:



1.Select **Policy> Security Policy**, click **new** to jump to the Policy Configuration Dialog. In the Basic tab:

Source:

- Zone：untrust
- Address：any

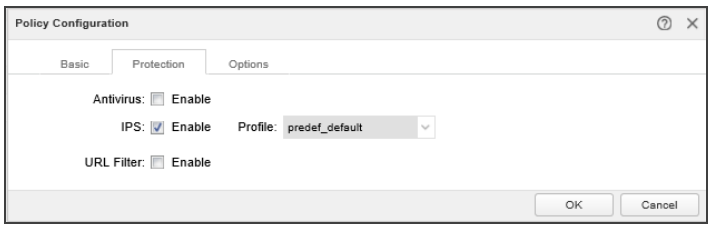
Destination:

- Zone：dmz
- Address：any

Others:

- Service：any
- Action：Permit

2.In the Protection Tab:

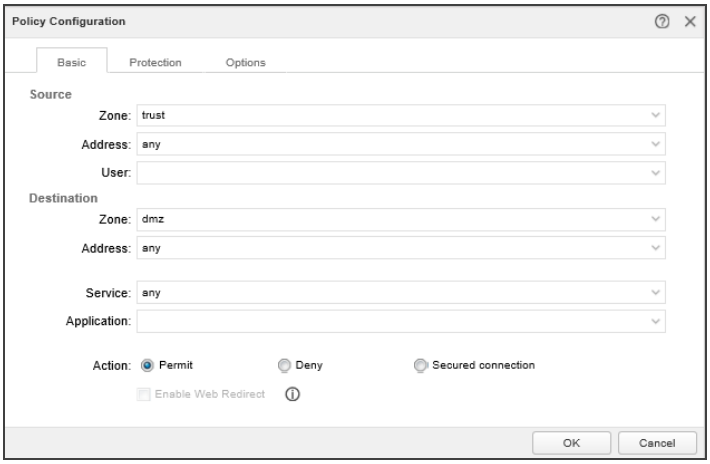


- IPS：Click the **Enable** check box .
- Profile：Select **predef_default** from the drop-down list

Step 5: Creating Security Policies.

Security policy: trust to dmz

1.Select **Policy> Security Policy**, click **new** to jump to the Policy Configuration Dialog. In the Basic tab:



Source:

- Zone：trust
- Address：any

Destination:

- Zone：dmz
- Address：any

Others:

- Service：any
- Action：Permit

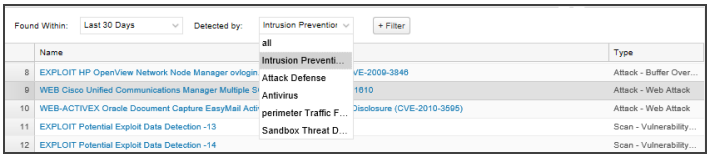
2.In the Protection Tab:



- IPS：Select the **Enable** check box .
- Profile：predef_default

Step 6: Viewing the results

After configuring the above steps, the device can protect Intranet against the known attacks. For example: the attacker creates SQL injections to attack the HTTP Server, and visits the URL of ' http://192.168.4.79/ccmcip/xml directorylist.jsp?n=X'or%20telephonenumber%20like%20''.



The device will display the attack information and block the attack.

Viewing the results from iCenter

1. Select **iCenter>Threat**, click + Filter to add the conditions.

- Detected by: Intrusion Prevention System

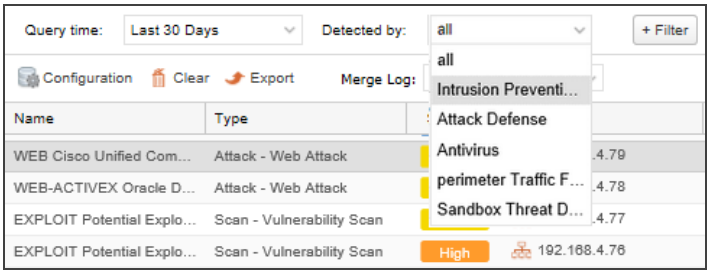
2. The log of Intrusion Prevention System will be displayed. Click the threat name to view the detailed information.



Viewing the results from Threat log

1. Select **Monitor>Log>Threat**, click + Filter to add the conditions.

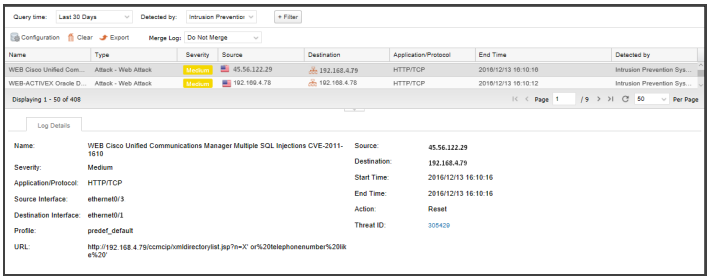
- Detected by: Intrusion Prevention System



Step 6: Viewing the results

2. The log of Intrusion Prevention System will be displayed.

Click the threat name to view the detailed information.



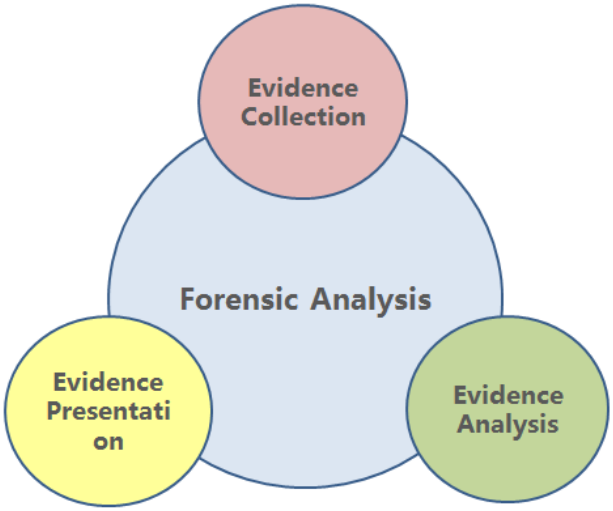
Forensic Analysis

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

This example shows how to in-depth view the threat of the whole network and analyze the threat evidence.

Forensic Analysis provides evidence chain of network threats to collect, multi-perspective analysis and the depth of integration.

- Evidence Collection: Through the configuration of Forensic Analysis function (packet capture), detect the attack generated at the same time evidence collection.
- Evidence Analysis: Analyze the collected evidence.
- Evidence Presentation: Display the threat details, logs, evidence pacp via iCenter, to achieve the threat of visualization.



Configuration Steps

At present, the system only supports the Forensic Analysis function of three threat detection engines (Advanced Threat Detection, Intrusion Prevention System, Anti Virus)

Advanced Threat Detection

Enable the packet capture for Advanced Threat Detection, the system will capture packets when generating logs.

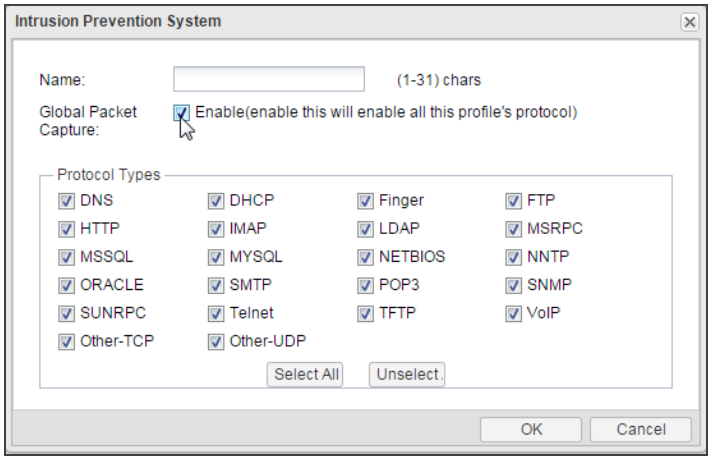
Select **Network > Zone**, Select "**trust**" zone, click **Edit**, and select the <Threat Protection>tab . Select the Capture Packets check box.



Intrusion Prevention System

1. Enable the packet capture for IPS rules, it will enable all this profile's protocols.

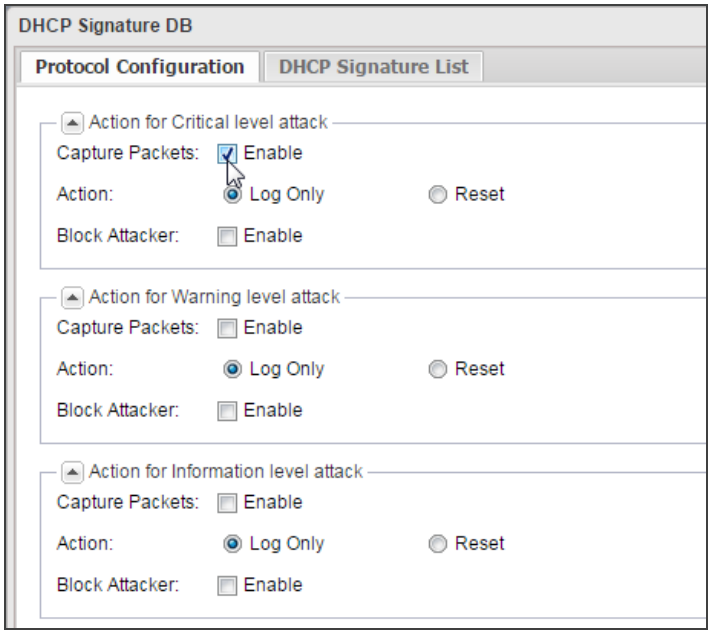
Select **Object>Intrusion Prevention System**, click **New**, and select the **Enable** check box to enable capture packets.



Intrusion Prevention System

2. According to your requirements, configure the capture packets for a specific protocol.

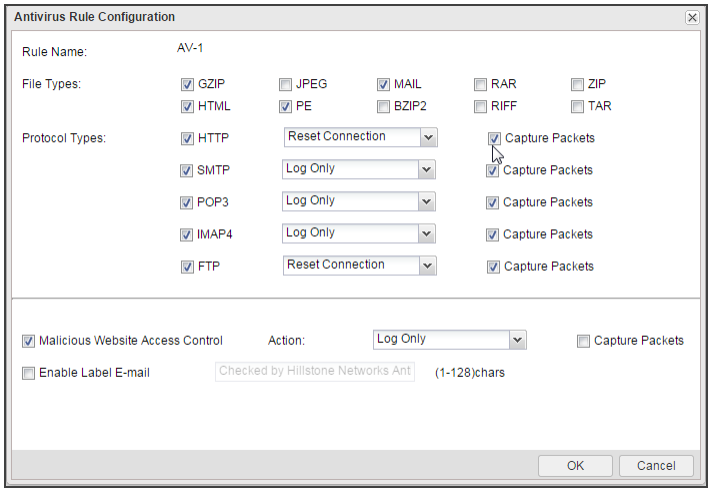
Select **Object>Intrusion Prevention System**, in the IPS rules list, click protocol type, for example 'DHCP', select the **Enable** check box to enable the capture packet for different attack levels.



Anti Virus

Enable the packet capture for Anti Virus rules.

Select **Object > Antivirus**, click **New**, Select the Enable check box before Capture Packet to enable the capture function.



Forensic Analysis Configuration Example

As follows, taking advanced threat detection (ATD) as an example to demonstrate the process of Forensic Analysis

Step 1: Threat Detection

Enabling Advanced Threat Detection and capture packets



Select **Network > Zone**. Select "**trust**" zone, click **Edit**, and select the <Threat Protection> tab.

- Advanced Threat Detection: Select the **Enable** check box .
- Capture Packets: Select the check box , the system will save the evidence messages, and support to download it.

Step 2: Evidence Collection

When ATD attacks occurred, the system will generate a relevant threat log and capture evidence, sent to the system database.

According to the source IP, Advanced threat detection engine capture relational pacp at the same time, it is the HTTP traffic data (including TCP interaction) in 5 minutes or 64K size package, and used to assist in the analysis.

Step 3: Evidence Analysis

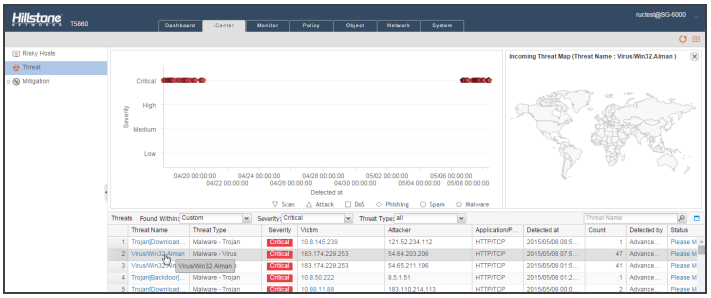
1. Analyze and get the threat detail information .

2. Collect the analysis of evidence.

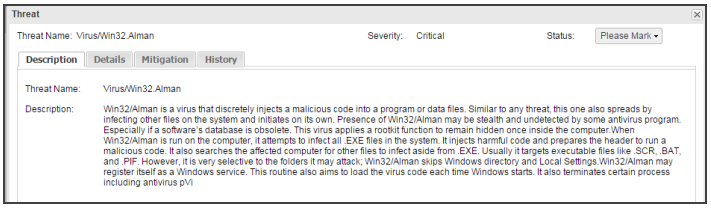
Step 4: Evidence Presentation

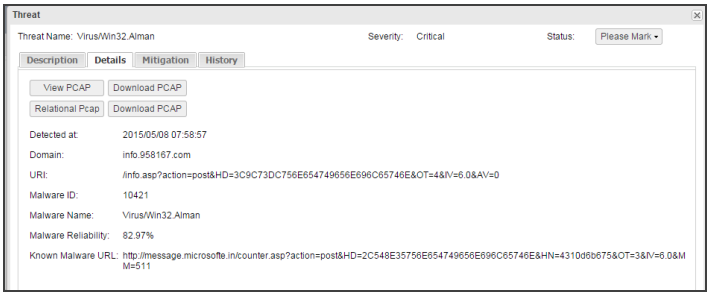
1. **Display the threat information, including the threat name, type, severity, victim host, attack host, etc.**

Click "iCenter", and select Threat tab.



Click the threat name link in the list, to view the threat details.

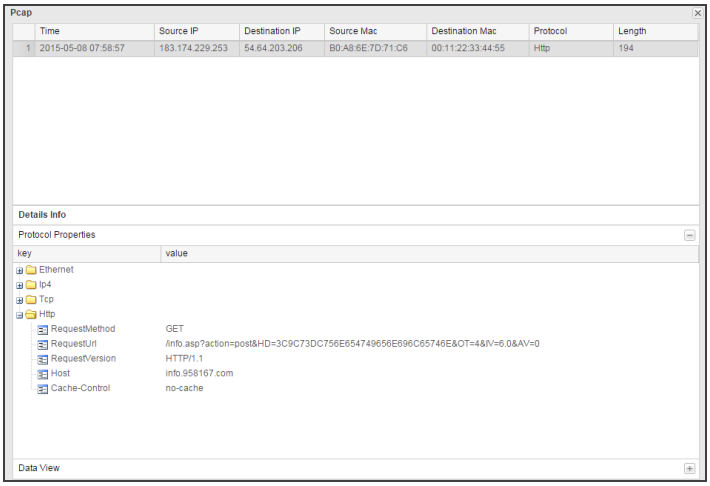


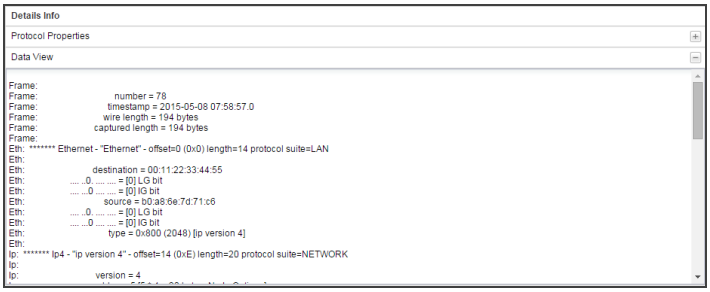


Step 4: Evidence Presentation

2. **Viewing the evidence details.**

Select the select the <Details>tab, and click **View PACP**.

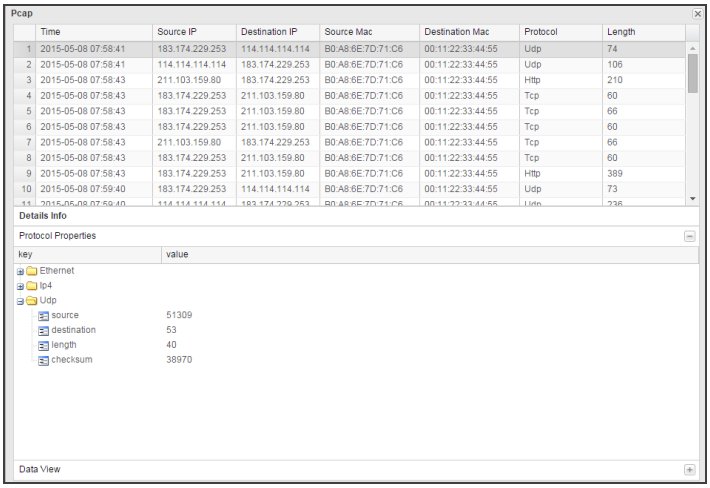


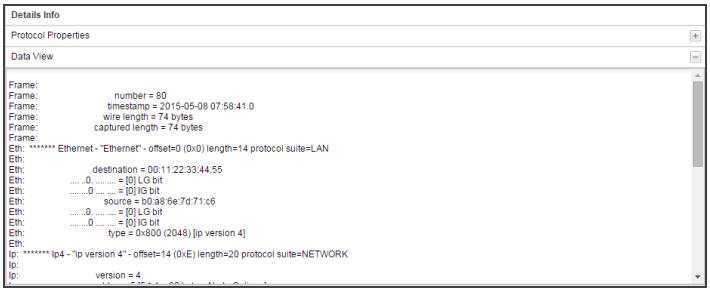


Step 4: Evidence Presentation

3. **Viewing the relational pacp details.**

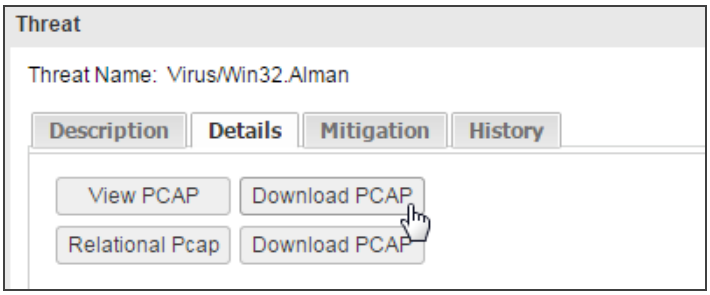
Select the select the <Details>tab, and click **Relational Pacp**.





4. **Downloading evidence.**

Select the select the <Details>tab, and click **Download Pacp**, the evidence will be downloaded to local.



Threat Intelligence Via Hillstone Cloud Service Platform

Hillstone Cloud Service Platform is a cloud security services platform, which provides 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.

- 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. For more information about CloudView, refer to the CloudView FAQs.
- Cloud Sandbox: It is a technology adopted by the Sandbox function. After a suspicious file being uploaded to the Hillstone cloud service platform, the cloud sandbox will collect behaviors of the file, analyze the collected data, verify the legality of the file, send the analysis result to system and deal with the malicious file according to the actions set by system.
- CloudVista (Threat Intelligence Center): Threat Intelligence function can upload some elements in the logs generated by each module to the cloud service platform, such as IP address, domain, etc. The cloud service platform will check whether the elements have threat intelligence through the threat center. You can view threat intelligence information related to elements through the threat intelligence center.

This example shows how to Obtain threat intelligence services through the Hillstone Cloud Service Platform.

The topology is shown as below. Device connects to theHillstone Cloud Service Platform, upload some elements in the logs generated by each module to the cloud service platform and obtain the threat intelligence .



Preparation

Before configuring the NETCONF function, prepare the following first:

1. Install the threat intelligence license.
2. Register a Cloud Service account. Enter the address "https://user.hillstonenet.com/login" in the web browser of the PC to register.

Configuration Steps

Step 1: Connect to the Hillstone Cloud Service Platform

Select **System > Connecting to Hillstone Cloud Service Platform**.

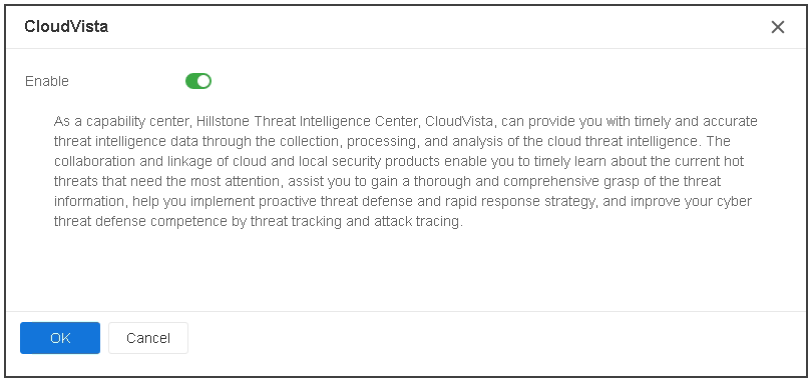


- Address: cloud.hillstonenet.com.cn
- Virtual Router: trust-vr
- User: hillstone
- Password: password@123

> **Note:** When using the default password to connect to the cloud platform, you can also get the corresponding cloud service, but you cannot view the data uploaded by the device from the cloud platform.

Step 2: Enable CloudVista Service

Select **System > Connecting to Hillstone Cloud Service Platform**, click the **CloudVista** button. In the CloudVista page, click the **Enable** button to enable the CloudVista service.



Viewing the results

After configuring the above steps, You can view the entries with threat intelligence on the ICenter page. In the threat list, hover your cursor over a object, and there is a button to its right. The ⋮ button appears on the right. Click this button and select **View threat intelligence**.

Identifying IoT Assets to Enable Security Control of IoT by Using Built-in Docker

This example describes how to use the built-in method of local asset identification to identify IoT device assets via WebUI and CLI. That is, this example uses built-in Docker of the firewall to deploy the asset identification system on the device to implement asset identification and security control.

> **Note:** The built-in method of local asset identification used in this example supports only A-series firewalls. We recommend that you use A2600 and higher models.

Networking Requirements

As shown in the following figure, a firewall (NGFW: 10.182.191.36) is deployed at the internal network border of the enterprise. The address of Docker within the firewall is set to 172.25.0.1/24. In addition, the security operation platform (Hillstone iSource 10.182.79.27) is deployed.

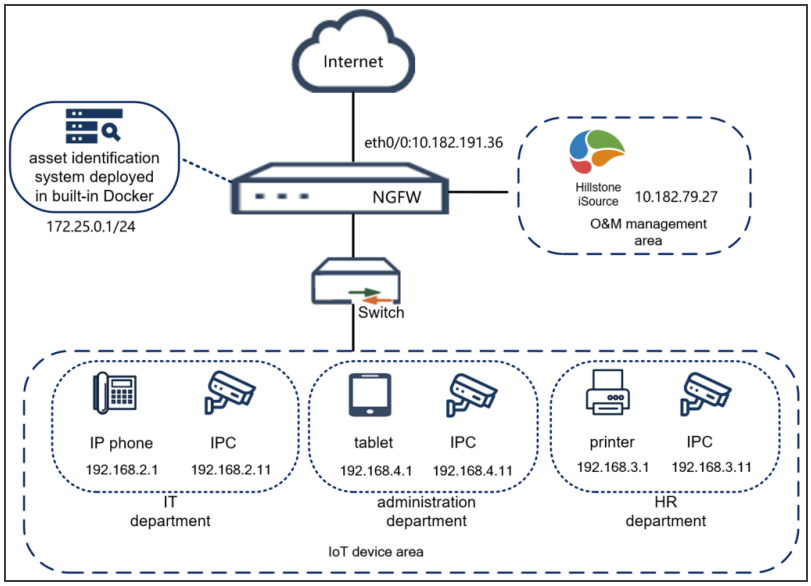
The internal IoT of the enterprise contains various types of IoT devices, categorized based on areas as follows:

- IT department (192.168.2.0/24) - IP phone and IPC;
- HR department (192.168.3.0/24) - printer and IPC;
- Administration department (192.168.4.0/24) - tablet and IPC.

To identify detailed information about IoT asset devices by using the built-in method of local asset identification, and to meet the following requirements with the IoT security monitor function of the firewall together:

- Identify&monitor IoT device: Perform asset identification and monitor management on IoT devices in the deployment environment.
- Manage IoT device traffic: Manage the network permissions of identified tablets. Specifically, disable their network traffic by using policy rules.

- Analyze IoT data: Combined with iSource and cloud platform in the deployment environment, upload IoT data to iSource for unified analysis statistics, control, and asset management.



*This example is configured and verified by using 5.5R10F4 in a test environment. Please configure the IP address for each interface based on the actual condition.

Preparations

Before you start, make sure that the following prerequisites are met:

- DHCP traffic from IoT devices in the network passes through the firewall or is mirrored to the firewall.
- The system version of the firewall supports the IoT monitor function. You can run the `show version` command to view the system version. Please use StoneOS 5.5R10F4 or later F version.
- The IoT license is installed on the firewall device and you have logged in to the device again.
- The image file of local asset identification system is obtained.
- iSource is deployed.

Configuration Steps

IoT asset identification

1. Create a Docker and allocate system resources.
2. Import the image file of local asset identification system.
3. Configure the CIDR block of the Docker network.
4. Run the container.
5. Enable and configure the local asset identification function.
6. Configure the identification list by specifying the address list of IoT devices.
7. Configure the terminal type——enable/disable the function of automatically synchronizing terminals to repository.
8. Configure the zone to enable IoT Monitor function and bind an identification list.

IoT monitor management

1. Configure the region based on the IoT device CIDR block of the IT department, administration department, and HR department.
2. View IoT monitor, including the manufacturer, type, online device, and various detailed statistics of all identified IoT devices.

IoT policy control

1. Configure the device object——specify the category dimension for IoT devices to map identified IoT devices to device objects.
2. Configure the policy rule——configure the policy rule based on device object.

IoT data analysis

- Upload IoT data to iSource——After you upload IoT data to iSource, iSource can implement further threat event response and handling such as asset management and blocking/policy deployment.

Configuration Steps of WebUI

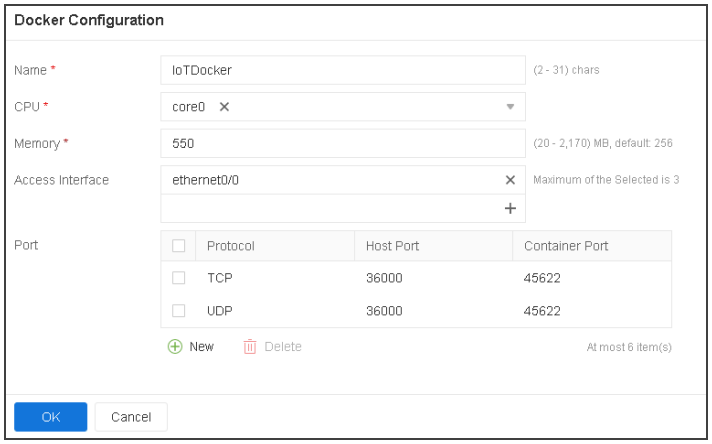
IoT Asset Identification Configuration

Step 1: Create a Docker and allocate system resources

Select **System** > **Docker Management**. On the **Docker Management** page, click **New** and configure the following parameters:

- Name: IoTDocker
- CPU: Select the CPU core to which Docker is bound. You can select the default Core0. (To use other CPU cores, in global configuration mode, use the `flow-core-num number` command to free other CPU cores)
- Memory: 550
- Access Interface: Select ethernet0/0 (the name of the interface that accesses Docker)
- Port: Click **New** and configure the port mapping of Docker communication.
  - Protocol-TCP, Host Port-36000, Container Port-45622
  - Protocol-UDP, Host Port-36000, Container Port-45622

Click **OK**.



Step 2: Import the image file of local asset identification system

1. Select **System** > **Docker Management**.
2. Click ⋮ in the **Operation** column and select **Import image file**.
3. In the **Import** panel, click **Browse** and select the obtained image file of local asset identification system: "local-iot-identify-docker-1.0.231206.gz".
4. Click **OK**.



Step 3: Configure the CIDR block of the Docker network

Select **System** > **Docker Management** > **Configuration** and configure the following parameter:

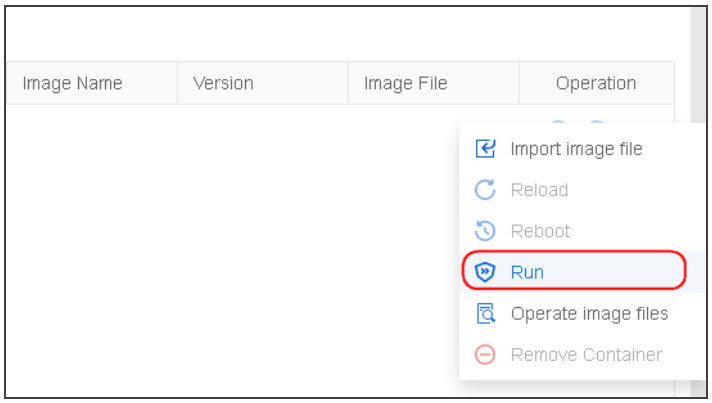
- IP/Netmask: 172.25.0.1/24. (This IP address is used for internal and external Docker communication. You can configure any IP address, which cannot conflict with other interfaces.)



Step 4: Run the container

Select **System** > **Docker Management** and perform the following operations:

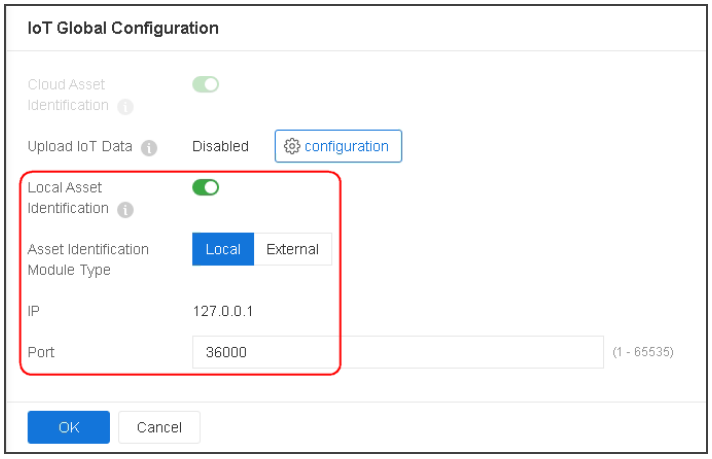
1. Click ⋮ in the **Operation** column and select **Run**.
2. Select the imported image file, load the image file, and then run the container.



Step 5: Enable and configure the local asset identification function

Select **Object** > **IoT Policy** > **Configuration**.

- Local Asset Identification: Click Enable.
- Asset Identification Module Type: Local
- IP: 127.0.0.1 (does not require configuration or modification)
- Port: 36000 (needs to be consistent with the host port number configured in Step 1)

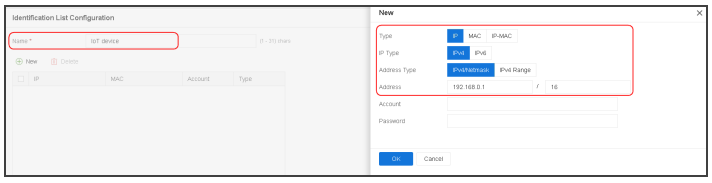


Click **OK**.

Step 6: Configure the identification list

Select **Object** > **IoT Policy** > **Identification List**. On the **Identification List** page, click **New**.

- Name: IoT device
- Click **New** and configure the following options:
  - Type: IP
  - IP Type: IPv4
  - Address Type: IPv4/Netmask
  - Address: 192.168.0.1/16 (the address range of IoT devices within the enterprise)



Click **OK**.

Step 7: Configure the terminal type. For example, automatically add the identified IPC to repository

Select **Object** > **IoT Policy** > **Terminal Type**. Then, turn on the switch in the **Add to Repository Automatically** column corresponding to IPC in the list.

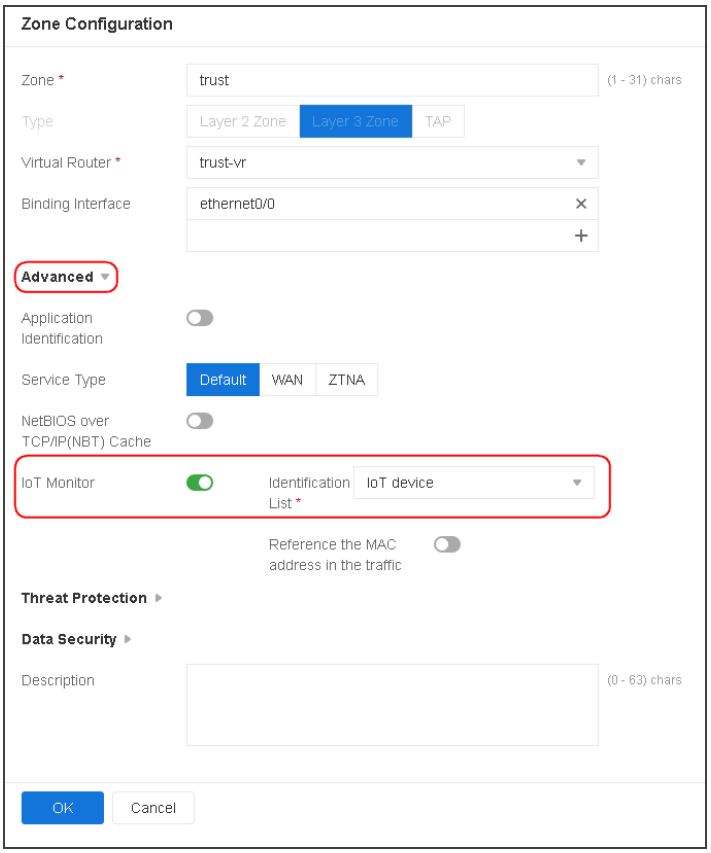


Step 8: Configure a zone to enable the IoT Monitor function of the zone. Select the zone used by IoT device traffic passing through the firewall based on the actual networking environment (In this example, the layer-3 zone "trust" is used)

Select **Network** > **Zone**. In the list, select "trust" and click **Edit**.

- Advanced: Click **Advanced** to expand this section.
- IoT Monitor: Click Enable.
- Identification List: Select the identification list "IoT device" that is created in Step 6.

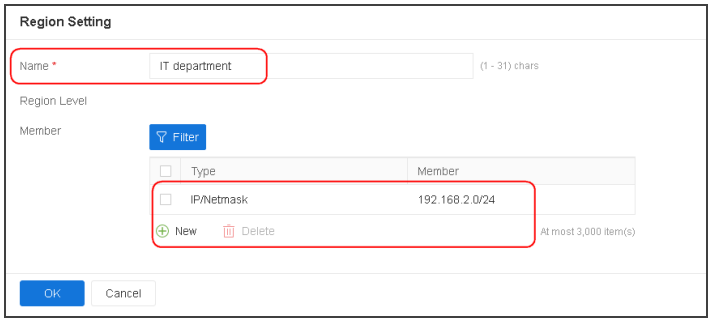
Click **OK**.



IoT Monitor Management

Step 1: Configure the Region

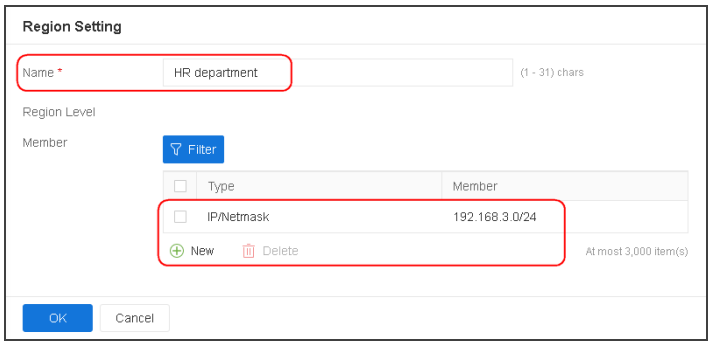
Select **Object** > **IoT Policy** > **Region Setting**. On the **Region Setting** page, click **New** and configure the following parameters:



- Name: IT department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.2.0/24

Click **OK**.

Repeat the steps above to create the region "HR department":

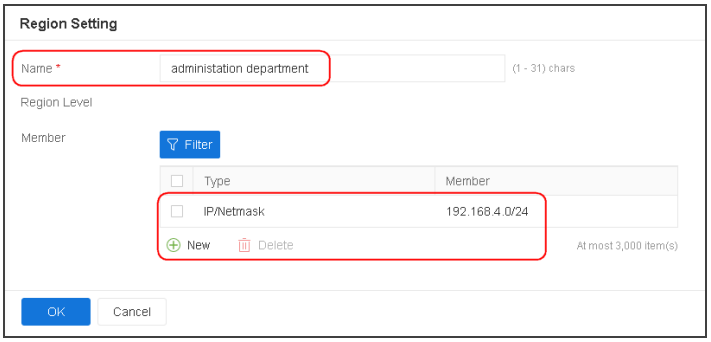


- Name: HR department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.3.0/24

Click **OK**.

Step 1: Configure the Region

Repeat the steps above to create the region "administration department":

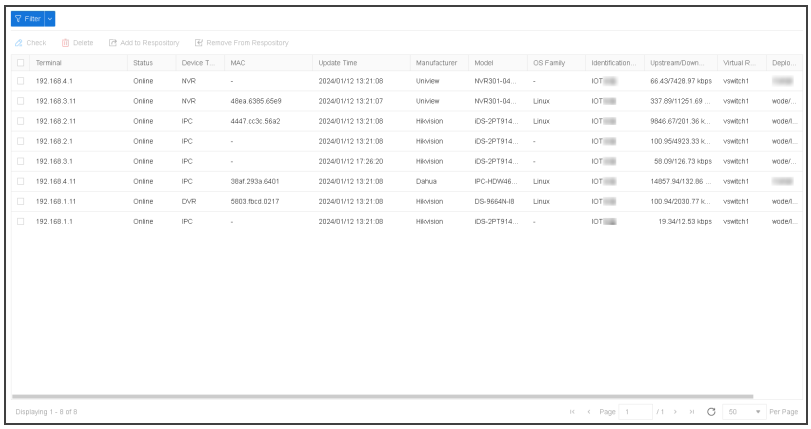


- Name: administration department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.4.0/24

Click **OK**.

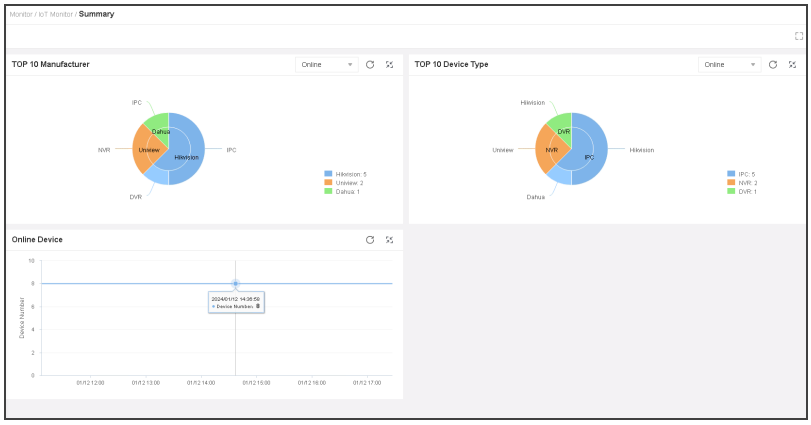
Step 2: View IoT monitor

Select **Monitor** > **IoT Monitor** > **Details** to view details about all identified IoT devices in the deployment environment.



Step 2: View IoT monitor

Select **Monitor** > **IoT Monitor** > **Summary** to view the top 10 device manufacturers and device type distribution.



IoT Policy Control

Step 1: Configure a device object

Select **Object** > **Device**. On the **Device** page, click **New**.

On the **Device Config** page, configure the following parameters:

- Device Name: tablet
- Type: Select Tablet
- You can configure other options as required



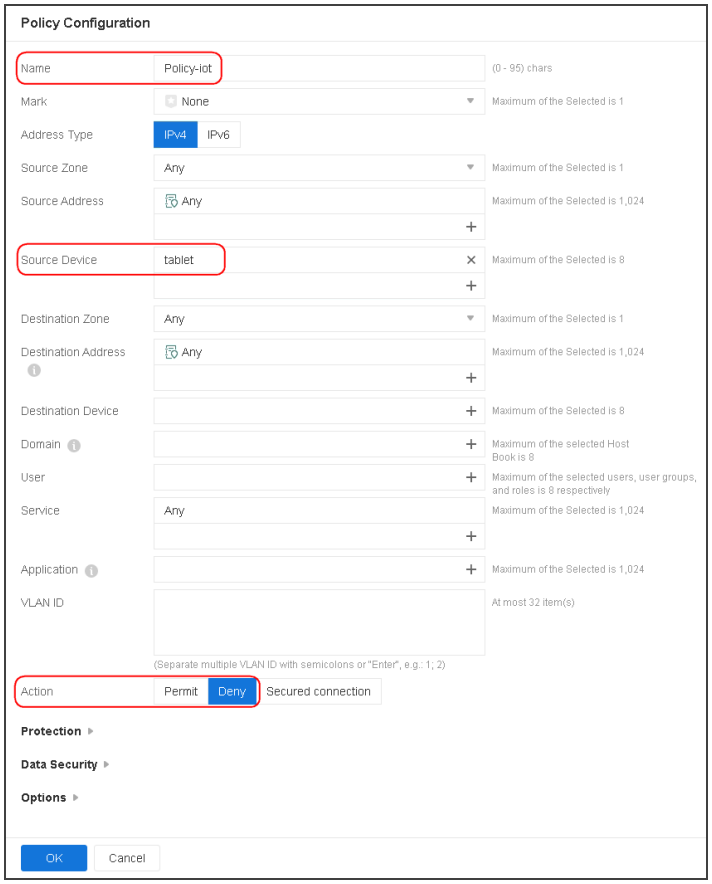
Click **OK**.

Step 2: Configure the policy rule to manage permissions on Internet access for tablets

Select **Policy** > **Security Policy** > **Policy**. On the **Policy Configuration** page, configure the following parameters:

- Name: Policy-iot
- Source Device: Select the "tablet" device object created in Step 1
- Action: Select Deny
- You can configure other options as required or default

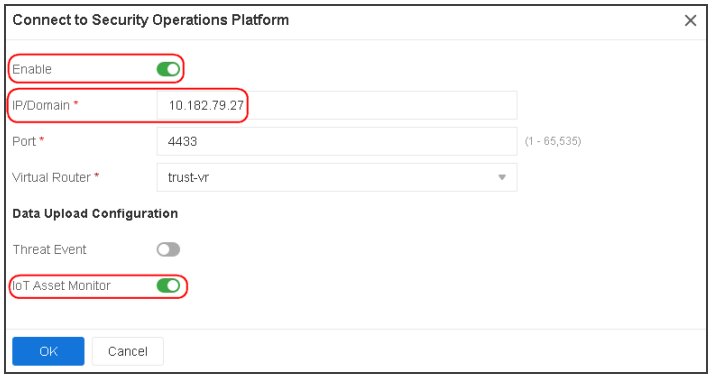
Click **OK**.



IoT Data Analysis

Connect to iSource and enable the IoT Asset Monitor function

Select **System** > **Extended Services**. In the **Connect to Security Operations Platform** section, click in the lower-left corner. In the **Connect to Security Operations Platform** panel, configure the following parameters:



- Enable: Click Enable
- IP/Domain: 10.182.79.27 (the iSource address in the networking environment)
- IoT Asset Monitor: Click Enable
- Keep the default values for other options

Click **OK**.

Configuration Steps of CLI

IoT Asset Identification Configuration

Step 1: Create a Docker and allocate system resources

```
hostname(config)# docker IoTDocker
hostname(config-docker)#  cpu 0
hostname(config-docker)# memory 512
hostname(config-docker)# port-map tcp host-port 36000 docker-port 45622
hostname(config-docker)# port-map udp host-port 36000 docker-port 45622
hostname(config-docker)# access-interface ethernet0/0
```

Step 2: Import the image file of local asset identification system

hostname# **import docker-image-file IoTDocker from ftp server 10.200.6.10 user testuser password 123456 local-iot-identify-docker-1.0.231206.gz**

Step 3: Configure the CIDR block of the Docker network

hostname (config)# **docker-config network 172.25.0.1/24** (This IP address is used for internal and external Docker communication. You can configure any IP address, which cannot conflict with other interfaces.)

Step 4: Run the container

hostname#**exec docker IoTDocker run local-iot-identify-docker-1.0.231206.gz**

Step 5: Enable and configure the local asset identification function

hostname# (config)# **iot-monitor docker-detect enable**

hostname# (config)# **iot-monitor docker-detect local-docker port 36000** (The port number needs to be consistent with the host port number configured in Step 1)

Step 6: Configure the identification list

hostname(config)# **iot-monitor identify-list iotdevice**

hostname(config-IoT-monitor-identify-list)# **ip network 192.168.0.1/16** (the address range of IoT devices within the enterprise)

hostname(config-IoT-monitor-identify-list)# **exit**

Step 7: Configure a zone to enable the IoT Monitor function of the zone. Select the zone used by IoT device traffic passing through the firewall based on the actual networking environment (In this example, the layer-3 zone "trust" is used)

hostname(config)#**zone trust**

hostname(config-zone-trust)# **iot-monitor enable iotdevice**

hostname(config-zone-trust)# **exit**

IoT Monitor Management

Step 1: Configure the Region

```
hostname(config)# iot-monitor district id 1 name IT (Configure the region of IT department)
hostname(config-IoT-monitor-district)# ip network 192.168.2.0/24
hostname(config)# iot-monitor district id 1 name HR (Configure the region of HR department)
hostname(config-IoT-monitor-district)# ip network 192.168.3.0/24
hostname(config)# iot-monitor district id 1 name admin (Configure the region of administration depart-
ment)
hostname(config-IoT-monitor-district)# ip network 192.168.4.0/24
```

Step 2: View IoT monitor

```
hostname(config)# show iot-monitor-list
Total: 5
ip vrouter/vswitch type manufacturer status OS_family Rx(kbps)/Tx(kbps) profile
192.168.4.1 trust-vr Ipad Huawei Online -65.57/7517.99 iotdevice
192.168.3.11 trust-vr IPC Hikvision Online -16600.00/11507.00 iotdevice
192.168.2.11 trust-vr IPC Hikvision Online -9464.91/192.992 iotdevice
192.168.2.1 trust-vr Voip Phone - Online -96.53/4729.00 iotdevice
192.168.3.1 trust-vr Printer HP Online- 166.49/7565.09 iotdevice
```

IoT Policy Control

Step 1: Configure a device object

```
hostname(config)# device pad
hostname(config-device)# type Ipad
hostname(config-device)# exit
```

Step 2: Configure the policy rule to manage permissions on Internet access for tablets

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-device pad
hostname(config-policy-rule)# action deny
hostname(config-policy-rule)# exit
hostname(config)#
```

IoT Data Analysis

Connect to iSource and enable the IoT Asset Monitor function

```
hostname(config)# cloud server isource
hostname(config-isource)# enable
hostname(config-isource)# address 10.182.79.27 (the iSource address in the networking environment)
hostname(config-isource)# upload-type iot-monitor-property
hostname(config-isource)# exit
```

Identifying IoT Assets to Enable Security Control by Deploying the Asset Identifying System on the VM

This example describes how to use the external method of local asset identification to identify IoT device assets via WebUI and CLI. That is, this example uses the asset identification system deployed on the VM to identify IoT device asset information by installing an asset identification program on the VM. This implements asset identification and security control.

Networking Requirements

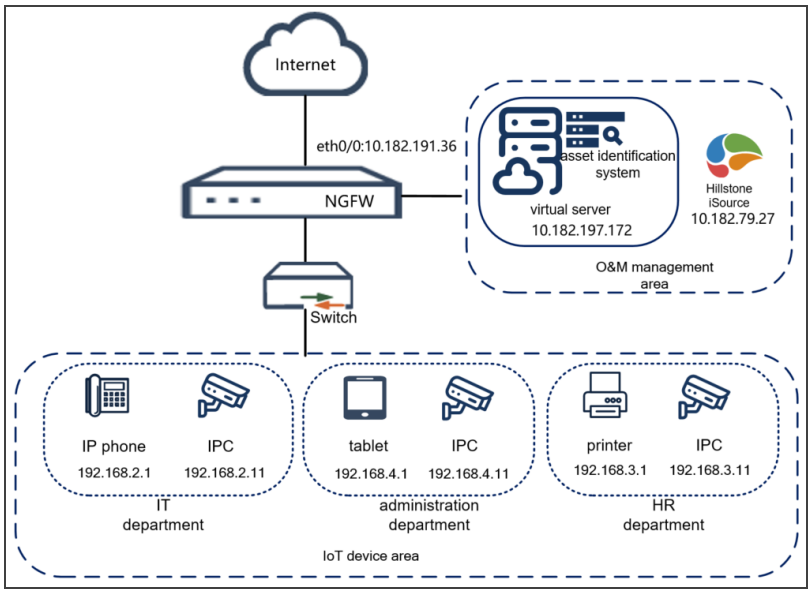
As shown in the following figure, a firewall (NGFW： 10.182.191.36) is deployed at the internal network border of the enterprise, and the asset identification system is deployed on the VMware ESXi server (10.182.197.172). In addition, the security operation platform (Hillstone iSource 10.182.79.27) is deployed.

The internal IoT of the enterprise contains various types of IoT devices, categorized based on areas as follows:

- IT department (192.168.2.0/24) - IP phone and IPC;
- HR department (192.168.3.0/24) - printer and IPC;
- Administration department (192.168.4.0/24) - tablet and IPC.

To identify detailed information about IoT device assets by using the asset identification system deployed on the VM, and to meet the following requirements with the IoT monitor function of the firewall together:

- Identify&monitor IoT device: Perform asset identification and monitor management on IoT devices in the deployment environment.
- Manage IoT device traffic: Manage the network permissions of identified tablets. Specifically, disable their network traffic by using policy rules.
- Analyze IoT data: Combined with iSource and cloud platform in the deployment environment, upload IoT data to iSource and cloud platform for unified analysis statistics, control, and asset management.



*This example is configured and verified by using 5.5R10F4 in a test environment. Please configure the IP address for each interface based on the actual condition.

Preparations

Before you start, make sure that the following prerequisites are met:

Networking environment:

- DHCP traffic from IoT devices in the network passes through the firewall or is mirrored to the firewall.
- iSource is deployed.

Firewall device:

- The system version of the firewall supports the IoT monitor function. You can run the `show version` command to view the system version. Please use StoneOS 5.5R10F4 or later F version.
- The IoT license is installed on the firewall device and you have logged in to the device again.

VMware ESXi server deployment:

- The VM environment is deployed based on system requirements: the version of VMware ESXi is 7.0 and later; the VM has at least 4 vCPUs, 4 GB of memory, and 20 GB of disk space and is installed with a NIC.
- The ESXi Server host is configured.

- The installation file in ZIP format (including ovf, vmdk, iso, and mf files) is obtained from Hillstone Networks technical support. After the package is decompressed, save ovf and vmdk files to your PC.

Configuration Steps

IoT asset identification

- **VM configuration**:
  1. Deploy the asset identification system on the VMware ESXi server.
- **Firewall configuration**:
  1. Enable and configure the local asset identification function.
  2. Configure the identification list by specifying the address list of IoT devices.
  3. Configure the terminal type——enable/disable the function of automatically synchronizing terminals to repository.
  4. Configure the zone to enable IoT Monitor function and bind an identification list.

IoT monitor management

1. Configure the region based on the IoT device CIDR block of the IT department, administration department, and HR department.
2. View IoT monitor, including the manufacturer, type, online device, and various detailed statistics of all identified IoT devices.

IoT policy control

1. Configure the device object——specify the category dimension for IoT devices to map identified IoT devices to device objects.
2. Configure the policy rule——configure the policy rule based on device object.

IoT data analysis

- Upload IoT data to iSource——After you upload IoT data to iSource, iSource can implement further threat event response and handling such as asset management and blocking/policy deployment.

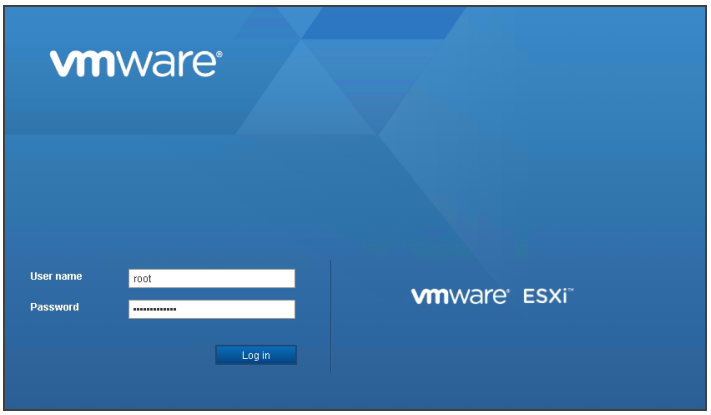
Configuration Steps of WebUI

IoT Asset Identification Configuration

VM Configuration

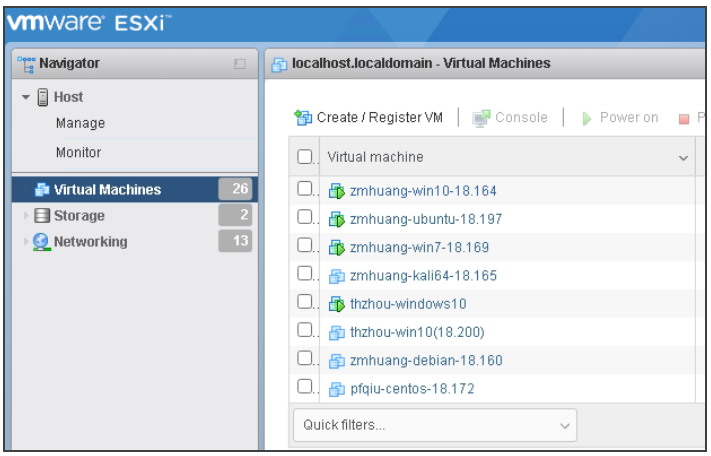
Step 1: Log in to the VMware ESXi platform

To access the VMware ESXi 7.0 platform, enter the user-name and password and click **Log in**.



Step 2: Create a VM

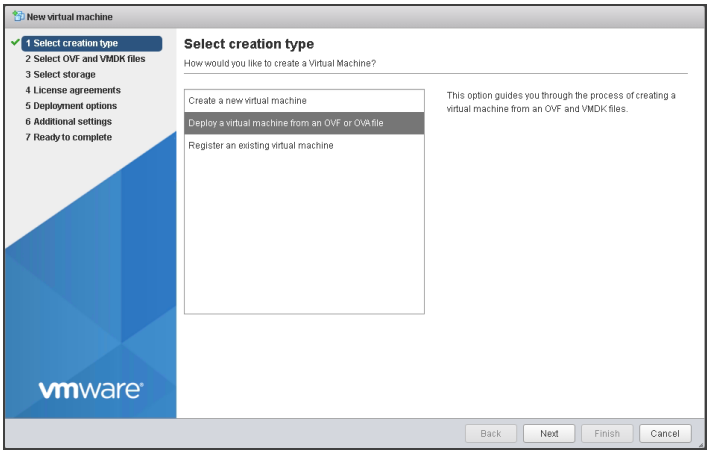
1. After you log in to the VMware ESXi 7.0 platform, click **Virtual Machines** in the left-side pane. On the page that appears, click **Create / Register VM**.



Step 2: Create a VM

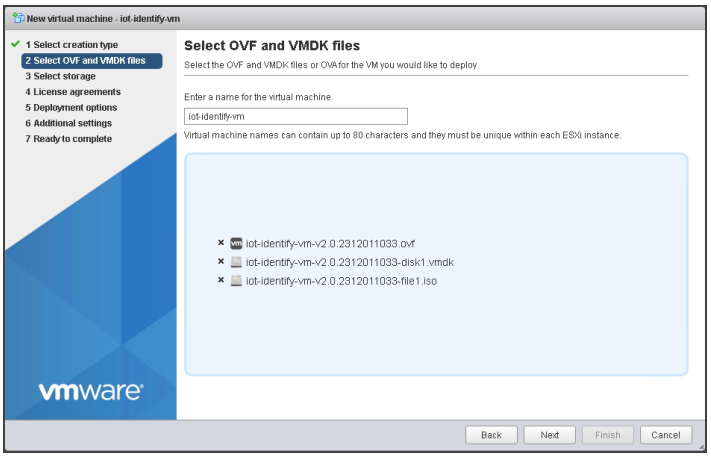
2. Select an existing VM type.
    - Select Deploy a virtual machine from an OVF or OVA file

    Click **Next**.



3. Select OVF and VMDK files for the VM to be deployed.
    - VM name: iot-identify-vm
    - Select the ovf, vmdk, and iso files from your PC or drag the files to the specified position.

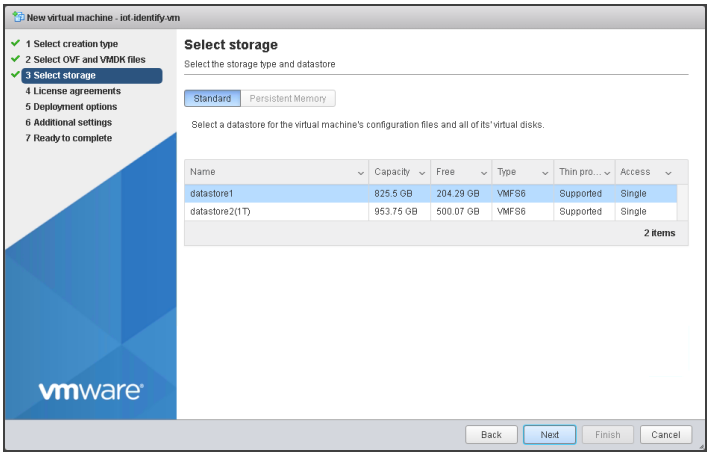
    Click **Next**.



4. Select storage.
    - Select the storage type and a datastore for the VM's configuration files and all of its' virtual disks.

    Click **Next**.

    Note: The hard disk needs to be larger than 20 GB in size.

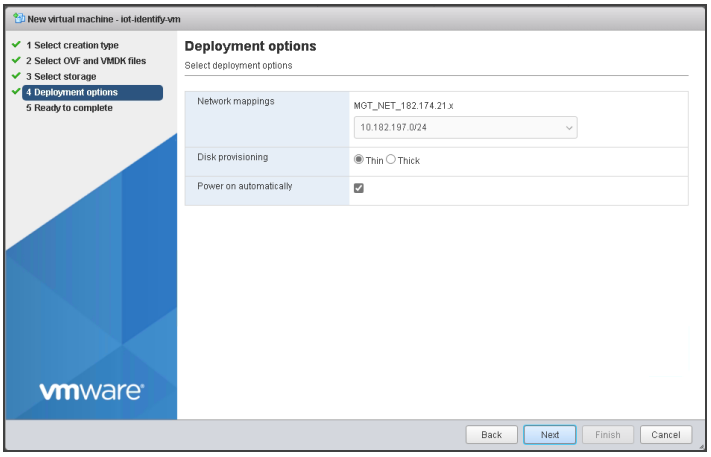


Step 2: Create a VM

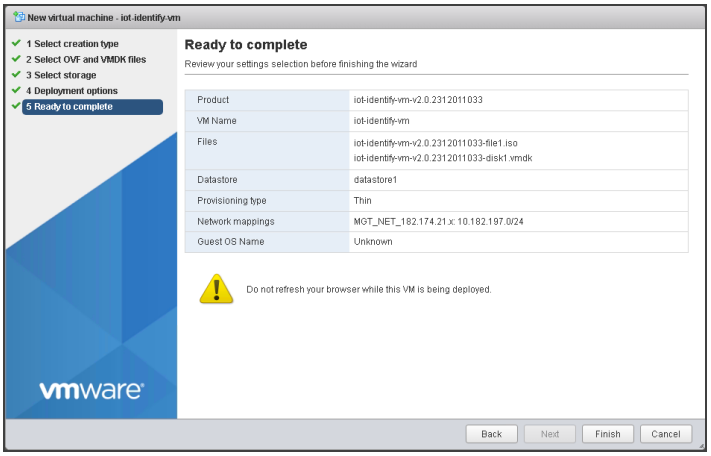
5. Configure deployment options.

   - Select network mappings based on the network environment
   - Disk provisioning: select Thin
   - Select Power on automatically

   Click **Next**.



6. After you check the configurations, click **Finish**.



After the system files are uploaded to the disk, the virtual machine is created.

> **Note:** The deployment process may take a long time. Do not refresh the page before the deployment is completed.

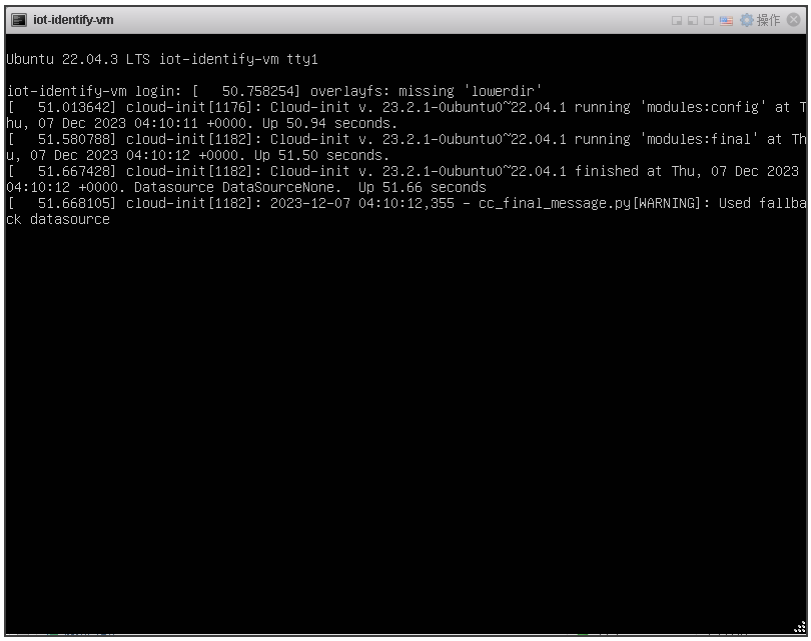
Step 3: Log in to the VM

1. After the VM is created, it will automatically power on and start.

Step 3: Log in to the VM

2. In the left-side Navigator, click **Virtual Machines**. On the page that appears, select the VM iot-identify-vm created in the steps above.

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 log in to the VM.

Step 4: Configure the NIC

After the VM is deployed, you need to modify the NIC configuration by specifying the configuration file within /etc/netplan based on the current environment.

1. In the console, enter the `cat /etc/netplan/00-installer-config.yaml` command to view information about the current configuration file.

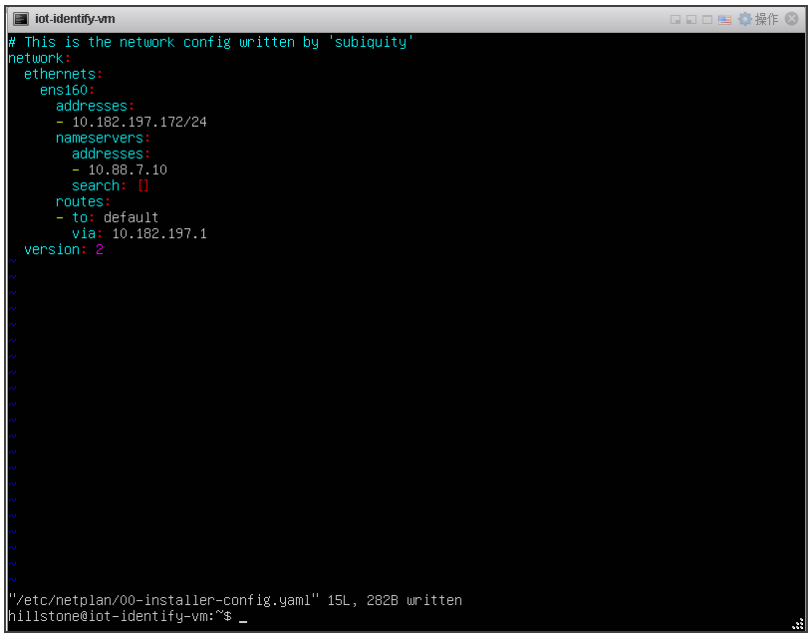
2. Enter the `vi /etc/netplan/00-installer-config.yaml` command to open the configuration file.

Step 4: Configure the NIC

3. Move the pointer over the position where you want to modify the configuration and press `i` to enter the edit mode. You can modify the address to 10.182.197.172.

   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, and this IP address is used as the IP address of the VM of IoT local asset identification.

4. After you modify the address, press ESC and then `:wq` to exit the configuration file and save the configuration information.



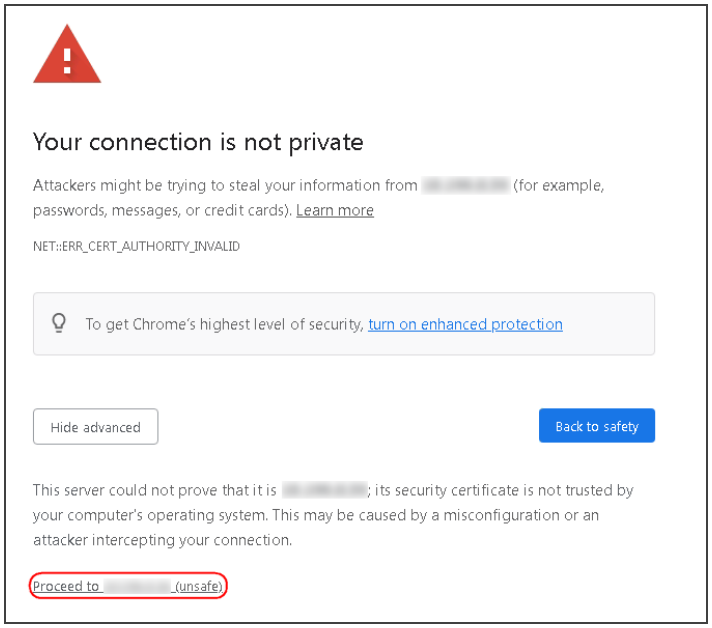
5. Restart the VM to ensure that the modified NIC information is applied.

Step 5: Install the asset identification program

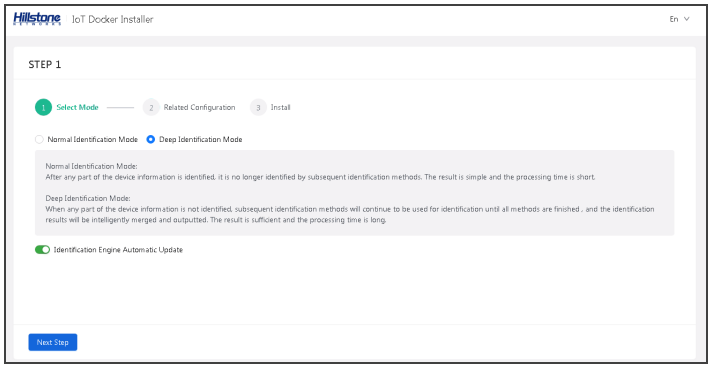
1. Open the browser and access the IP address configured in the steps above, such as https://10.182.197.172:22654.

Step 5: Install the asset identification program

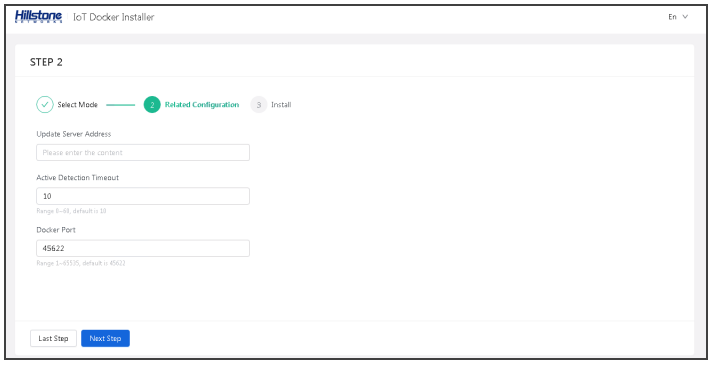
2. With a self-signed certificate, your browser will warn you that "Your connection is private". Click **Advanced** > **Proceed to XXX**.



3. Enter the asset identification program installation wizard, select **Deep Identification Mode**, and then click **Next Step**.

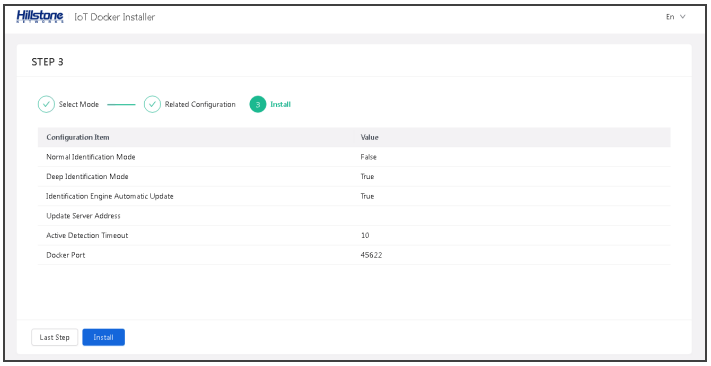


4. In the Related Configuration step, use the default values. That is, use Update Server provided by Hillstone Networks.



Step 5: Install the asset identification program

5. Confirm the configurations and click **Install**.



6. After the installation is completed, the asset identification program will automatically start.

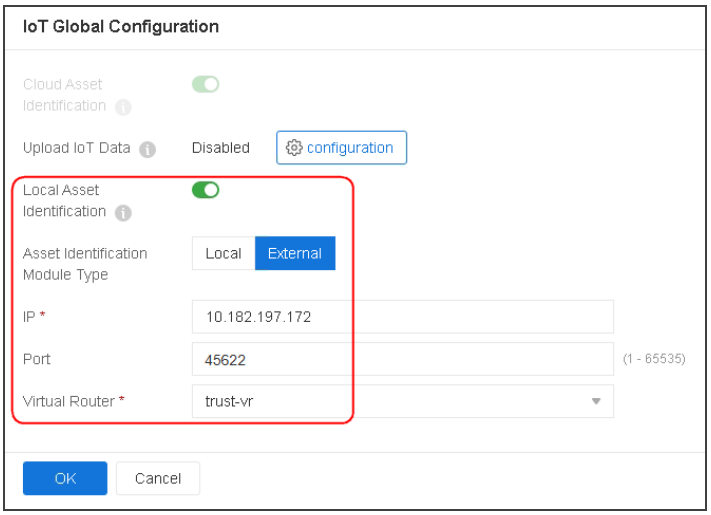
Firewall Configuration

Step 1: Enable and configure the local asset identification function

Log in to the firewall and select **Object** > **IoT Policy** > **Configuration**.

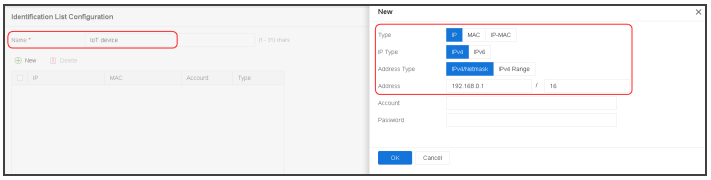
- Local Asset Identification: Click Enable.
- Asset Identification Module Type: External
- IP: 10.182.197.172 (the deployed VM address)
- Port: 45622 (The default port number is used in this example. If customization is required, this option must be consistent with the "Docker Port" configured in step 5 "Related Configuration " of the virtual machine configuration)
- Virtual Router: trust-vr

Click **OK**.



Step 2: Configure the identification list

Select **Object** > **IoT Policy** > **Identification List**. On the **Identification List** page, click **New**.



- Name: IoT device
- Click New and configure the following options:
  - Type: IP
  - IP Type: IPv4
  - Address Type: IPv4/Netmask
  - Address: 192.168.0.1/16 (the address range of IoT devices within the enterprise)

Click **OK**.

Step 3: Configure the terminal type. For example, automatically add the identified IPC to repository

Select **Object** > **IoT Policy** > **Terminal Type**. Then, turn on the switch in the **Add to Repository Automatically** column corresponding to IPC in the list.

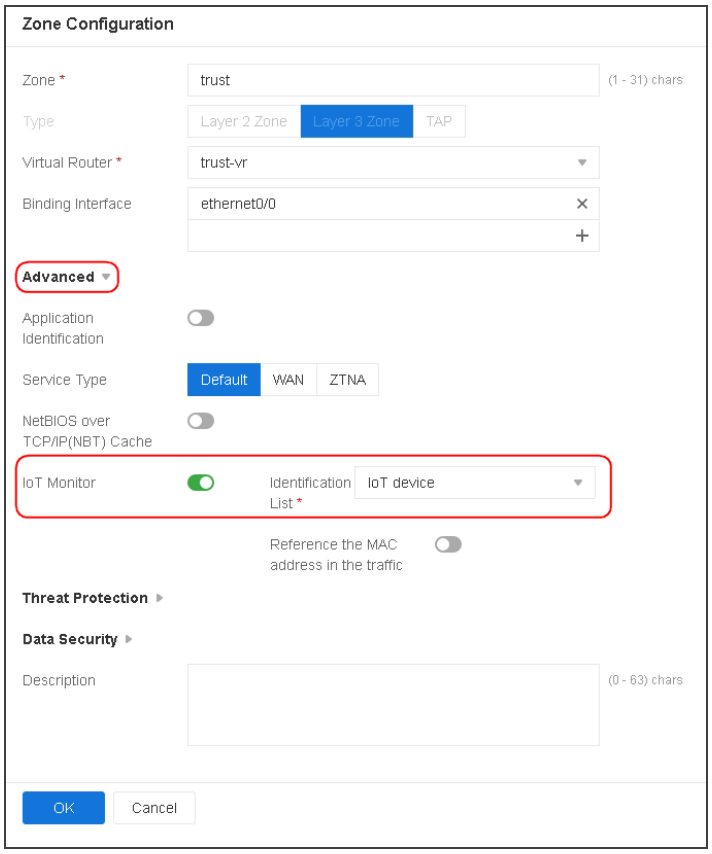


Step 4: Configure a zone to enable the IoT Monitor function of the zone. Select the zone used by IoT device traffic passing through the firewall based on the actual networking environment (In this example, the layer-3 zone "trust" is used)

Select **Network** > **Zone**. In the list, select "trust" and click **Edit**.

- Advanced: Click **Advanced** to expand this section.
- IoT Monitor: Click Enable.
- Identification List: Select the identification list "IoT device" that is created in Step 2.

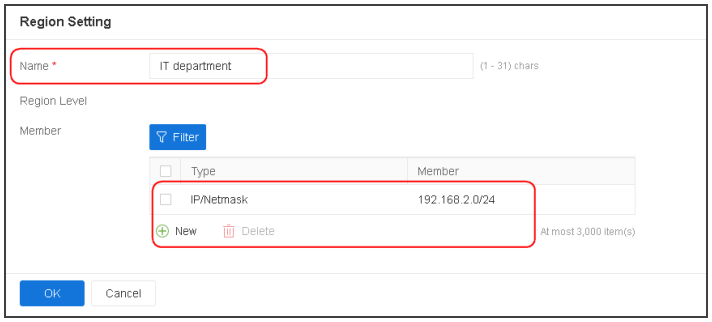
Click **OK**.



IoT Monitor Management

Step 1: Configure the Region

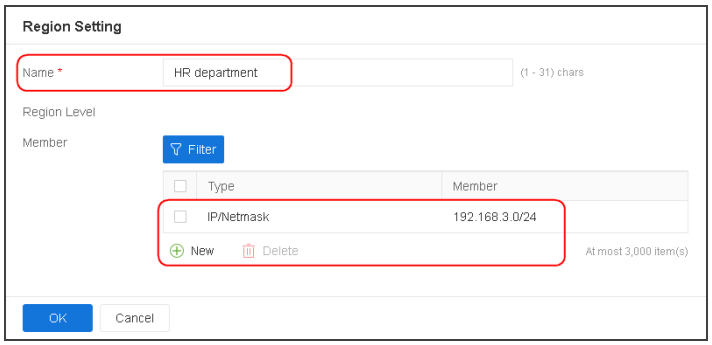
Select **Object** > **IoT Policy** > **Region Setting**. On the **Region Setting** page, click **New** and configure the following parameters:



- Name: IT department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.2.0/24

Click **OK**.

Repeat the steps above to create the region "HR department":

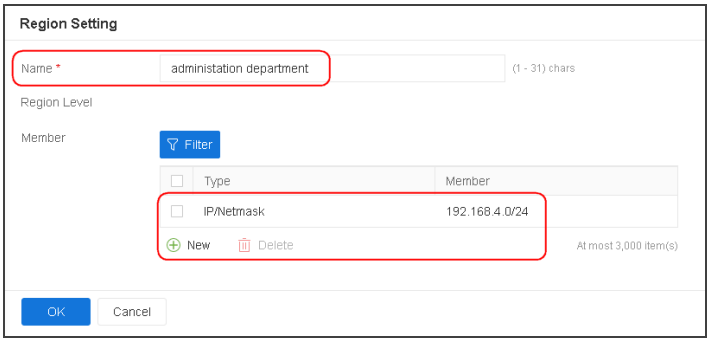


- Name: HR department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.3.0/24

Click **OK**.

Step 1: Configure the Region

Repeat the steps above to create the region "administration department":

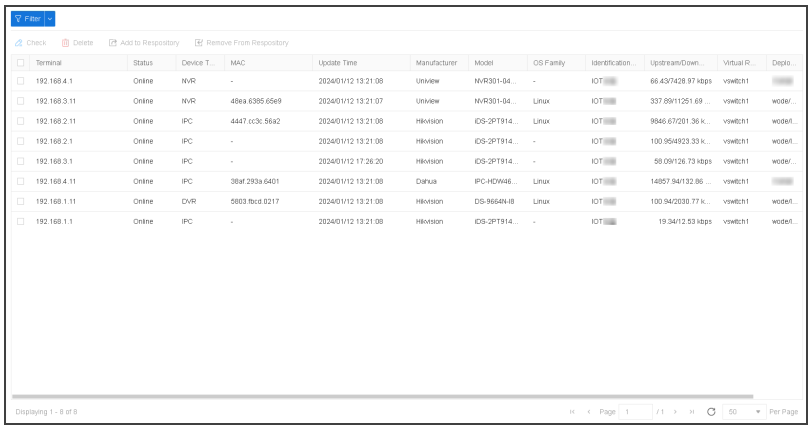


- Name: administration department
- Member: Click **New**.
  - Type: IP/Netmask
  - Member: 192.168.4.0/24

Click **OK**.

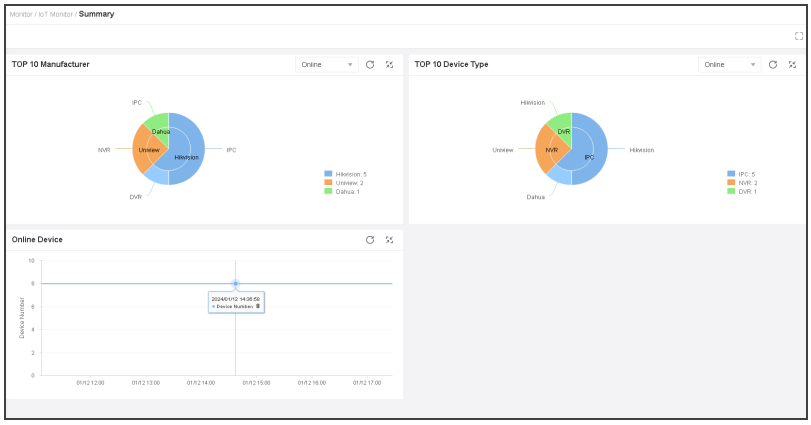
Step 2: View IoT monitor

Select **Monitor** > **IoT Monitor** > **Details** to view details about all identified IoT devices in the deployment environment.



Step 2: View IoT monitor

Select **Monitor** > **IoT Monitor** > **Summary** to view the top 10 device manufacturers and device type distribution.



IoT Policy Control

Step 1: Configure a device object

Select **Object** > **Device**. On the **Device** page, click **New**.

On the **Device Config** page, configure the following parameters:

- Device Name: tablet
- Type: Select Tablet
- You can configure other options as required



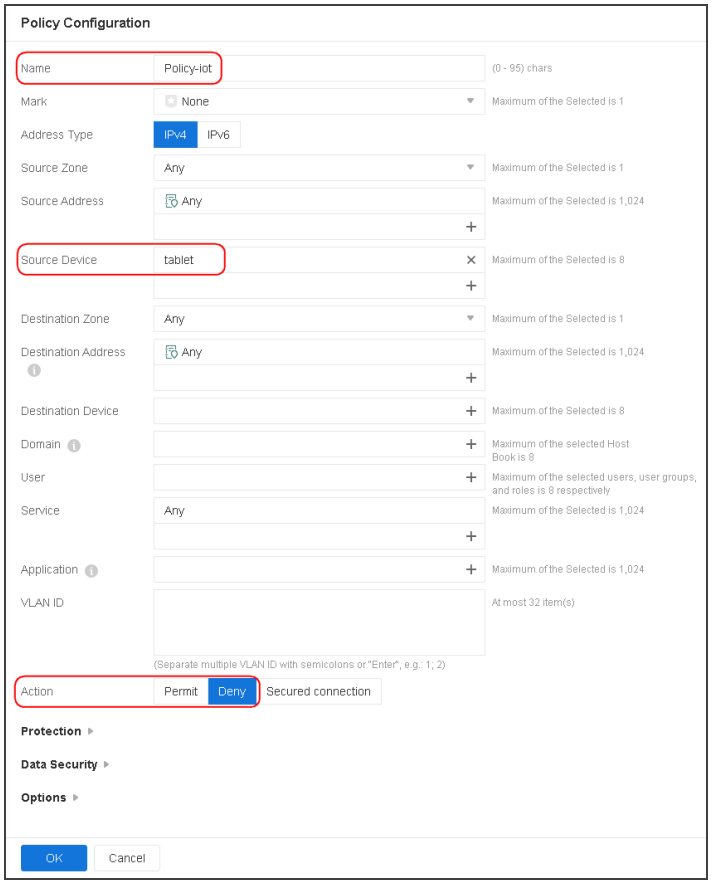
Click **OK**.

Step 2: Configure the policy rule to manage permissions on Internet access for tablets

Select **Policy** > **Security Policy** > **Policy**. On the **Policy Configuration** page, configure the following parameters:

- Name: Policy-iot
- Source Device: Select the "tablet" device object created in Step 1
- Action: Select Deny
- You can configure other options as required or default

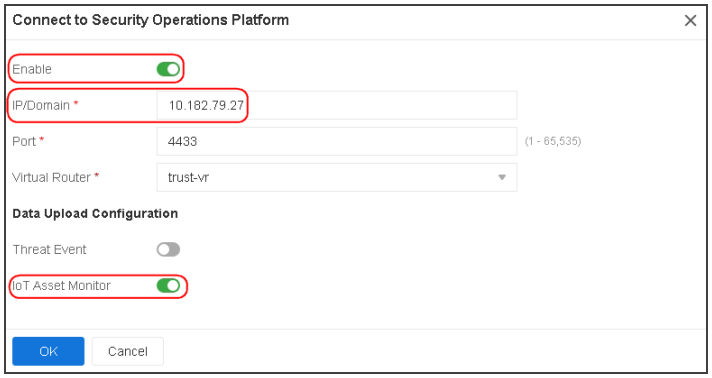
Click **OK**.



IoT Data Analysis

Connect to iSource and enable the IoT Asset Monitor function

Select **System** > **Extended Services**. In the **Connect to Security Operations Platform** section, click in the lower-left corner. In the **Connect to Security Operations Platform** panel, configure the following parameters:



- Enable: Click Enable
- IP/Domain: 10.182.79.27 (the iSource address in the networking environment)
- IoT Asset Monitor: Click Enable
- Keep the default values for other options

Click **OK**.

Configuration Steps of CLI

IoT Asset Identification Configuration

VM Configuration

For more information, see the VM Configuration section.

Firewall Configuration

Step 1: Enable and configure the local asset identification function

hostname# (config)# `iot-monitor docker-detect enable`

hostname# (config)# **iot-monitor docker-detect external-docker ip 10.182.197.172 port 45622** (In this example, the default port number is used. If customization is required, the port number needs to be consistent with the "Docker Port" configured in "Related Configuration" in step 5 of the virtual machine configuration.)

Step 2: Configure the identification list

hostname(config)# **iot-monitor identify-list iotdevice**

hostname(config-IoT-monitor-identify-list)# **ip network 192.168.0.1/16** (the address range of IoT devices within the enterprise)

hostname(config-IoT-monitor-identify-list)# **exit**

Step 3: Configure a zone to enable the IoT Monitor function of the zone. Select the zone used by IoT device traffic passing through the firewall based on the actual networking environment (In this example, the layer-3 zone "trust" is used)

hostname(config)#**zone trust**

hostname(config-zone-trust)# **iot-monitor enable iotdevice**

hostname(config-zone-trust)# **exit**

IoT Monitor Management

Step 1: Configure the Region

hostname(config)# **iot-monitor district id 1 name IT** (Configure the region of IT department)

hostname(config-IoT-monitor-district)# **ip network 192.168.2.0/24**

hostname(config)# **iot-monitor district id 1 name HR** (Configure the region of HR department)

hostname(config-IoT-monitor-district)# **ip network 192.168.3.0/24**

hostname(config)# **iot-monitor district id 1 name admin** (Configure the region of administration department)

hostname(config-IoT-monitor-district)# **ip network 192.168.4.0/24**

Step 2: View IoT monitor

```
hostname(config)# show iot-monitor-list
Total: 5
ip vrouter/vswitch type manufacturer status OS_family Rx(kbps)/Tx(kbps) profile
192.168.4.1 trust-vr Ipad Huawei Online -65.57/7517.99 iotdevice
192.168.3.11 trust-vr IPC Hikvision Online -16600.00/11507.00 iotdevice
192.168.2.11 trust-vr IPC Hikvision Online -9464.91/192.992 iotdevice
192.168.2.1 trust-vr Voip Phone - Online -96.53/4729.00 iotdevice
192.168.3.1 trust-vr Printer HP Online- 166.49/7565.09 iotdevice
```

IoT Policy Control

Step 1: Configure a device object

```
hostname(config)# device pad
hostname(config-device)# type Ipad
hostname(config-device)# exit
```

Step 2: Configure the policy rule to manage permissions on Internet access for tablets

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
hostname(config-policy-rule)# src-device pad
hostname(config-policy-rule)# action deny
hostname(config-policy-rule)# exit
hostname(config)#
```

IoT Data Analysis

Connect to iSource and enable the IoT Asset Monitor function

```
hostname(config)# cloud server isource

hostname(config-isource)# enable

hostname(config-isource)# address 10.182.79.27 (the iSource address in the networking environment)

hostname(config-isource)# upload-type iot-monitor-property

hostname(config-isource)# exit
```

Data Security

The data security allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs) on user network behavior.

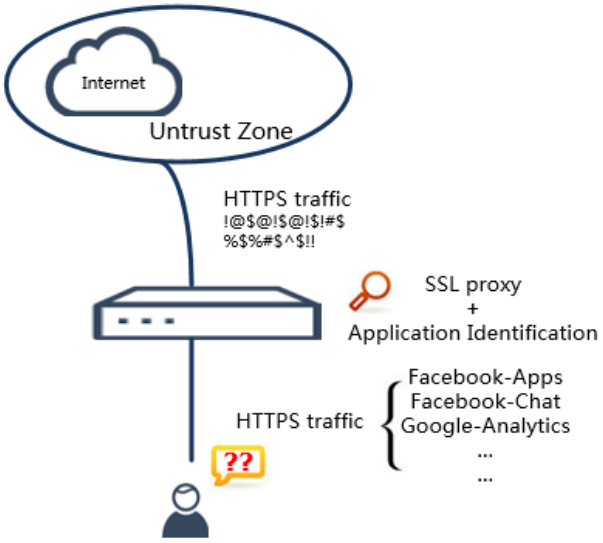
This chapter contains the following recipe:

- "Decrypting HTTPS Traffic and Identifying the Encrypted Application" on Page 452
- "URL Filtering for HTTPS Traffic without the CA Certificate" on Page 456

Decrypting HTTPS Traffic and Identifying the Encrypted Application

This example introduces how to decrypt HTTPS traffic and identify the encrypted application, which meets the requirements of fine-grained application management.

As shown in the below scenario, an internal user accesses a HTTPS website and the traffic is encrypted by SSL protocol. With the SSL proxy and application identification functions enabled, the device can decrypt the HTTPS traffic and identify the encrypted application.



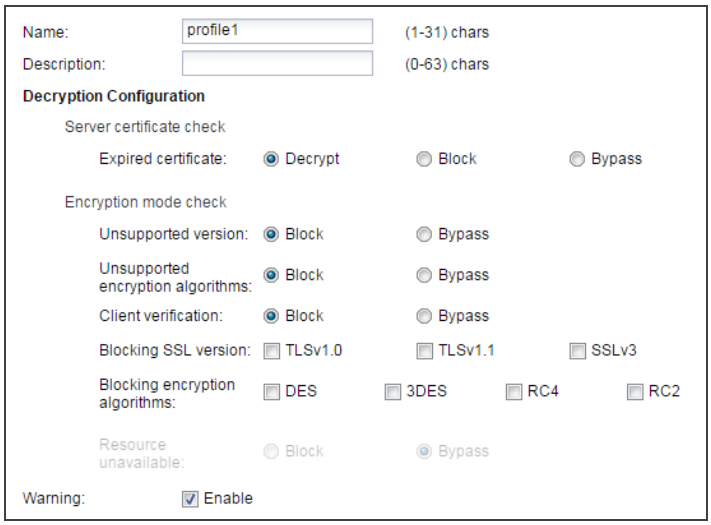
Configuration Steps

Step 1: Configuring a SSL proxy profile

Select **Policy > SSL Proxy**, and click **New**.

In the Basic tab:

- Name: profile1
- Expired certificate: Decrypt
- Unsupported version: Block
- Unsupported encryption algorithms: Block
- Client verification: Block
- Warning: Enable



Step 2: Specifying a SSL profile in the security policy

Configure a security policy that allows internal users to access Internet, and specify a SSL proxy profile in the Advanced tab:

- SSL Proxy: Select the **Enable** checkbox and select **profile1** from the drop-down list.

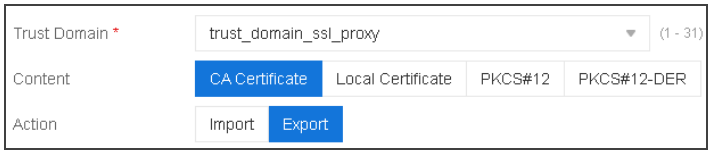


Step 3: Importing the device certificate to client's Web browser

Export the certificate from the device.

Click **System > PKI**. In the Management tab:

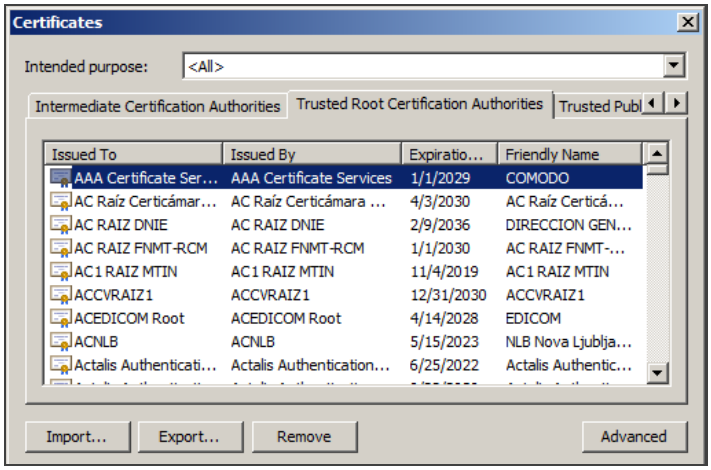
- Trust Domain: trust_domain_ssl_proxy
- Content: CA Certificate
- Action: Export



Click **OK** to export the certificate.

Import the certificate to client's Web browser.

1. In the Chrome Web browser, select **Settings > Show advanced settings**.
2. In the HTTPS/SSL section, select **Manage certificates**.
3. In the Trusted Root Certification Authorities tab, select **Import**.
4. Follow the wizard to import the certificate.



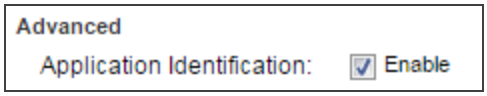
Step 4: Upgrading to the professional application signature database and enabling the application identification function

In CLI, execute the upgrade command to upgrade to the professional application signature database

```
SG-6000# exec app update professional
```

Step 4: Upgrading to the professional application signature database and enabling the application identification function

Select **Network > Zone**, and double-click the **untrust** zone. In the Basic tab:

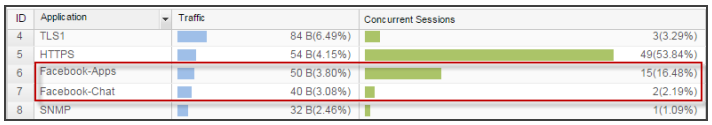


- Application Identification: Select **Enable**.

Step 6: Viewing application monitor

Select **Monitor > Application > Application Details**.

When an internal user accesses a HTTPS website, the SSL proxy function decrypts the HTTPS traffic and the application identification function identify the encrypted application.



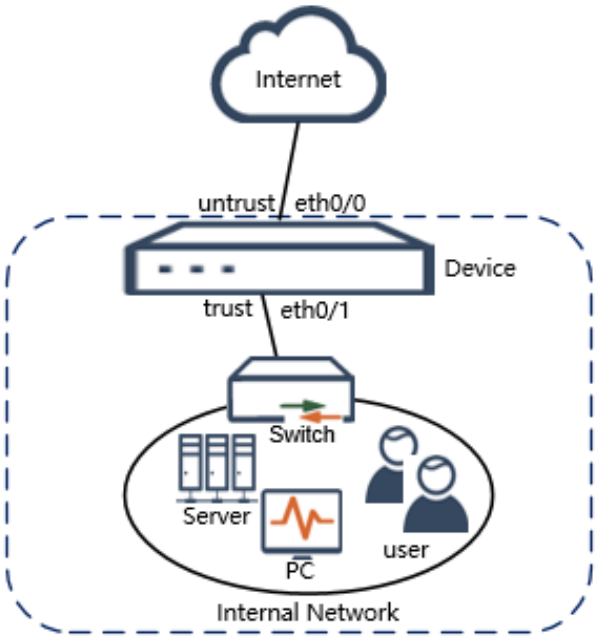
ID	Application	Traffic	Concurrent Sessions
4	TLS1	84 B(6.49%)	3(3.29%)
5	HTTPS	54 B(4.15%)	49(53.84%)
6	Facebook-Apps	50 B(3.80%)	15(16.48%)
7	Facebook-Chat	40 B(3.08%)	2(2.19%)
8	SNMP	32 B(2.46%)	1(1.09%)

URL Filtering for HTTPS Traffic without the CA Certificate

This example shows how to achieve the URL filtering for HTTPS traffic without installing the CA certificate.

As shown in the following topology, Hillstone device works as the gateway of an enterprise. The ethernet0/0 connects the Internet and belongs to the untrust zone. The ethernet0/1 connects to the Intranet and belongs to the trust zone.

With the configured URL filtering rule, staff of the enterprise (the network segment: 10.100.0.0/16) are prohibited from accessing shopping websites and the entertainment websites https:// www.bcd.com during working hours (09:00 to 18:00, Monday to Friday). The access and search attempts will be logged.



Preparation

Before configuring the URL filtering function, prepare the following first:

1. Install the URL service license and reboot the device.
2. Update the predefined URL database.

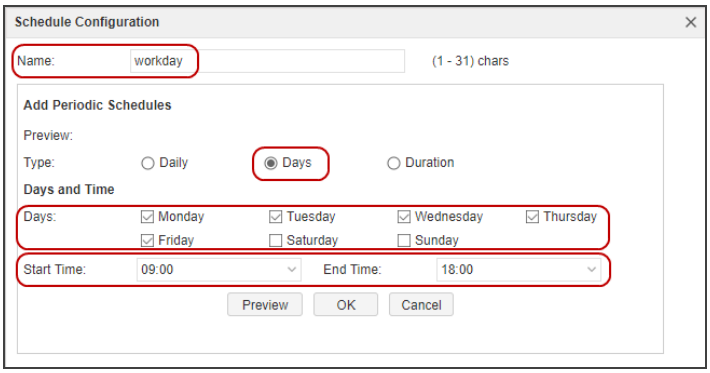
Configuration Steps

Step 1: Configure a schedule

Select **Object > Schedule**, and click **New**.

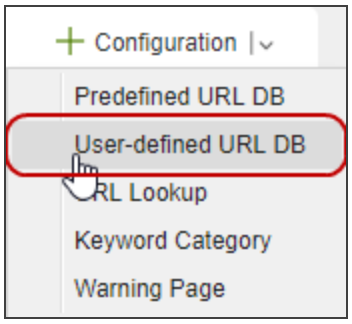
In the **Schedule Configuration** dialog:

- Name: workday
- Days: Click **Add** to add a periodic schedule.
- Type: Days.
- Days: Monday, Tuesday, Wednesday, Thursday, Friday
- Start Time: 09:00
- End Time: 18:00



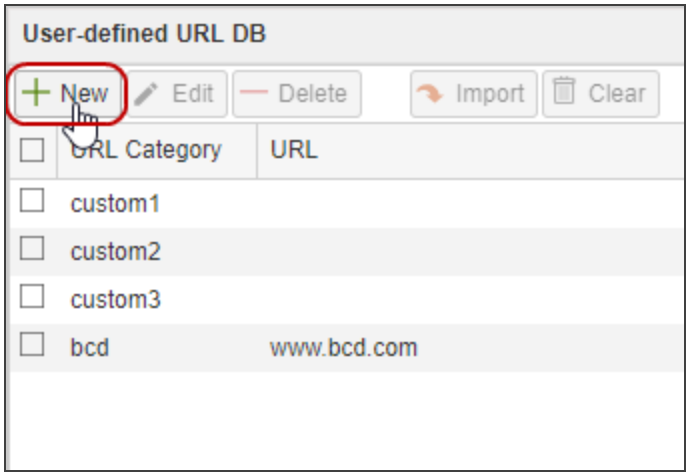
Step 2: Configure the user-defined URL category named bcd that contains https://www.bcd.com

Select **Object > URL Filtering**, and select **Configuration > User-defined URL DB** at the top-right corner.



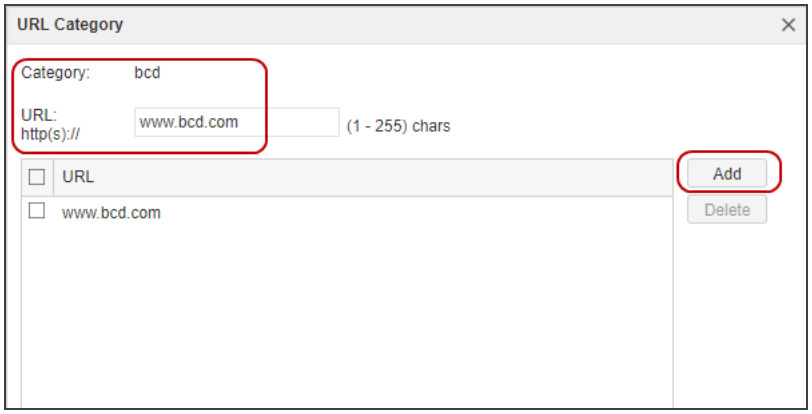
Step 2: Configure the user-defined URL category named bcd that contains https://www.bcd.com

In the **User-defined URL DB** dialog, click **New**.



In the **URL Category** dialog:

- Category: bcd
- URL http(s)://: www.bcd.com
- Click **Add** to add the "https://www.b-cd.com" and its category to the table.

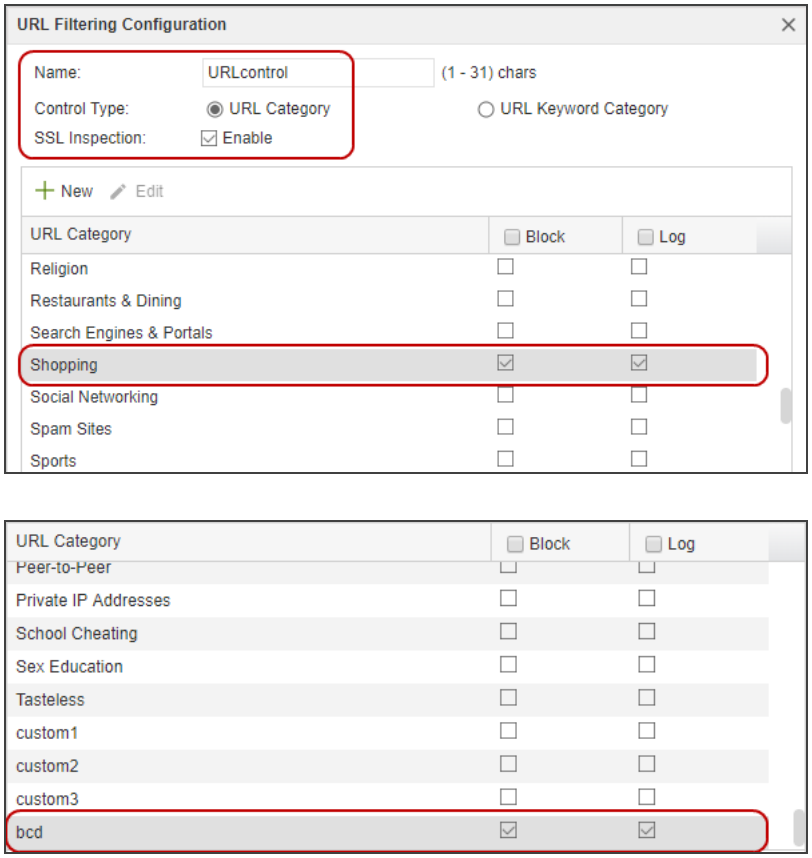


Step 3: Configure the URL filtering rule named URLcontrol, and enable the SSL Inspection

Select **Object > URL Filtering**, and click **New**.

In the **URL Filtering Rule Configuration** dialog:

- Name: URLcontrol
- Control Type: URL Category
- SSL Inspection: Select the **Enable** check box to enable SSL negotiation packets inspection.
- Select the predefined URL category **Shopping**, and then select the **Block** check box and **Log** check box.
- Select the user-defined URL category **bcd**, and then select the **Block** check box and **Log** check box.

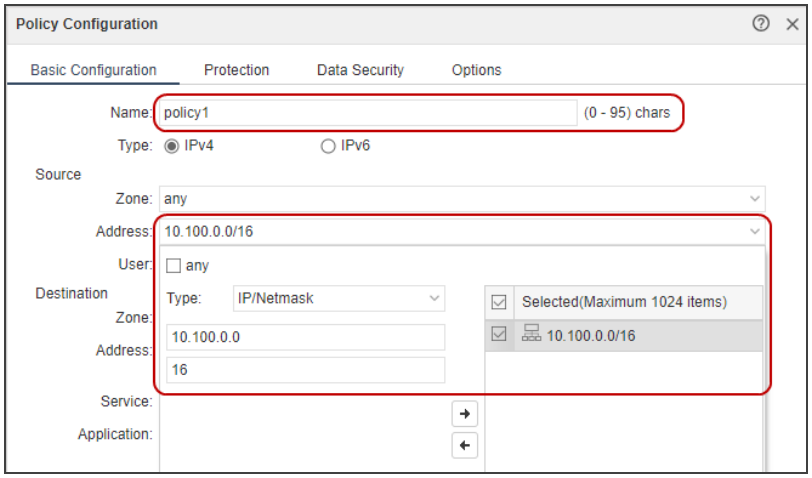


Step 4: Bind the URL filtering rule to a policy rule

Select **Policy > Security Policy**, and click **New**.

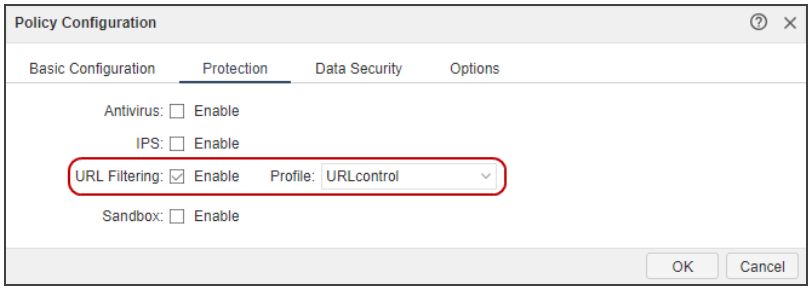
In the **Basic Configuration** tab of the **Policy Configuration** dialog:

- Name: policy1
- Source Address: Select the address type **IP/Netmask** , type 10.100.0.0 and 16 into the **IP**and **Netmask** text box respectively, and click -> to add the address to the right pane.



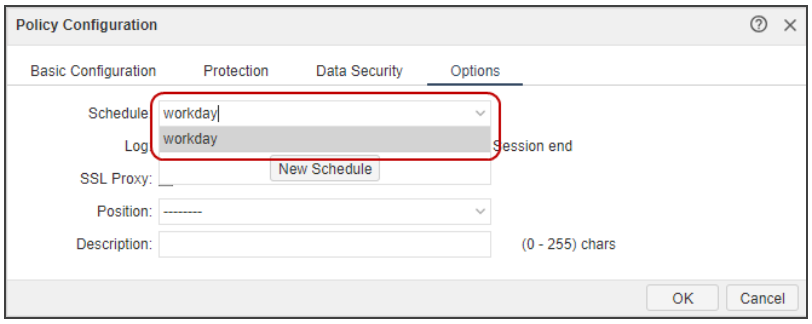
In the **Protection** tab of the **Policy Configuration** dialog:

- URL Filtering: Select the **Enable** check box.
- Profile: Select the created URL filtering rule "URLcontrol" from the drop-down list.



In the **Options** tab of the **Policy Configuration** dialog:

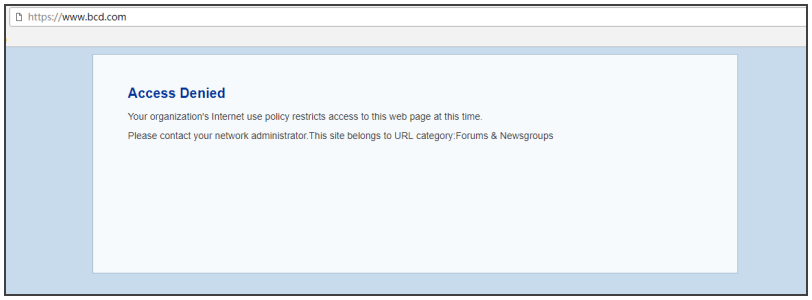
- Schedule: Select the schedule "workday" from the **Schedule** drop-down list.



Step 5: Result

After the configuration, adjust the configured rule to the highest priority rule for traffic matching.

When the rule takes effect, during the working hours, company staff cannot access shopping websites and the entertainment websites "https:// www.bcd.com". The system will log the access and search attempts.



IPv6

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 includes the following recipe:

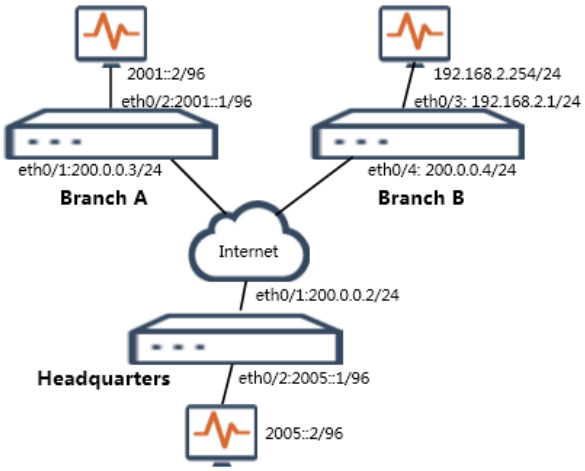
- "Connecting IPv6 and IPv4 Networks" on Page 463
- "Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 474
- "Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 483
- "Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel" on Page 494
- "Allowing Communication Between IPv6 networks by Configuring a 6RD Tunnel" on Page 497

Connecting IPv6 and IPv4 Networks

One enterprise has a headquarters, branch A and branch B. The headquarters and two branches all can access the Internet. The headquarters and branch A are deployed with IPv6 network for intranet and IPv4 network for internet, while the branch B is deployed with IPv4-only networks for both intranet and internet. For the business needs, it's necessary to connect IPv6 and IPv4 networks to achieve the following goals:

- The IPv6 network of headquarters can connect with the IPv4 Internet and be accessed by the Internet users.
- The networks of headquarters can connect with the IPv6 network of branch A via 6in4 tunnel.
- The networks of headquarters can connect with the IPv4 network of branch B.

The headquarters, branch A and branch B is deployed with a Hillstone device separately and the topology is as follows:



There are three parts of configurations:

- Configuring networks of headquarters
- Configuring networks of branch A
- Configuring networks of branch B

Configuring Networks of Headquarters

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 200.0.0.2 255.255.255.0
hostname(config-if-eth0/1)# manage http
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# dns-proxy
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2005::1/96
hostname(config-if-eth0/2)# manage ping
hostname(config-if-eth0/2)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 branchA
hostname(config-if-tun1)# exit
```

Step 2: Configure the route and NAT rules, including headquarters accessing the Internet, headquarters communicating with branch B, and public IP accessing IPv6 server of headquarters.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from 2005::/96 to 2003::/96 service any eif ethernet0/1 trans-to eif-ip mode dynamicport
hostname(config-vrouter)# snatrule id 2 from 2005::2/96 to 2004::2 service any eif ethernet0/1 trans-to eif-ip mode dynamicport
hostname(config-vrouter)# snatrule id 3 from any to 200.0.0.2 service any eif ethernet0/2 trans-to 2005::1 mode dynamicport
hostname(config-vrouter)# dnatrule id 1 from 2005::/96 to 2003::/96 service any v4-mapped
hostname(config-vrouter)# dnatrule id 2 from 2005::2/96 to 2004::2 service any trans-to 200.0.0.4
hostname(config-vrouter)# dnatrule id 3 from any to 200.0.0.2 service any trans-to 2005::2
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# ipv6 route 2001::/96 tunnel1
hostname(config-vrouter)# exit
```

Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
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-global
hostname(config-policy)# rule id 2
Rule id 2 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2004::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 3
Rule id 3 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2003::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

```
hostname(config)# policy-global
hostname(config-policy)# rule id 4
Rule id 4 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2001::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 5
Rule id 5 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2001::/96
hostname(config-policy-rule)# dst-ip 2005::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 6
Rule id 6 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip ipv6-any
hostname(config-policy-rule)# dst-ip ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

Step 4: Configure an IPv6 tunnel.

```
hostname(config)# tunnel ip6in4 branchA manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 200.0.0.3
hostname(config-ip6in4-manual)# exit
hostname(config)# ip name-server 8.8.8.8 vrouter trust-vr
hostname(config)# ip dns-proxy domain any name-server 8.8.8.8 vrouter trust-vr
hostname(config)# ipv6 dns64-proxy id 1 prefix 2003::/96 source 2005::/96 trans-mapped-ip any
```

Note: The **`ipv6 dns64-proxy`** command is not supported for some versions.

Configuring Networks of Branch A

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 200.0.0.3 255.255.255.0
hostname(config-if-eth0/1)# manage ping
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2001::1/96
hostname(config-if-eth0/2)# manage ping
hostname(config-if-eth0/2)# exit
hostname(config)# interface tunnel1
hostname(config-if-tun1)# zone trust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# tunnel ip6in4 headquarters
hostname(config-if-tun1)# exit
```

Step 2: Configure the route and NAT rules.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# ipv6 route 2005::/96 tunnel1
hostname(config-vrouter)# exit
```

Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 31
Rule id 31 is created
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-global
hostname(config-policy)# rule id 32
Rule id 32 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2001::/96
hostname(config-policy-rule)# dst-ip 2005::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
hostname(config)# policy-global
hostname(config-policy)# rule id 33
Rule id 33 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip 2005::/96
hostname(config-policy-rule)# dst-ip 2001::/96
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

```
hostname(config)# policy-global
hostname(config-policy)# rule id 34
Rule id 34 is created
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# src-ip ipv6-any
hostname(config-policy-rule)# dst-ip ipv6-any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# exit
```

Step 4: Configure an IPv6 tunnel.

```
hostname(config)# tunnel ip6in4 headquarters manual
hostname(config-ip6in4-manual)# interface ethernet0/1
hostname(config-ip6in4-manual)# destination 200.0.0.2
hostname(config-ip6in4-manual)# exit
```

Configuring Networks of Branch B

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.2.1 255.255.255.0
hostname(config-if-eth0/1)# manage ping
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 200.0.0.4 255.255.255.0
hostname(config-if-eth0/4)# manage ping
hostname(config-if-eth0/4)# exit
```

Step 2: Configure the route and NAT rules.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule id 1 from any to any service any eif ethernet0/4 trans-to eif-ip
mode dynamicport
hostname(config-vrouter)# dnatrule id 1 from 200.0.0.2 to 200.0.0.4 service any trans-to 192.168.2.254
hostname(config-vrouter)# ip route 0.0.0.0/0 200.0.0.1
hostname(config-vrouter)# exit
```

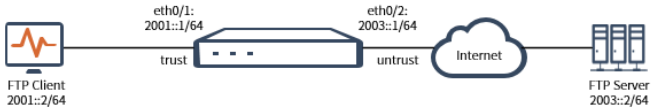
Step 3: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 35
Rule id 35 is created
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
```

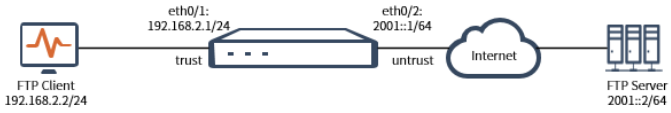
Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG

This example introduces how to configure ALG to realize the FTP service in IPv6-only or IPv4/IPv6 hybrid networks, including the following three scenarios:

- **Scenario 1: IPv6-only network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Both internal and external network IP addresses are deployed with IPv6 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.



- **Scenario 2: IPv4 network to IPv6 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv4 addresses and the external network is deployed with IPv6 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.



- **Scenario 3: IPv6 network to IPv4 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv6 addresses and the external network is deployed with IPv4 addresses. With the ALG function configured, the internal FTP client can access the FTP server in the extranet.



Before You Start

Before starting the configuration, you need to ensure that the configuration of the FTP server and the FTP client has been completed.

This example only describes the relevant configuration on the device.

Configuration Steps of Scenario 1

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ip address 2002::1/64
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Enable the ALG function of FTP.

hostname(config)# **alg ftp**

Note: The ALG function of FTP is enabled by default.

Step 4: Verify result.

Download session in FTP active mode:

session: id 44, proto 6, flag 0, flag1 20000, flag2 0, flag3 0, created 39340, life 1787, policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64348->[2001::2]:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2003::2]:64348

session: id 2, proto 6, flag 8000000, flag1 20000, flag2 0, flag3 0, created 39408, life 1800, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/208810): [2001::2]:20->[2003::2]:64363

flow1(32(ethernet0/2)/40208810): [2003::2]:64363->[2001::2]:20

Download session in FTP passive mode:

session: id 61, proto 6, flag 10000, flag1 20000, flag2 0, flag3 0, created 39683, life 1775, policy 1,app 4 (FTP) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64362->[2001::2]:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2003::2]:64362

session: id 22, proto 6, flag 8000000, flag1 20000, flag2 0, flag3 0, created 39684, life 1776, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40208810): [2003::2]:64398->[2001::2]:56008

flow1(31(ethernet0/1)/208810): [2001::2]:56008->[2003::2]:64398

Configuration Steps of Scenario 2

Step 1: Configure the interface and zone.

```
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
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2001::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from any to any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from any to 192.168.2.10 service any trans-to 2001::10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from any to 192.168.2.10 service any trans-to ip 2001::2
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of FTP.

```
hostname(config)# alg ftp
```

Note: The ALG function of FTP is enabled by default.

Step 5: Verify result.

Download session in FTP active mode:

session: id 64, proto 6, flag e, flag1 20007, flag2 0, flag3 0, created 133143, life 1797, policy 2,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40300b10): 192.168.2.2:58259->192.168.2.10:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2001::10]:1025

session: id 14, proto 6, flag 8000016, flag1 2000b, flag2 0, flag3 0, created 133147, life 297, policy 2,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/208810): [2001::2]:20->[2001::10]:58261

flow1(32(ethernet0/2)/40200810): 192.168.2.2:58261->192.168.2.10:20

Download session in FTP passive mode:

session: id 20, proto 6, flag e, flag1 20007, flag2 0, flag3 0, created 133393, life 1797, policy 2,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40300b10): 192.168.2.2:58272->192.168.2.10:21

flow1(31(ethernet0/1)/308b10): [2001::2]:21->[2001::10]:1030

session: id 2, proto 6, flag 800000e, flag1 20007, flag2 0, flag3 0, created 133397, life 1797, policy 2,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40200810): 192.168.2.2:58273->192.168.2.10:61665

flow1(31(ethernet0/1)/208810): [2001::2]:61665->[2001::10]:61665

Configuration Steps of Scenario 3

Step 1: Configure the interface and zone.

```
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 2003::1/64
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 192.168.1.1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service ftp permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from ipv6-any to 2003::10 service any trans-to 192.168.1.10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from ipv6-any to 2003::10 service any trans-to ip 192.168.1.2
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of FTP.

```
hostname(config)# alg ftp
```

Note: The ALG function of FTP is enabled by default.

Step 5: Verify result.

Download session in FTP active mode:

session: id 6, proto 6, flag e, flag1 2000b, flag2 0, flag3 0, created 40792, life 1799, policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64537->[2003::10]:21

flow1(31(ethernet0/1)/300b10): 192.168.1.2:21->192.168.1.10:1034

session: id 5, proto 6, flag 8000016, flag1 20007, flag2 0, flag3 0, created 40798, life 1799, policy 1,app 70(FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(31(ethernet0/1)/200810): 192.168.1.2:20->192.168.1.10:64538

flow1(32(ethernet0/2)/40208810): [2003::2]:64538->[2003::10]:20

Download session in FTP passive mode:

session: id 21, proto 6, flag e, flag1 2000b, flag2 0, flag3 0, created 40093, life 1799, policy 1,app 4(FTP) flag 0x1, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/2)/40308b10): [2003::2]:64435->[2003::10]:21

flow1(31(ethernet0/1)/300b10): 192.168.1.2:21->192.168.1.10:1026

session: id 14, proto 6, flag 800000e, flag1 2000b, flag2 0, flag3 0, created 40099, life 300, policy 1,app 70 (FTP-DATA) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

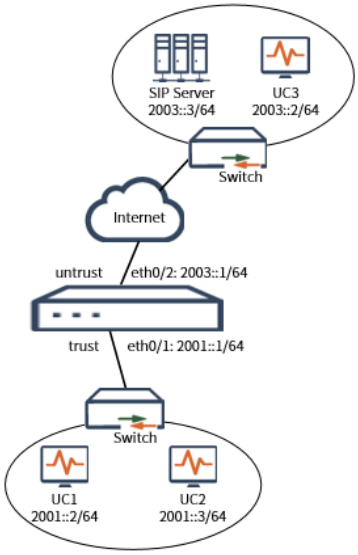
flow0(32(ethernet0/2)/40208810): [2003::2]:64436->[2003::10]:56075

flow1(31(ethernet0/1)/200810): 192.168.1.2:56075->192.168.1.10:56075

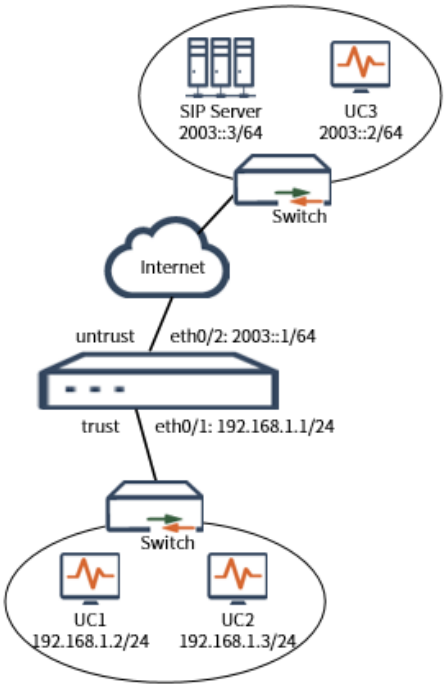
Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG

This example introduces how to configure ALG to realize the SIP communication in IPv6-only or IPv4/IPv6 hybrid networks, including the following three scenarios:

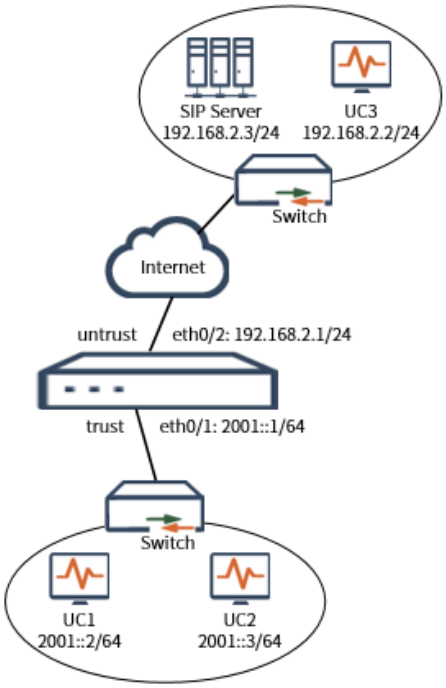
- **Scenario 1: IPv6-only network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. Both internal and external network IP addresses are deployed with IPv6 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



- **Scenario 2: IPv4 network to IPv6 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv4 addresses and the external network is deployed with IPv6 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



- **Scenario 3: IPv6 network to IPv4 network**. In the topology below, an enterprise sets up a Hillstone security device as the export gateway to connect internal network with the Internet. The internal network is deployed with IPv6 addresses and the external network is deployed with IPv4 addresses. With the ALG function configured, the internal SIP UC1 and the external SIP UC3 can successfully establish communication with each other.



Before You Start

Before starting the configuration, you need to ensure that the configuration of the SIP Server and the SIP user agent (SIP UC) has been completed. This example only describes the relevant configuration on the device.

Configuration Steps of Scenario 1

Step 1: Configure the interface and zone.

```
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 ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 4: Verify result.

View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

```
hostname# show pinhole
Total pinhole count in D-Plane: 5
[Pinhole0]=========================================
Seq 10
App SIP MEDIA (id:875)
Flag: Enabled,
[Ingress info]-----------------------------------------------
Zone trust (id:2)
Flow0 (ifid 0) :::any -> 2003::2:5001
[Egress info]------------------------------------------------
Zone untrust (id:3)
Flow1 (ifid 0) 2003::2:5001 -> :::any
[Life info]--------------------------------------------------
After_hit 600
Before_hit 120
Timer 217
[Other info]-------------------------------------------------
Auth_user_id 0
```

Configuration Steps of Scenario 2

Step 1: Configure the interface and zone.

```
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)# interface ethernet0/2
hostname(config-if-eth0/2)# zone untrust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 2003::1/64
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from any to any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from any to 192.168.1.10 service any trans-to 2003::10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from any to 192.168.1.10 service any trans-to ip 2003::3
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 5: Verify result.

View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

```
hostname# show pinhole
Total pinhole count in D-Plane: 5
[Pinhole
1]=============================================================-
====
Seq 15
App SIP MEDIA (id:875)
Flag: Enabled,
[Ingress info]-------------------------------------------------
Zone untrust (id:3)
Flow0 (ifid 0) :::any -> 2003::10:1025
[Egress info]--------------------------------------------------
Zone trust (id:2)
Flow1 (ifid 31) 192.168.1.2:5002 -> 192.168.1.10:any
[Life info]----------------------------------------------------
After_hit 600
Before_hit 120
Timer 38
[Other info]---------------------------------------------------
Auth_user_id 0
```

Configuration Steps of Scenario 3

Step 1: Configure the interface and zone.

```
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 2002::1/64
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 192.168.2.1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure the policy.

```
hostname(config)# rule id 1 from ipv6-any to ipv6-any service sip permit
Rule id 1 is created
hostname(config-policy)# rule id 1
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# exit
```

Step 3: Configure the NAT rule.

```
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from ipv6-any to 2001::10 service any trans-to 192.168.2.10 mode dynamicport
rule ID=1
hostname(config-nat)# dnatrule id 1 from ipv6-any to 2001::10 service any trans-to ip 192.168.2.3
rule ID=1
hostname(config-nat)# exit
```

Step 4: Enable the ALG function of SIP.

```
hostname(config)# alg sip
```

Note: The ALG function of SIP is enabled by default.

Step 5: Verify result.

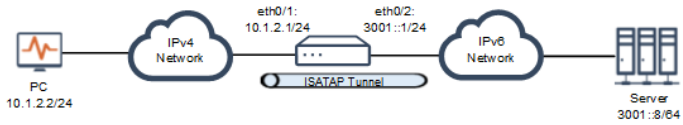
View the information of media pinhole. Total pinhole count is 5, including 1 register pinhole and 4 media pinhole.

```
SG-6000# show pinhole
Total pinhole count in D-Plane: 5
[Pin-
hole1]==================================================
Seq 36
App SIP MEDIA (id:875)
Flag: Enabled,
[Ingress info]--------------------------------------------------
Zone trust (id:2)
Flow0 (ifid 0) 0.0.0.0:any -> 192.168.2.10:5002
[Egress info]---------------------------------------------------
Zone trust (id:2)
Flow1 (ifid 31) 2001::2:5002 -> 2001::10:any
[Life info]-----------------------------------------------------
After_hit 600
Before_hit 120
Timer 107
[Other info]----------------------------------------------------
Auth_user_id 0
```

Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel

This example introduces how to configure ISATAP tunnel to realize dual stack host access to IPv6 network in IPv4 network.

In the topology below, PC supports dual protocol stacks. Hillstone device is connected to the corresponding IPv6 network and IPv4 network. It is required to configure the ISATAP tunnel so that the dual-stack host PC in the IPv4 network can access the server in the intranet IPv6 network.



Configuration Steps

Step 1: Configure the interface and zone.

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 10.1.2.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ipv6 enable
hostname(config-if-eth0/2)# ipv6 address 3001::1/24
hostname(config-if-eth0/2)# exit
```

Step 2: Configure ISATAP tunnel and bind a interface

```
hostname(config)# tunnel ip6in4 tunnel isatap
hostname(config-ip6in4-isatap)# interface ethernet0/1
hostname(config-ip6in4-isatap)# exit
hostname(config)#
```

Configure the tunnel interface and bind the tunnel interface to the ISATAP tunnel.

```
hostname(config)#  interface tunnel1
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# ipv6 address 2001::/64 eui-64
hostname(config-if-tun1)# ipv6 address fe80::5efe:10.1.2.1 link-local
hostname(config-if-tun1)# tunnel ip6in4 tunnel
hostname(config-if-tun1)# no ipv6 nd ra suppress
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-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 routing for PC, take win7 PC as an example

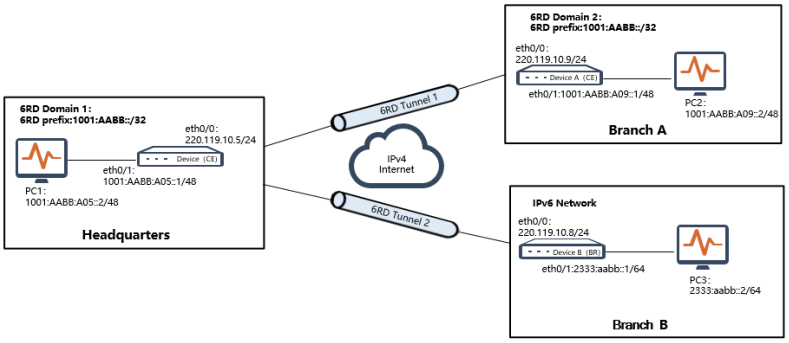
```
C:\>netsh interface ipv6 isatap set router 10.1.2.1
C:\>netsh interface ipv6 isatap set router 10.1.2.1 enabled
```

Step 6: Verify result.

The dual-stack host (10.1.2.2) can access the IPv6 Server (3001::8) through FTP successfully.

Allowing Communication Between IPv6 networks by Configuring a 6RD Tunnel

This example shows you how to configure a 6RD (IPv6 Rapid Deployment on IPv4 Infrastructures) tunnel to allow service providers to deploy IPv6 in a lightweight and secure manner via their existing IPv4-access network infrastructure.



* This example is used in a laboratory environment. Please configure the IP addresses of each interface according to the actual connections.

The figure above shows the network topology. This example includes the following two scenarios:

- **Scenario 1: 6RD Domain -6RD Domain**.The headquarters deploys a Hillstone security device Device and branch A deploys a Hillstone security device Device A. Device and Device A support both IPv4 and IPv6 and they are CE devices. Both Device and Device A are connected to the IPv6 network on one end and the IPv4 network on the other end. Assume that the ISP provides an IPv6 prefix of **1001:AABB::/32**. To allow hosts in two different 6RD domains to communicate, you need to configure a 6RD tunnel between Device and Device A.
- **Scenario 2: 6RD Domain -IPv6 Network**.The headquarters deploys a Hillstone security device Device and branch B deploys a Hillstone security device Device B. Both Device and Device B are connected to the IPv6 network on one end and the IPv4 network on the other end. Device in headquarters is a 6RD CE device and connects to the 6RD domain, which is an IPv6 network. Device B in branch B is a 6RD BR device and connects to a regular IPv6 network outside the 6RD domain. To allow hosts in the 6RD domain and IPv6 network to communicate, you need to configure a 6RD tunnel between Device and Device B.

Configuration Tips

For the 6RD Domain -6RD Domain in Scenario 1, the addresses of devices and PC1 at the headquarters and branch A need to meet the following requirements:

- The IPv6 prefix of the interface ethernet0/1 on the headquarters device (Device) needs to be consistent with the 6RD delegated prefix calculated by device. (In this example, the 6RD delegated prefix is **1001: AABB: A05::/48**)
- The IP address of PC1 and the interface ethernet0/1 of the headquarters device (Device) need to belong to the same IPv6 network segment. The IP address of PC2 and the interface ethernet0/1 of the branch A device (Device A) need to belong to the same IPv6 network segment.
- The headquarters device (Device) and branch A device (Device A) need to have the same IPv4 prefix for ethernet0/1, and this prefix length needs to be the same as that of the IPv4 prefix configured on the 6RD tunnel (In this example, the IPv4 prefix length is **ipv4-mask-len 16**).

Configuration Steps of Scenario 1

Configure Headquarters Device (Device)

Step 1: Configure the IPv4 address and zone of the interface ethernet 0/0 of the headquarters device (Device).

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 220.119.10.5/24
hostname(config-if-eth0/0)# exit
```

Step 2: Configure the 6RD tunnel.

```
hostname(config)# tunnel ip6in4 test 6rd
hostname(config-ip6in4-6rd)# interface ethernet0/0
hostname(config-ip6in4-6rd)# ipv6-prefix 1001:AABB::/32(Specify the 6RD prefix)
hostname(config-ip6in4-6rd)# ipv4-mask-len 16(Specify the IPv4 prefix length)
hostname(config-ip6in4-6rd)# subtunnel-limit 10(Specify the maximum number of 6RD subtunnels)
hostname(config-ip6in4-6rd)# exit
```

> **Note:** After you specify the 6RD prefix and IPv4 prefix length, the 6RD CE automatically calculates the 6RD delegated prefix. To view the 6RD delegated prefix via command **show ip6in4 6rd-tunnel** [*tunnel-name*].

Step 3: Configure the tunnel interface.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ip6in4 test
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# exit
```

Step 4: View the 6RD tunnel configurations.

```
SG-6000(config)#show ip6in4 6rd-tunnel test

Name: test

Index: 11

Interface: ethernet0/0

IPv6-prefix: 1001:AABB::/32

IPv4-mask-length: 16

Border-relay-address: 0.0.0.0

Tunnel interface: tunnel1

IPv6-delegated-prefix: 1001:AABB:A05::/48（The 6RD delegated prefix calculated by device）

Sub-tunnel Limit: 10
```

Step 5: Configure the IPv6 address and zone of the interface ethernet 0/1 of the headquarters device (Device).

```
hostname(config)#1interface ethernet0/1

hostname(config-if-eth0/1)# zone trust

hostname(config-if-eth0/1)# ipv6 enable

hostname(config-if-eth0/1)# ipv6 address 1001:AABB:A05::1/48（Note: This prefix must be consistent with the 6RD delegated prefix calculated by device）

hostname(config-if-eth0/1)# exit
```

Step 6: Configure a route for tunnel.

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route 1001:AABB::/32 tunnel1

hostname(config-vrouter)# exit
```

Step 7: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
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 8: Configure an address and default route for PC1

Set the address to 1001:AABB:A05::2/48 for PC1 based on the 6RD delegated prefix,. This address is in the same network segment as that of ethernet0/1 of Device.

Note:The method for configuring IPv6 addresses and default route varies based on the operating system of your PC.

Configure Device A

Step 1: Configure the IPv4 address and zone of the interface ethernet 0/0 of the Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 220.119.10.9/24
hostname(config-if-eth0/0)# exit
```

Step 2: Configure the 6RD tunnel.

```
hostname(config)# tunnel ip6in4 test 6rd
hostname(config-ip6in4-6rd)# interface ethernet0/0
hostname(config-ip6in4-6rd)# ipv6-prefix 1001:AABB::/32(Specify the 6RD prefix)
hostname(config-ip6in4-6rd)# ipv4-mask-len 16(Specify the IPv4 prefix length)
hostname(config-ip6in4-6rd)# subtunnel-limit 10(Specify the maximum number of 6RD subtunnels)
hostname(config-ip6in4-6rd)# exit
```

> **Note:** After you specify the 6RD prefix and IPv4 prefix length, the 6RD CE automatically calculates the 6RD delegated prefix. To view the 6RD delegated prefix via command **show ip6in4 6rd-tunnel** [*tunnel-name*].

Step 3: Configure the tunnel interface.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ip6in4 test
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# exit
```

Step 4: View the 6RD tunnel configurations.

```
SG-6000(config)#show ip6in4 6rd-tunnel test
Name: test
Index: 11
Interface: ethernet0/0
IPv6-prefix: 1001:AABB::/32
IPv4-mask-length: 16
Border-relay-address: 0.0.0.0
Tunnel interface: tunnel1
IPv6-delegated-prefix: 1001:AABB:A09::/48（The 6RD delegated prefix calculated by device）
Sub-tunnel Limit: 10
```

Step 5: Configure the IPv6 address and zone of the interface ethernet 0/1 of the Device A.

```
hostname(config)#1interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ipv6 enable
hostname(config-if-eth0/1)# ipv6 address 1001:AABB:A09::1/48（Note: This prefix must be consistent with the 6RD delegated prefix calculated by device）
hostname(config-if-eth0/1)# exit
```

Step 6: Configure a route for tunnel.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ipv6 route 1001:AABB::/32 tunnel1
hostname(config-vrouter)# exit
```

Step 7: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
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 8: Configure an address and default route for PC2.

Set the address to 1001:AABB:A05::2/48 for PC2 based on the 6RD delegated prefix. This address is in the same network segment as that of ethernet0/1 of Device A.

Note:The method for configuring IPv6 addresses and default route varies based on the operating system of your PC.

Configuration Steps of Scenario 2

Configure Headquarters Device (Device)

Step 1: Configure the IPv4 address and zone of the interface ethernet 0/0 of the headquarters device (Device).

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 220.119.10.5/24
hostname(config-if-eth0/0)# exit
```

Step 2: Configure the 6RD tunnel.

```
hostname(config)# tunnel ip6in4 test 6rd
hostname(config-ip6in4-6rd)# interface ethernet0/0
hostname(config-ip6in4-6rd)# ipv6-prefix 1001:AABB::/32(Specify the 6RD prefix)
hostname(config-ip6in4-6rd)# ipv4-mask-len 16(Specify the IPv4 prefix length)
hostname(config-ip6in4-6rd)# subtunnel-limit 10(Specify the IPv4 prefix length)
hostname(config-ip6in4-6rd)# border-relay-address 220.119.10.8 (Specify the IPv4 address of 6RD BR)
hostname(config-ip6in4-6rd)# exit
```

> **Note:** After you specify the 6RD prefix and IPv4 prefix length, the 6RD CE automatically calculates the 6RD delegated prefix. To view the 6RD delegated prefix via command **show ip6in4 6rd-tunnel** [*tunnel-name*].

Step 3: Configure the tunnel interface.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ip6in4 test
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# exit
```

Step 4: View the 6RD tunnel configurations.

```
SG-6000(config)#show ip6in4 6rd-tunnel test

Name: test

Index: 11

Interface: ethernet0/0

IPv6-prefix: 1001:AABB::/32

IPv4-mask-length: 16

Border-relay-address: 220.119.10.8

Tunnel interface: tunnel1

IPv6-delegated-prefix: 1001:AABB:A05::/48（The 6RD delegated prefix calculated by device）

Sub-tunnel Limit: 10
```

Step 5: Configure the IPv6 address and zone of the interface ethernet 0/1 of the headquarters device (Device)

```
hostname(config)#1interface ethernet0/1

hostname(config-if-eth0/1)# zone trust

hostname(config-if-eth0/1)# ipv6 enable

hostname(config-if-eth0/1)# ipv6 address 1001:AABB:A05::1/48（Note: This prefix must be consistent with the 6RD delegated prefix calculated by device.）

hostname(config-if-eth0/1)# exit
```

Step 6: Configure a route for tunnel.

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route 2333:aabb::/32 tunnel1

hostname(config-vrouter)# exit
```

Step 7: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
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 8: Configure an address and default route for PC1.

Set the address to 1001:AABB:A05::2/48 for PC1 based on the 6RD delegated prefix. This address is in the same network segment as that of ethernet0/1 of Device.

Note: The method for configuring IPv6 addresses and default route varies based on the operating system of your PC.

Configure Device B

Step 1: Configure the IPv4 address and zone of the interface ethernet 0/0 of the Device B.

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 220.119.10.8/24
hostname(config-if-eth0/0)# exit
```

Step 2: Configure the 6RD tunnel.

```
hostname(config)# tunnel ip6in4 test 6rd
hostname(config-ip6in4-6rd)# interface ethernet0/0
hostname(config-ip6in4-6rd)# ipv6-prefix 1001:AABB::/32(Specify the 6RD prefix)
hostname(config-ip6in4-6rd)# ipv4-mask-len 16(Specify the IPv4 prefix length)
hostname(config-ip6in4-6rd)# subtunnel-limit 10(Specify the maximum number of 6RD subtunnels)
hostname(config-ip6in4-6rd)# exit
```

> **Note:** After you specify the 6RD prefix and IPv4 prefix length, the 6RD CE automatically calculates the 6RD delegated prefix. To view the 6RD delegated prefix via command **show ip6in4 6rd-tunnel** [*tunnel-name*].

Step 3: Configure the tunnel interface.

```
hostname(config)# interface tunnel1
hostname(config-if-tun1)# tunnel ip6in4 test
hostname(config-if-tun1)# zone untrust
hostname(config-if-tun1)# ipv6 enable
hostname(config-if-tun1)# exit
```

Step 4: View the 6RD tunnel configurations.

```
SG-6000(config)#show ip6in4 6rd-tunnel test

Name: test

Index: 11

Interface: ethernet0/0

IPv6-prefix: 1001:AABB::/32

IPv4-mask-length: 16

Border-relay-address: 0.0.0.0

Tunnel interface: tunnel1

IPv6-delegated-prefix: 1001:AABB:A08::/48 （The 6RD delegated prefix calculated by device）

Sub-tunnel Limit: 10
```

Step 5: Configure the IPv6 address and zone of the interface ethernet 0/1 of the Device B.

```
hostname(config)#1interface ethernet0/1

hostname(config-if-eth0/1)# zone trust

hostname(config-if-eth0/1)# ipv6 enable

hostname(config-if-eth0/1)# ipv6 address 2333:aabb::1/64

hostname(config-if-eth0/1)# exit
```

Step 6: Configure a route for tunnel.

```
hostname(config)# ip vrouter trust-vr

hostname(config-vrouter)# ipv6 route 1001:AABB::/32 tunnel1

hostname(config-vrouter)# exit
```

Step 7: Configure the policy.

```
hostname(config)# policy-global
hostname(config-policy)# rule id 1
Rule id 1 is created
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 8: Configure an address and default route for PC3.

Set the address to 2333:aabb::2/64 for PC3 , this address is in the same network segment as that of ethernet0/1 of Device B.

Note: The method for configuring IPv6 addresses and default route varies based on the operating system of your PC.

Result of Scenario 1

Step 1: Use the Ping command on Device to view the tunnel established between headquarters and branch A and their connectivity.

```
SG-6000# ping ipv6 1001:AABB:A09::1

Sending ICMPv6 packets to 1001:AABB:A09::1

Seq hop time(ms)

1 64 0.109

2 64 0.131

3 64 0.115

4 64 0.128

5 64 0.110

statistics:

5 packets sent, 5 received, 0% packet loss, time 4000ms

rtt min/avg/max/mdev = 0.109/0.118/0.131/0.015 ms
```

Step 2: View the session information of the tunnel.

```
SG-6000# show session tunnel

session: id 3407871, proto 41, flag 20, flag1 0, flag2 0, flag3 0, created 272719, life 64000, policy type 0,
policy default, app 0(Other) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/0)/200951): 220.119.10.9:0->220.119.10.5:0

flow1(18): tunnel session, tunnel_id: 4, valid
```

Result of Scenario 2

Step 1: Use the Ping command on Device to view the tunnel established between headquarters and branch B and their connectivity.

```
SG-6000# ping ipv6 2333:aabb::1

Sending ICMPv6 packets to 2333:aabb::1

Seq hop time(ms)

1 64 0.115

2 64 0.120

3 64 0.113

4 64 0.112

5 64 0.126

statistics:

5 packets sent, 5 received, 0% packet loss, time 3996ms

rtt min/avg/max/mdev = 0.112/0.117/0.126/0.008 ms
```

Step 2: View the session information of the tunnel.

```
SG-6000# show session tunnel

session: id 3407871, proto 41, flag 20, flag1 0, flag2 0, flag3 0, created 272719, life 64000, policy type 0,
policy default, app 0(Other) flag 0x0, auth_user_id 0, reverse_auth_user_id 0

flow0(32(ethernet0/0)/200951): 220.119.10.8:0->220.119.10.5:0

flow1(18): tunnel session, tunnel_id: 4, valid
```

Change Log

Cookbook V1

Release Date: January, 2015

Added the following cases:

1. " Using Security Policy to Allow Access to Another Zone" on Page 15 (Security Policy)
2. "Allowing Internet to Visit a Private Server Using DNAT" on Page 21 (DNAT)
3. "Allowing Private Network to Access Internet Using SNAT" on Page 26 (SNAT)
4. "Allowing the Internet Access via User Authentication" on Page 99 (User Authentication, WebAuth)
5. "Connection between Two Private Networks Using IPSec VPN (IKEv1)" on Page 147 (IPSec VPN)
6. "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 199 (SSL VPN, SCVPN)
7. " Ensuring Uninterrupted Connection Using HA" on Page 347 (High Availability, HA)
8. " QoS Control" on Page 369 (Quality of Service, QoS, Traffic Management)

Cookbook V2

Release Date: April, 2015

Added the following cases:

1. "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 390 (Abnormal Behavior Detection, ABD)
2. Finding Malware Attacks via Advanced Threat Detection (Advanced Threat Detection, ATD)

Cookbook V3

Release Date: July, 2015

Add the following cases:

1. "Decrypting HTTPS Traffic and Identifying the Encrypted Application" on Page 452 (SSL Proxy, Decryption, Encrytion)
2. "Using an iOS/Android Device to Remotely Access Intranet Services" on Page 223 (iOS, Android, Mobile, iPad, remote device, SSL VPN)
3. "Forensic Analysis " on Page 406
4. "Deploying Tap Mode to Monitor Network Traffic " on Page 48(Tap Mode)

Cookbook V4

Release Date: September, 2015

Add the following cases:

1. "Upgrading Firmware to Higher Version" on Page 5 (Upgrade)
2. "Allowing Remote Users (PC) to Access a Private Network Using L2TP over IPSec VPN" on Page 230 (L2TP VPN)
3. "Connection between Two Private Networks Using GRE over IPSec VPN" on Page 277 (GRE, IPSec VPN)

Cookbook V5

Release Date : January, 2017

Add the following cases:

1. "Protecting Intranet to Defend Attacks via Intrusion Prevention System" on Page 398(IPS)
2. "Outbound Link Load Balance" on Page 376(LLB)

Optimize the following cases:

1. "Protecting Internal Servers and Host to Defend Attack via Abnormal Behavior Detection" on Page 390(ABD)
2. Finding Malware Attacks via Advanced Threat Detection(ATD)

Cookbook V6

Release Date : October, 2017

Add the following cases:

1. "Allowing Remote Users (iOS/Android) to Access a Private Network Using L2TP over IPSec VPN" on Page 249 (L2TP VPN)

Cookbook V7

Release Date : August, 2018

Add the following cases:

1. " Using AD Polling for SSO" on Page 107 (Authentication)
2. " Allowing Internet Access via AD Polling" on Page 116(Authentication)
3. " Allowing Internet Access via AD Agent" on Page 127(Authentication)
4. "Connecting IPv6 and IPv4 Networks" on Page 463
5. "URL Filtering for HTTPS Traffic without the CA Certificate" on Page 456

Cookbook V8

Release Date : June, 2019

Add the following cases:

1. "Connection between Two Private Networks Using IPSec VPN (IKEv2)" on Page 160 (IPSec VPN)
2. "Upgrading Firmware to Higher Version in HA mode" on Page 9 (Upgrade)
3. "Configuring the Device to Communicate with Zabbix Using SNMP" on Page 31 (SNMP)

Cookbook V8.1

Release Date : November, 2019

Add the following cases:

1. "Connecting to Microsoft Azure Using Site-to-Site VPN" on Page 212 (IPSec VPN)

Cookbook V9

Release Date : October, 2020

Add the following cases:

1. " DNS Proxy" on Page 57 (DNS Proxy)
2. "Dynamically Manage Access Authority Via Radius Dynamic Authorization" on Page 38 （Authorization）
3. "Realizing Multicast Forwarding Through PIM-SM Multicast Protocol" on Page 75 （Routing, PIM）
4. "Realizing Multicast Forwarding Through PIM-SSM Multicast Protocol" on Page 84 （Routing, PIM）
5. Ensuring Uninterrupted Connection Using HA AA （HA）
6. " Allowing Internet Access via TS Agent" on Page 138 （Authentication）
7. " Configuring VXLAN Static Unicast Tunnel" on Page 293（VPN）
8. "Realizing FTP Service in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 474（IPv6）
9. "Realizing SIP Communication in IPv6-only or IPv4/IPv6 Hybrid Networks Using ALG" on Page 483 （IPv6）
10. "Realizing Dual-stack Host in IPv4 Network Accessing IPv6 Network Via ISATAP Tunnel" on Page 494 （IPv6）

Cookbook V10

Release Date : December, 2021

Add the following cases:

1. "Deploying HA Scenario for Multicast Forwarding Through PIM-SM" on Page 91 （Routing, PIM）
2. "Adding an SNAT Rule to StoneOS through NETCONF" on Page 63 (NETCONF)
3. "Allowing Remote Users (PC) to Access a Private Network Using L2TP and SSL VPN" on Page 264(SSL VPN L2TP VPN)
4. "Threat Intelligence Via Hillstone Cloud Service Platform" on Page 413（Hillstone Cloud Service Platform）

Optimize the following cases:

1. "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 199 (Add the scene of using the Two-Step Verification function and communicating through TCP.)

Cookbook V11

Release Date : January, 2023

Add the following cases:

1. "Binding the Log Processing Process and Database Storage Process to Core MAX" on Page 68 (Core MAX)
2. "Making Two Firewalls Working in Hot Standby Mode by Deploying them in HA Peer to Ensure the Continuity of Service " on Page 355（HA）
3. "Using Two Devices as Gateways to Forward Business Traffic and Back Up Each Other Based on HSVRP, which Ensures Uniterrupted Business Traffic" on Page 360（HA）
4. "Establishment of IPSec VPN Based on Certificate Authentication " on Page 173 (IPSec VPN)
5. "Realizing Dynamic Switch between IPSec Links Using IPSec VPN Smart Link" on Page 186 (IPSec VPN)
6. "Allowing Communication Between IPv6 networks by Configuring a 6RD Tunnel" on Page 497 (IPv6)
7. "Windows User Remotely Accessing Internal Server Through ZTNA" on Page 314 (ZTNA)
8. " Android User Remotely Accessing Internal Server Through ZTNA" on Page 335 (ZTNA)

Optimize the following cases:

1. " Ensuring Uninterrupted Connection Using HA" on Page 347（HA）

Cookbook V12

Release Date :May, 2024

Add the following cases:

1. "DHCP ZTP" on Page 71 （DHCP zero touch provisioning (ZTP) process）
2. "Windows User Accessing Internal Server by Using Internal Network Access via ZTNA" on Page 298 (ZTNA)
3. "Outbound Link Load Balance with Customizable SLA Metrics" on Page 381 (SLA, Quality of Service)
4. "Identifying IoT Assets to Enable Security Control of IoT by Using Built-in Docker" on Page 416 (IOT, Threat Prevention)
5. "Identifying IoT Assets to Enable Security Control by Deploying the Asset Identifying System on the VM" on Page 431 (IOT, Threat Prevention)

Optimize the following cases:

1. "Allowing Remote Users to Access a Private Network Using SSL VPN" on Page 199 （SSL VPN）
2. "Windows User Remotely Accessing Internal Server Through ZTNA" on Page 314 (ZTNA)
3. " Android User Remotely Accessing Internal Server Through ZTNA" on Page 335 (ZTNA)
4. "Connection between Two Private Networks Using IPSec VPN (IKEv2)" on Page 160

This book is updated on requirement, not periodically.

The current version you are using is based on StoneOS 5.5R11.