Hillstone Networks

[[[未定义的变量General.F User-GuideTitle]]]

Version 5.5R11F



New Features Guide Introduction

New Features Guide for StoneOS 5.5R11 F Releases is a supplementary note for StoneOS manual. This new features guide is based on StoneOS 5.5R11 manual, added the new functions or modifications for F releases.

- "StoneOS 5.5R11F3" on Page 3
- "StoneOS 5.5R11F2" on Page 573
- "StoneOS 5.5R11F1" on Page 896

Distributed Devices Support to Send Monitor Data such as Threat Logs to Cloud Platform and iSource

WebUI

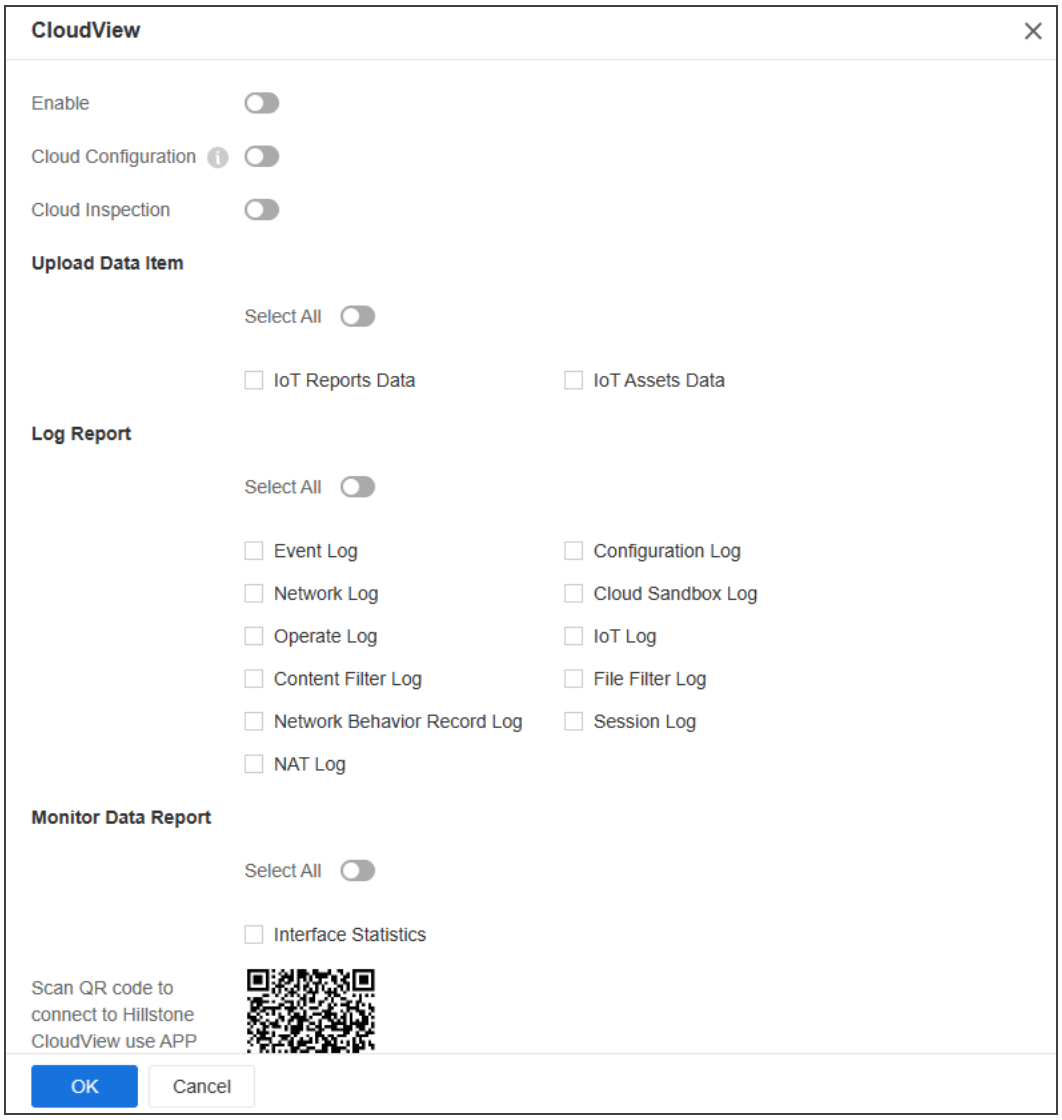
Configuring CloudView

CloudView can be used to visualize device information, traffic data, threat events, and system logs that are uploaded to the cloud platform.

To configure CloudView, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.

2. Click **CloudView**.



3. In this panel, configure the following options.

Option	Description
Enable	Click the **Enable** button to enable the Hillstone CloudView service.

Option	Description
Cloud Configuration	You can configure this function only when CloudView is enabled. Click the enable button to allow CloudView to send configuration to the device. The system will load the real-time configuration sent by CloudView. • PTF Dynamic IP Blacklist: Log in to CloudView to send the configuration of the PTF dynamic IP blacklist to the root VSYS of the device. Both IPv4 and IPv6 addresses are supported. You can also specify the virtual router to take effect as well as the block duration. When the system receives the configuration task from CloucView, corresponding dynamic IP blacklist entries, configuration logs, and operation logs are generated.
Cloud Inspection	Click the **Enable** button to enable the cloud inspection function and upload the collected inspection data to the cloud service platform. With the cloud inspection function, the device can receive and execute the inspection instructions from the cloud, and upload the collected inspection data to the cloud service platform, which enables you to carry out real-time monitoring and management on the cloud anytime and anywhere.
Upload Data Item	Select the data item that you want to upload to the cloud platform, including the IoT reports data, and IoT Assets data. If you enable Select All, all IoT data are uploaded.
Log Report	Select the type of logs that you want to upload to the cloud plat-

Option	Description
	form, including event logs, threat logs, configuration logs, network logs, cloud sandbox logs, operation logs, content filter logs, file filter logs, network behavior record logs, session logs, and NAT logs. If you enable Select All, all logs are uploaded. Note: • For X series devicesK6580/K9180 devices, you are not allowed to upload threat logs to the cloud platform. • The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.
Monitor Data Report	Select the monitor data type that you want to upload to the cloud platform, including the traffic ranking, session ranking, URL ranking, device information, VPN statistics, and interface statistics (including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface in the device). If you enable Select All, all monitor data is uploaded. **Notes:** For X series devicesK6580/K9180 devices, you are only allowed to upload interface statistics to the cloud platform.
Scan QR code to connect to	Scan the QR code using a QR reader app on your smartphone or mobile device to connect to Hillstone CloudView via APP.

Option	Description
Hillstone CloudView use APP	
Visit CloudView	Click the button to visit CloudView.

4. Click **OK**.

For more information, refer to the **System > Connecting to Hillstone Cloud Service Platform** topic in *StoneOS_WebUI_User_Guide*. FR 35753

Configuring the Data Types Sent to iSource

To configure the data types sent to iSource after the device is connected to iSource, take the following steps:

1. Select **System > Extended Services**. In the **Connect to Security Operations Platform**, click  in the lower-left corner.

2. In the **Data Upload Configuration** section, configure the following options as needed:

   - Turn on the switch next to Threat Log to send threat logs to iSource. By default, this feature is disabled.
   - Turn on the switch next to Forensic Pcap to send threat-related evidential packets captured by the device to iSource. By default, this feature is disabled.
   - Turn on the switch next to IoT Asset Monitor to send detected IoT asset data to iSource.

3. Click **OK**.

Notes:

- A-series devices that are installed with SSD , K-series devices (except K6580/K9180) that are installed with SSDCloudEdgesupport to upload threat-related evidential packets captured by the device to iSource.

For more information, refer to the **System** > **Connecting to iSource** topic in *StoneOS_WebUI_User_Guide*. FR 35753

CLI

Enabling Log Report

To upload log data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

- **log-cf** -Specifies to upload content filter logs of the device to the cloud platform.
- **log-config** - Specifies to upload configuration logs of the device to the cloud platform.
- **log-dlp** - Specifies to upload file content logs of the device to the cloud platform.
- **log-event** - Specifies to upload event logs of the device to the cloud platform. By default, the upload interval is 10 minutes. Before you enable the function, make sure that the device is enabled with the **logging event on** function.
- **log-iot** - Specifies to upload IoT logs of the device to the cloud platform.
- **log-nat** - Specifies to upload NAT logs of the device to the cloud platform.
- **log-nbr** - Specifies to upload network behavior audit logs of the device to the cloud platform.
- **log-network** - Specifies to upload network logs of the device to the cloud platform.

- **log-operat** - Specifies to upload operation logs of the device to the cloud platform.
- **log-sandbox** - Specifies to upload cloud sandbox logs of the device to the cloud platform.
- **log-session** - Specifies to upload session logs of the device to the cloud platform.
- **threat-event** - Specifies to upload threat events of the device to the cloud platform. By default, the upload interval is 60 minutes.
- **all** - Specifies to upload all monitoring data above of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

Notes:

- The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.

Enabling Monitoring Data Uploading

To upload monitoring data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}

- **traffic-rank** -Specifies to upload the traffic ranking data of the device to the cloud platform.
- **stats-session** - Specifies to upload the session ranking data of the device to the cloud platform.
- **stats-url-rank** - Specifies to upload the URL ranking data of the device to the cloud platform.

- **stats-device** -Specifies to upload the device information data of the device to the cloud platform.
- **scvpn-user** - Specifies to upload the VPN statistics of the device to the cloud platform.
- **stats-interface** - Specifies to upload the interface statistics of the device to the cloud platform, including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface.
- **all** - Specifies to upload all monitoring data of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}

For more information, refer to the **System Management** > **Connecting to Hillstone Cloud Service Platform** topic in *StoneOS_CLI_User_Guide*. FR 35753

Configuring the Data Types Sent to iSource

To configure data types sent to iSource, in iSource configuration mode, use the following command:

upload-type {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**}

- **all** – Specifies to send all types of data to iSource.
- **forensic-pcap** – Specifies to send threat-related evidential packets captured by the device to iSource.
- **iot-monitor-property** – Specifies to send detected IoT asset data to iSource.
- **threat-event** – Specifies to send threat logs to iSource

In iSource configuration mode, use the **no upload-type** {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**} command to cancel specifying the data types sent to iSource.

Notes:

- A-series devices that are installed with SSD , K-series devices (except K6580/K9180) that are installed with SSDCloudEdgesupport to upload threat-related evidential packets captured by the device to iSource.

For more information, refer to the **System Management** > **Connecting to iSource** topic in *StoneOS_CLI_User_Guide*. FR 35753

Supporting to Obtain the Number of Concurrent Connections and New Connection Rate of Current NAT Sessions of Device by Using SNMP

MIB

HILLSTONE-SYSTEM-MIB

The following tables is the parsing results of HILLSTONE-SYSTEM-MIB.

Name	OID	Value
sysSerialNumber	.1.3.6.1.4.1.28557.2.2.1.1	Data type: String Description: Product serial number
sysSoftware	.1.3.6.1.4.1.28557.2.2.1.2	Data type: String Description: Software version
sysCPU	.1.3.6.1.4.1.28557.2.2.1.3	Data type: Integer Description: CPU utilization
sysTotalMemory	.1.3.6.1.4.1.28557.2.2.1.4	Data type:

Name	OID	Value
		Gauge32 Description: Total memory
sysCurMemory	.1.3.6.1.4.1.28557.2.2.1.5	Data type: Gauge32 Description: Used memory
sysTotalSession	.1.3.6.1.4.1.28557.2.2.1.6	Data type: Counter Description: Maximum session number of the system
sysCurSession	.1.3.6.1.4.1.28557.2.2.1.7	Data type: Gauge32 Description: Active session number
sysHAStatus	.1.3.6.1.4.1.28557.2.2.1.8	Data type: Integer Description: HA status • 0 - Invalid • 1 - Started • 2 - Hello • 3 - Backup device • 4 - Primary device

Name	OID	Value
		• 15 - Failure
sysSnmpStackStatus	.1.3.6.1.4.1.28557.2.2.1.9	Data type: Integer Description: SNMP running status
sysTr069StackStatus	.1.3.6.1.4.1.28557.2.2.1.10	Data type: Integer Description: TR069 running status
sysVedorOUI	.1.3.6.1.4.1.28557.2.2.1.11	Data type: String Description: Provider name
sysLogStackStatus	.1.3.6.1.4.1.28557.2.2.1.12	Data type: Integer Description: Syslog running status
sysLogServerAddress1	.1.3.6.1.4.1.28557.2.2.1.13	Data type: String Description: Syslog server IP address 1
sysLogServerAddress2	.1.3.6.1.4.1.28557.2.2.1.14	Data type: String Description: Syslog server IP address 2
sysDeviceReloadAction	.1.3.6.1.4.1.28557.2.2.1.15	Data type: Integer Data type: String Description: Device reloading. When the value equals 2, the device

Name	OID	Value
		will reboot.
sysStatisticsPeriod	.1.3.6.1.4.1.28557.2.2.1.16	Data type: Integer Description: Statistic interval. Default value is 24 hours.
sysMemRatio	.1.3.6.1.4.1.28557.2.2.1.17	Data type: Gauge32 Description: Memory usage ratio.
sysSessionRampupRate	.1.3.6.1.4.1.28557.2.2.1.18	Data type: Gauge32 Description: New session connection ratio(used for Statistics).
sysOverallThroughput	.1.3.6.1.4.1.28557.2.2.1.19	Data type: Counter64 Description: Root VSYS throughput.
sysCTWapStat	.1.3.6.1.4.1.28557.2.2.1.20	Data type: String Description: WAP status information
sysRamupRate	.1.3.6.1.4.1.28557.2.2.1.21	Data type: Integer Description: New session connection ratio(not related to Statistics).

Name	OID	Value
sysL4SynCheckDrop	.1.3.6.1.4.1.28557.2.2.1.22	Data type: Integer Description: Number of the dropped packets during TCP snchronous message error
sys L4SynBitCheckDrop	.1.3.6.1.4.1.28557.2.2.1.23	Data type: Integer Description: Number of the dropped packets during syc bit of TCP message error
sysL4SeqCheckDrop	.1.3.6.1.4.1.28557.2.2.1.24	Data type: Integer Description: Number of the dropped packets during serial number error
sysL4HwCPUError	.1.3.6.1.4.1.28557.2.2.1.25	Data type: Integer Description: Number of the dropped packets during Octeon chip error
sysHistoryMaxSessNum	.1.3.6.1.4.1.28557.2.2.1.26	Data type: Gauge32 Description: Maximum number of sessions in history.
sysTCPSessNum	.1.3.6.1.4.1.28557.2.2.1.27	Data type: Gauge32

Name	OID	Value
		Description: Number of current TCP sessions.
sysUDPSessNum	.1.3.6.1.4.1.28557.2.2.1.28	Data type: Gauge32 Description: Number of current UDP sessions.
sysICMPSessNum	.1.3.6.1.4.1.28557.2.2.1.29	Data type: Gauge32 Description: Number of current ICMP sessions.
sysCurSessionIPv4	.1.3.6.1.4.1.28557.2.2.1.31	Data type: Gauge32 Description: Total number of concurrent IPv4 sessions
sysCurSessionIPv6	.1.3.6.1.4.1.28557.2.2.1.32	Data type: Gauge32 Description: Total number of concurrent IPv6 sessions
sysRampupRateIPv4	.1.3.6.1.4.1.28557.2.2.1.33	Data type: Integer Description: Total rate of new IPv4 sessions

Name	OID	Value
sysRampupRateIPv6	.1.3.6.1.4.1.28557.2.2.1.34	Data type: Integer Description: Total rate of new IPv6 sessions
sysPeerHAStatus	.1.3.6.1.4.1.28557.2.2.1.36	Data type: Integer Description: HA status of the peer device • 0 - none • 1 - init • 2 - hello • 3 - backup • 4 - master • 15 – failed
sysHAGroupStatus	.1.3.6.1.4.1.28557.2.2.1.37	Data type: Integer Description: HA status of the master device and backup device in the HA group • 0 - normal • 1 - abnormal
sysHAStatusChangeTimes	.1.3.6.1.4.1.28557.2.2.1.38	Data type: Integer

Name	OID	Value
		Description: Number of master/backup status changes in the HA group
sysOverallIPv4Throughput	.1.3.6.1.4.1.28557.2.2.1.39	Data type: Counter64 Description: IPv4 throughout of root VSYS
sysOverallIPv6Throughput	.1.3.6.1.4.1.28557.2.2.1.40	Data type: Counter64 Description: IPv6 throughout of root VSYS
sysCurSessionNat	.1.3.6.1.4.1.28557.2.2.1.42	Data type: Gauge32 Description: Number of concurrent connections of current NAT sessions
sysRampupRateNat	.1.3.6.1.4.1.28557.2.2.1.43	Data type: Gauge32 Description: New connection rate of current NAT sessions
sysTopAppthroughputTable: Throughput information of the TOP application		
hillstoneAppIndex	.1.3.6.1.4.1.28557.2.2.1.30.1.1	Data type: Integer Description: The index of the TOP 10 Application.

Name	OID	Value
hillstoneAppthroughput	.1.3.6.1.4.1.28557.2.2.1.30.1.2	Data type: DisplayString Description: The throughput of the TOP 10 application in last 24 hours.
sysPendingSessionQueueFullDrop	.1.3.6.1.4.1.28557.2.2.1.35	Data type: Integer Description: Number of packets dropped caused by full cache queue of sessions.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 41159

Supporting Publishing RA Messages Containing Route Option Information

CLI

IPv6 Neighbor Discovery Protocol Configuration

Neighbor Discovery Protocol (NDP) is a fundamental component of the IPv6 protocol. It operates at the link layer and is responsible for discovering other nodes on the link, determining the link-layer addresses of other nodes, finding available routers, and maintaining reachability information to other nodes. In addition to performing all the functions of the Address Resolution Protocol (ARP), Router Discovery, and Redirect Message in IPv4, it also provides advanced functions such as Neighbor Unreachability Detection (NUD).

The current version of StoneOS supports the following protocol-related configurations:

- Configuring DAD function
- Specifying reachable time
- Configuring RA message parameters
- Specifying the RA message transmission interval
- Specifying the RA message lifetime
- Configure RA message publication to include route option information
- Specifying DRP
- Configuring the LAN port RA message transmission status
- Adding/Deleting static IPv6 neighbor cache entries

Configuring RA Message Parameters

Router Advertisement (RA) messages are briefly referred to as RA messages. Routers periodically send RA messages to announce their availability and link and Internet parameters for configuration, including the network address prefix in use, the recommended Hop Limit value, the local MTU value, and labels for the type of auto-configuration nodes should use, as well as DNS configuration options, etc.

.....

Configuring RA Message Publication to Include Route Option Information

Application Scenarios

When there are multiple routers in the link where the host is located, the host needs to select the forwarding router based on the destination address of the packet. In this case, the firewall device can improve the host's ability to choose an appropriate forwarding router by sending RA messages containing specific routing options to the host.

After the host receives an RA message containing route option information, it will update its routing table. When the host sends packets to other devices, it queries the route option information in this list to select an appropriate route for sending the packet.

By default, the firewall's RA messages to the host do not include route option information.

Prerequisites

- Before executing this command, you need to first enable the IPv6 function on the interface using the **ipv6 enable** command in interface configuration mode.
- By default, the device does not send RA messages. Therefore, if you want to advertise route options to hosts, you need to first enable the device to send RA messages using the **no ipv6 nd ra suppress** command in interface configuration mode.

Note

- On the same interface, the system supports a maximum of 17 route option configurations.

Configuration Method

To configure RA message publication to include route option information, in interface configuration mode, use the following commands:

ipv6 nd ra route-information *ipv6-address-prefix prefix-length* **lifetime***route-lifetime***preference** {**high** | **medium** | **low**}

- *ipv6-address-prefix* - Specifies the IPv6 address prefix for the route, in the format X:X:X:X::X.
- *prefix-length* - Specifies the prefix length of the route. The value range is 0 to 128.
- **lifetime***route-lifetime* - Specifies the lifetime of the route, after which the route will expire. The unit is seconds, with a value range of 0 to 4294967295.
- **preference** {**high** | **medium** | **low**} - Specifies the priority of the route as high (**high**), medium (**medium**), or low (**low**). When the host receives multiple routing options with the same prefix, it selects the router with the highest priority to send the packet.

In interface configuration mode, use the **no ipv6 nd ra route-information** *ipv6-address-prefix prefix-length* command to cancel the configuration that includes route option information in RA messages.

Viewing the Routing Options Configuration of the Interface

To view the interface routing options configuration, use the following command in any mode:

show ipv6 ra-route-information [**interface** *interface-name*]

- **interface** *interface-name* - View the configured routing options for the specified interface. If not configured, it indicates viewing the configured routing options for all interfaces in the system.

The following is an example of a return result:

```
hostname#show ipv6 ra-route-information interface
ethernet0/2:
Prefix : 2001:DB8::2 Length : 64
RouteLifetime : 1800 Preference : low
(The above return result indicates: A route option with a destination address of 2001:DB8::2/64, a lifetime of 1800 seconds, and high priority has been configured on the ethernet0/2 interface. The RA messages published from the ethernet0/2 interface will include this route option information.)
```

For more information, refer to the **IPv6 > IPv6 Neighbor Discovery Protocol Configuration** section in the *StoneOS CLI User Guide*. FR 43721

Optimizing Memory Allocation By Reducing The Maximum Concurrent Connections

CLI

Optimizing Memory Allocation By Reducing The Maximum Concurrent Connections

Device Supported: :

- All models of A series devices
- All models of B series devices
- K series some devices (excluding K20803/K9180)

Notes: This function involves memory allocation and may affect the normal operation of services. You need to configure it under the guidance of Hillstone technical support personnel.

In the firewall system, CP (Control Plane) memory is used to store data generated by system configuration and management, and DP (Data Plane) memory is used to store data generated by system traffic forwarding and services.

If you enable too many security functions (such as IPS, AV, etc.) or create too many statistics sets in the device, it may consume a large amount of CP memory. For devices with smaller memory, this might affect the normal startup and operation of the device due to insufficient CP memory. To address this, when such devices are in a low-traffic period, you need to reduce the maximum concurrent connections to optimize memory allocation. Reducing the maximum concurrent connections will free up some DP memory, which will then be allocated to CP memory, thus increasing CP memory to avoid device issues caused by insufficient CP memory.

Optimize memory allocation by reducing the maximum concurrent connections. In any mode, use the following command:

exec session-adjust *value* **cp**

- *value* - Reduce the maximum concurrent connections of the device to the specified value to free up some DP memory, which will be allocated to CP memory. The range of maximum concurrent connections varies for different devices. You can enter the **exec session-adjust** command and press the Tab key to view the range of maximum concurrent connections for the current device.

For devices that have already adjusted memory allocation, if you encounter a business peak period, to avoid affecting the normal operation of services, you can use the **exec session-adjust reset** command to restore the default maximum concurrent connections. At this time, the CP memory size will also be restored to the default value.

Notes: After restarting the device, the configuration takes effect.

For more information, refer to the **System Management** > **The Maximum Concurrent Sessions** section in the *StoneOS CLI User Guide*. FR 37551

Optimizing the Configuration and Effective Method of URL Category and Keyword Category

WebUI

Configuring URL Filtering

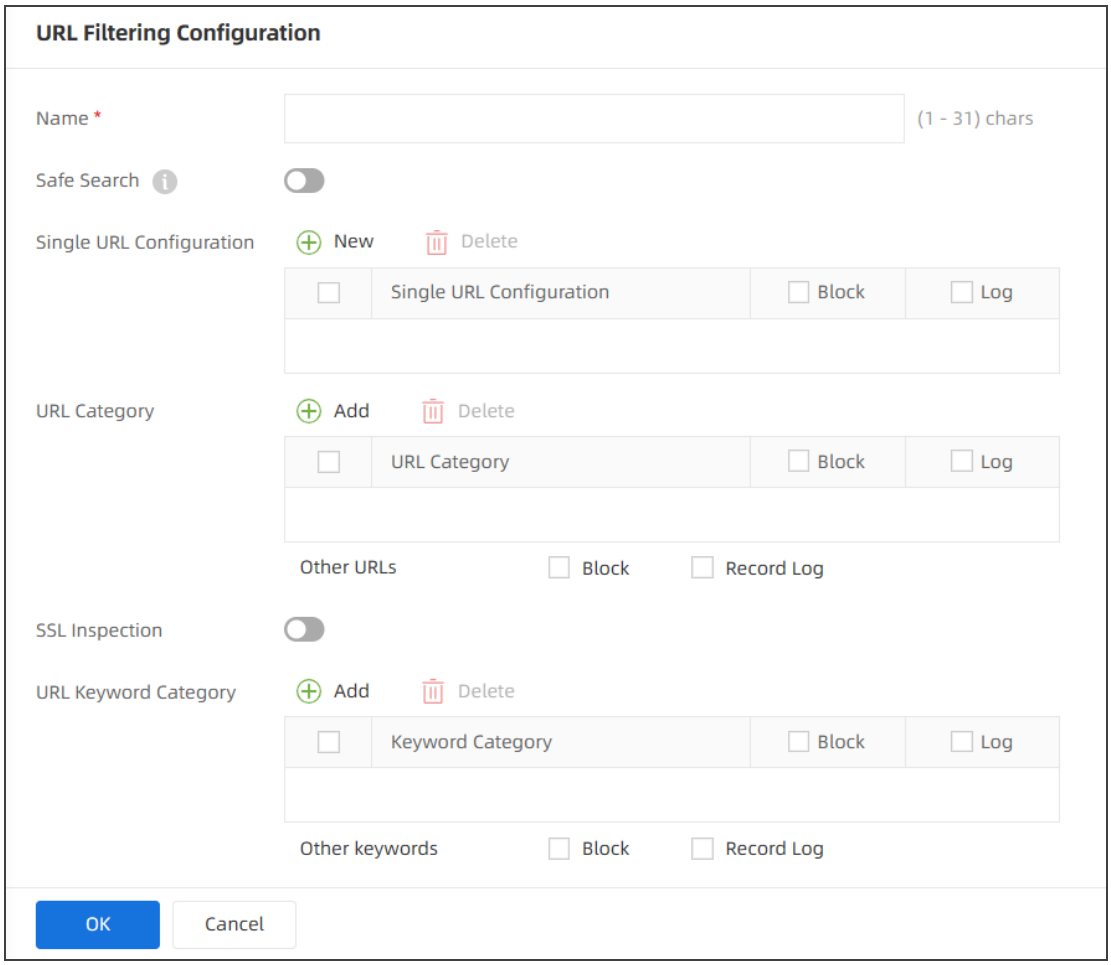
Configuring URL filtering contains two parts:

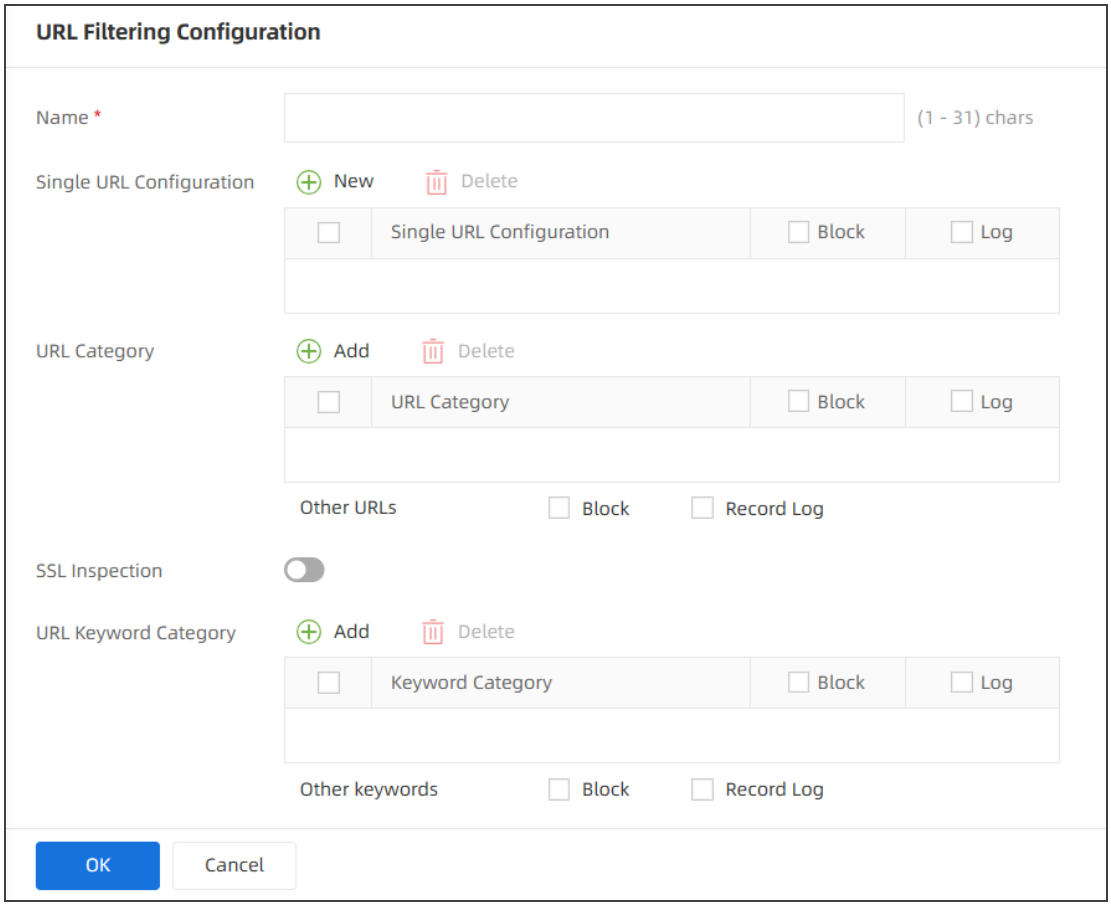
- Create a URL filtering rule
- Bind a URL filtering rule to a security zone or policy rule

Creating a URL filtering rule

1. Select **Object > URL Filtering > Profile**.

2. Click **New**.


URL Filtering Configuration
Name *
(1 - 31) chars
Safe Search
Single URL Configuration
New
Delete
Single URL Configuration
Block
Log
URL Category
Add
Delete
URL Category
Block
Log
Other URLs
Block
Record Log
SSL Inspection
URL Keyword Category
Add
Delete
Keyword Category
Block
Log
Other keywords
Block
Record Log
OK
Cancel



Configure the following options.

Option	Description
Name	Specifies the name of the rule. You can configure the same URL filtering rule name in different VSYSs.
Safe Search	Many search engines, such as Google, Bing, Yahoo!, Yandex, and YouTube, all have a "SafeSearch" setting, which can filter adult content, and then return search results at different levels based on the setting. The system supports the safe search function in the URL filtering Profile to detect the "SafeSearch" setting of search engine and perform corresponding control actions. Select the

Option	Description
	Enable check box to enable the safe search function to detect the settings of the search engine's “SafeSearch" and perform corresponding control actions. **Notes:** • The safe search function only can be used in the following search engines currently: Google, Bing, Yahoo!, Yandex, and YouTube. • The safe search function can only be used in combination with the SSL proxy function because the search engine uses the HTTPS protocol. Therefore, when “SafeSearch” is enabled, enable the SSL proxy function for the policy rule that is bound with the URL filter profile. • To ensure the valid "SafeSearch" function of Google, you need to configure policy rules to block the UDP 80 and UDP 443 ports.
Control Action	Specifies the safe search action. o Block: Selects the check box to specify the action as block. When the "SafeSearch" setting of the search engine is not set, users will be prevented from accessing the search page and a warning page will pop up which provides users with the link for "SafeSearch" setting. o Enforce: Selects the check box to specify the action as enforce. When the "SafeSearch" setting of the search engine is not set, the system will force it to the

Option	Description
	“strict” level.

3. In the **URL Category** part to configure the URL category control type for URL filtering rules to control the access to some certain category of website.

In the URL Category part, configure the following options.

Option	Description
New	Creates a new URL category. For more information about URL categories, see "StoneOS 5.5R11F3" on Page 3.
Edit	Selects a URL category from the list, and click **Edit** to edit the selected URL category. **URL Keyword Category** controls the access to the website whose URL contains the specific keywords. Click the **URL Keyword Category** option to configure. The options are: • New: Creates new keyword categories. For more information about keyword category, see "StoneOS 5.5R11F3" on Page 3. • Edit: Select a URL keyword category from the list, and click **Edit** to edit the selected URL keyword categories. • Keyword category: Shows the name of the configured keyword categories. • Block: Selects the check box to block access to the website whose URL contains the specified keywords. • Log: Selects the check box to log the access to the website

Option	Description
	whose URL contains the specified keywords. • Other URLs: Specifies the actions to the URLs that do not contain the keywords in the list, including **Block Access** and **Record Log**.
URL category	Shows the name of pre-defined and user-defined URL categories in the VSYS.
Block	Selects the check box to block access to the corresponding URL category.
Log	Selects the check box to log access to the corresponding URL category.
Other URLs	Specifies the actions to the URLs that are not in the list, including **Block Access** and **Record Log**.
URL Category	Controls user access to websites of specified URL categories. **Notes:** When a URL matches multiple URL categories, the system will match based on the "type" of the URL category, and ultimately execute the configuration with the highest priority. Type priority: Custom URL categories in the list > Pre-defined URL categories in the list > All URLs outside the list. • Add: Click **Add**, search for and add the required URL categories on the **URL Category** page. You can also click ⊕

Option	Description
	to create a URL category. For more information, see the section on creating a URL category. • Block: Select the checkbox to prevent access to websites of the specified URL category. • Record Log: Select the checkbox to log the behavior of accessing websites of specified URL categories. • Delete: Select URL categories, click **Delete** to batch delete the specified URL categories. • All URLs outside the list: Specifies the control actions for all URLs that do not fall into the URL categories defined in the URL filtering template, including "Block" and "Log".
SSL inspection	Select the **Enable** button to enable SSL negotiation packets inspection. For HTTPS traffic, the system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this function is configured. Then, the system will perform URL filtering in accordance with the domain name. If SSL proxy is configured at the same time, SSL negotiation packets inspection method will be preferred for URL filtering.
URL keyword category	Control user access to websites containing specified URL keyword categories. **Notes:** When a URL matches multiple URL keyword categories, the system first matches according to the "type"

Option	Description
	of the keyword category, then matches according to the "control action," and ultimately executes the configuration with the highest priority. The priorities are as follows: • Type priority: Custom keyword categories in the list > Predefined keyword categories in the list > All keywords outside the list. • Control action priority: Block and log > Block only > Log only > Neither block nor log. • Add: Click the "Add" button to search for and add the required keyword categories on the <URL Keyword Category> page. Alternatively, click the  button to create a new keyword category. Refer to the Configure Keyword Categories section for related configurations. • Block: Check the checkbox to block websites containing the specified keywords in the URL. • Log recording: Check the checkbox to log actions for websites with the corresponding keywords in the URL. • Delete: Select the keyword categories and click the "Delete" button to batch delete the specified keyword categories. • All keywords outside the list: Specify control actions for websites that do not contain keywords configured in the

Option	Description
	URL filtering template, including "block" and "log".

4. In the **URL Keyword Category** part to configure the URL keyword category control type for URL filtering rules to control the access to the website whose URL contains the specific keywords.

   In the URL Keyword Category part, configure the following options.

Option	Description
New	Creates new keyword categories. The system supports predefined keyword categories and custom keyword categories. For more information about keyword category, see "StoneOS 5.5R11F3" on Page 3.
Edit	Select a URL keyword category from the list, and click **Edit** to edit the selected URL keyword categories.
Keyword category	Shows the name of the configured keyword categories.
Block	Selects the check box to block access to the website whose URL contains the specified keywords.
Log	Selects the check box to log the access to the website whose URL contains the specified keywords.
Other URLs	Specifies the actions to the URLs that do not contain the keywords in the list, including **Block Access** and **Record Log**.

5. Click **OK** to save the settings.

Notes: The control type of a URL filtering rule can configure both the URL category and the URL keyword category.

For more information, refer to the **Object** > **URL Filtering** > **Configure URL Filtering** section in the *StoneOS WebUI User Guide*. FR 44695

Supporting to Configure Start Time and Expire Time for a Single Policy

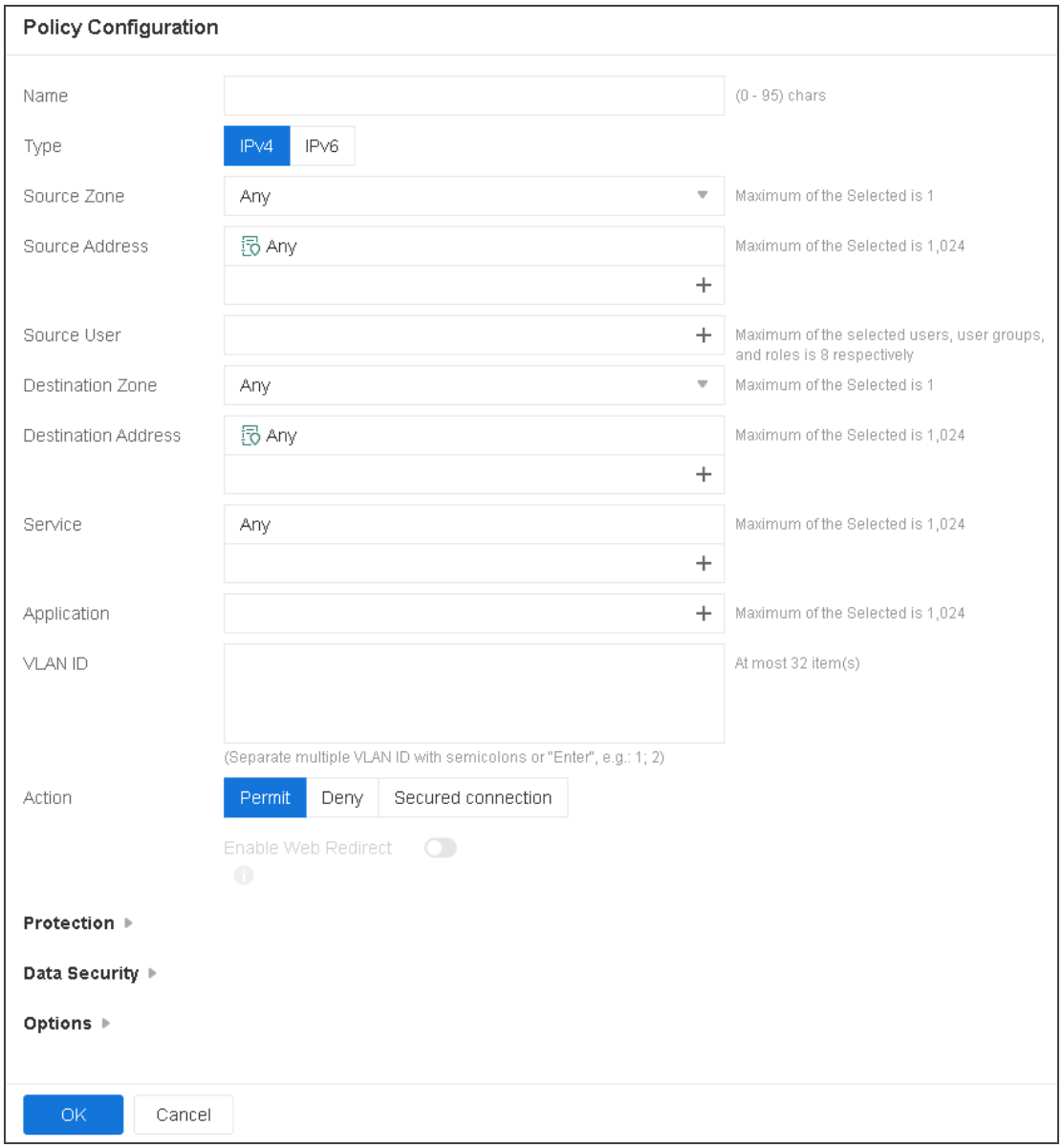
WebUI

Configuring a Security Policy Rule

To configure a security policy rule, take the following steps:

1. Select **Policy > Security Policy > Policy**.

2. At the top-left corner, click **New** to open the **Policy Configuration** page.



Configure the corresponding options.

Option	Description
Name	Type the name of the security policy.

Option	Description
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware can configure the IPv6 type. If IPv6 is selected, all of the IPv6/-prefix, IP range, and addressbook should be configured in the IPv6 format.
Source Zone	Specifies a source zone. In the single-zone mode, select a zone from the **Source Zone** dropdown list. If the multi-zone mode is enabled, take the following steps: 1. Click **Source Zone** to go to the pop-out Zone list. 2. Click the zones you need. You can select up to 16 zones. 3. Click **OK**. You can also perform the following operations: • When selecting the zones, you can click ⊕ to create new zones. • Any is the default zone. Enable **Any**to restore to the default.
Source Address	Specifies the source addresses. 1. Click **Address** to select an address type from the **Address** dialog. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane.

Option	Description
	4. After adding the desired addresses, click **Close** to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ icon to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • The default address configuration is any. Enable **Any** to restore the configuration to this default one.
Source Device	Specifies the source device of the policy rule.

Option	Description
	1. Click **Source Device**. The dialog box displays existing device objects. 2. Select one or more device objects. At most 8 device objects can be selected. 3. Click **Close**. You can also perform the following operations: • When you select a device object, you can click ⊕ to create one. • When you select a device object, you can click ▼ in the search box to search for device objects by device name, manufacturer, type, model, OS family, and OS version.
Destination Zone	Specifies a destination zone. In the single-zone mode, select a zone from the **Destination Zone** dropdown list. If the multi-zone mode is enabled, take the following steps: You can also perform the following operations: • When selecting the zones, you can click ⊕ to create new zones. • Any is the default zone. Enable **Any** to restore to the default.
Destination Address	Specifies the destination addresses. 1. Click **Address** to select an address type from the **Address**

Option	Description
	dialog. 2. Select or type the destination addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the destination address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ icon to create a new address entry. • You can click ▾ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address mem-

Option	Description
	ber whose hostname is aaa may be matched. • The default address configuration is any. Enable **Any** to restore to the default.
Destination Device	Specifies the destination device of the policy rule. 1. Click **Destination Device**. The dialog box displays existing device objects. 2. Select one or more device objects. At most 8 device objects can be selected. 3. Click **Close**. You can also perform the following operations: • When you select a device object, you can click ⊕ to create one. • When you select a device object, you can click ▼ in the search box to search for device objects by device name, manufacturer, type, model, OS family, and OS version.
Domain	Specifies the domain/host book. The domain, destination address, and application cannot be configured at the same time. 1. Click **Domain**, select a type: Domain, Host Book. 2. Select a domain/host book to add it to the left pane. • If Domain is selected, you need to enter a domain name and click **Add**. At most 1,024 domain names

Option	Description
	can be added. • If Host Book is selected, you can select a host book. At most 8 host books can be added. You can also search for host books based on keyword or click ⊕ to create a host book. 3. After adding the desired domains/host books, click **Close**. Note: After you specify the domain/host book, the policy rule is not used for redundancy check.
User	Specifies a role, user or user group for the security policy rule. 1. Click **User** to select the AAA server where the users and user groups reside. To specify a role, select **Role** from the **AAA Server/Role** drop-down list. 2. Based on the type of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click the selected users/user groups/roles to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the user configuration.
Service	Specifies a service or service group. 1. From the **Service** drop-down menu, select a type: Service,

Option	Description
	Service Group. 2. You can search the desired service/service group, expand the service/service group list. If Service is selected, you can click next to the search box to filter services by keyword, name, and protocol type of service. 3. After selecting the desired services/service groups, click the selected services/service groups to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the service configuration. You can also perform other operations: • To add a new service or service group, click icon. • The default service configuration is any. Enable **Any** to restore to the default. Specifies a service rule. When configuring the service rule of the policy rule, you can add a predefined or user-defined service that have been configured in the service book. When the required service does not exist in the service book, the administrator can specify the protocol type and port number of the service by configuring the service rules, thus simplifying the configuration steps of the policy. Specify a protocol type for the user-defined service. The available

Option	Description
	options include TCP, UDP, ICMP, SCTP and Others. If needed, you can add multiple service items. The parameters for the protocol types are described as follows: 1. From the **Service** drop-down menu, select a type: Service Rule. 2. From the **Protocol Type**drop-down menu, select a protocol type: TCP, UDP, ICMP, ICMPv6 and All. The parameters for the protocol types are described as follows: **TCP/UDP**: • Destination port: • Min - Specifies the minimum port number of the specified service rule. • Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535. • Source port: • Min - Specifies the minimum port number of the specified service rule. • Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535.

Option	Description
	Notes: • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. ICMP: • Type: Specifies an ICMP type for the service rule. The value range is 0（Echp-Reply）, 3（Destination-Unreachable）, 4（Source Quench）, 5（Redirect）, 8（Echo）, 11（Time Exceeded）, 12（Parameter Problem）, 13（Timestamp）, 14（Timestamp Reply）, 15（Information Request）, 16（Information Reply）, 17（Address Mask Request）, 18（Address Mask Reply）, 30（Traceroute）, 31（Datagram Conversion Error）, 32（Mobile Host Redirect）, 33（IPv6 Where-Are-You）, 34（IPv6 I-Am-Here）, 35（Mobile Registration Request）, 36（Mobile Registration Reply）. • Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 15,

Option	Description
	the default value is : min code - 0, max code - 15. Notes: • The minimum code cannot exceed the maximum code. • If "Max " is not configured, system will use "Min" as the single code. ICMPv6: • Type: Specifies an ICMPv6 type for the service rule. The value range is 1（Dest-Unreachable）, 2（Packet Too Big）, 3（Time Exceeded）, 4（Parameter Problem）, 5-99 (Unallocated Error message), 100（Private experimentation）, 101（Private experimentation）, 102-126 (Unallocated Error message), 127（Reserved for expansion of ICMPv6 error message）, 128（Echo Request）, 129（Echo Reply）, 130（Multicast Listener Query）, 131（Multicast Listener Report）, 132（Multicast Listener Done）, 133（Router Solicitation）, 134（Router Advertisement）, 135（Neighbor Solicitation）, 136（Neighbor Advertisement）, 137（Redirect Message）, 138（Router Renumbering）, 139（ICMP Node Information Query）, 140（ICMP Node Inform-

Option	Description
	ation Response），141（Inverse Neighbor Discovery Solicitation Message），142（Inverse Neighbor Discovery Advertisement Message），143（Version 2 Multicast Listener Report），144（Home Agent Address Discovery Request Massage），145（Home Agent Address Discovery Reply Massage），146（Mobile Prefix Solicitation），147（Mobile Prefix Advertisement），148（Certification Path Solicitation Message），149（Certification Path Advertisement Message），150（ICMP message utilized by experimental mobility protocols such as Seamoby），151（Multicast Router Advertisement），152（Multicast Router Solicitation），153（Multicast Router Termination），154（FMIPv6 Messages），200（Private experimentation），201（Private experimentation）and 255（Reserved for expansion of ICMPv6 informational）. • Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 255, the default value is : min code - 0, max code - 255. SCTP: • Destination port ◦ Min- Specifies the minimum port number of

Option	Description
	the specified service rule. • Max- Specifies the maximum port number of the specified service rule. The value range is 0 to 65535. • Source port • Min - Specifies the minimum port number of the specified service rule. • Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535. **Notes:** • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. **ALL**: • Protocol: Specifies a protocol name for the service rule. If it is a unknown protocol, you can directly

Option	Description
	enter the corresponding protocol number. . Notes: • The minimum code cannot exceed the maximum code. • If "Max " is not configured, system will use "Min" as the single code. 3. Click **Add** to add the configured service rules to the list on the left. 4. Click **Close** .
Application	Specifies an application/application group/application filters. 1. Click **Application**, in the pop-up dialog, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click the selected applications/application groups/application filters to add them to the left pane. 3. After adding the desired objects, click **Close** to complete the application configuration. You can also perform other operations:

Option	Description
	• To add a new application group, select **Application Groups** from the **Application** drop-down menu and click ⊕ icon. • To add a new application filter, select **Application Filters** from the **Application** drop-down menu and click ⊕ icon. **Note**: Deprecated predefined applications cannot be added.
VLAN ID	Specifies the VLAN ID that is matched to the policy rule. The value range is from 1 to 4,094. If multiple VLAN IDs are specified, separate them with semicolons. Each policy rule supports up to 32 VLAN IDs.

Action	Specifies an action for the traffic that is matched to the policy rule, including:
	• Permit - Select **Permit** to permit the traffic to pass through.
	• Deny - Select **Deny** to deny the traffic.
	• Secured Connection:
	  • WebAuth - Performs Web authentication on the matched traffic. Select **WebAuth** from the drop-down list after selecting the **Secured Connection** option, and then select an authentication server from the following drop-down list.
	  • From tunnel (VPN) - For the traffic from a peer to local, if this option is selected, system will first determine if the traffic originates from a tunnel. Only

Option	Description
	such traffic will be permitted. Select **From tunnel (VPN)** from the drop-down list after selecting the **Secured Connection** option, and then select a tunnel from the following drop-down list. • Tunnel (VPN) - For the traffic from local to a peer, select this option to allow the traffic to pass through the VPN tunnel. Select **Tunnel (VPN)** from the drop-down list after selecting the **Secured Connection** option, and then select a tunnel from the following drop-down list. To allow traffic from this specified VPN tunnel at the same time, select **Bi-directional policy**. When the policy rule is created, another policy rule with the **From tunnel (VPN)** field set to this VPN tunnel will be automatically created. **Note**: The Bi-directional VPN Policy function can be configured only when you create a policy rule. • Portal server - Performs portal authentication on the matched traffic. Select **Portal server** from the drop-down list after selecting the **Secured Connection** option, and then type the URL address of the portal server.
Enable Web Redirect	Enable the Web redirect function to redirect the HTTP request from clients to a specified page automatically. With this function

Option	Description
	enabled, system will redirect the page you are requesting over HTTP to a prompt page. 1. Click the **Enable Web Redirect** button. 2. Type a redirect URL into the **Notification page URL** box. When using Web redirect function, you need to configure the Web authentication function. For more configurations, see User Online Notification.
Audit Comment	After the "Configuration Audit" function is enabled, this option is required when creating or modifying a policy, and you must add policy audit comments to the text box. The range is 1 to 255 characters. For detailed operation of this function, please refer to Configuring Policy Audit Function. When the "Configuration Audit" function is not enabled, this option is optional and the range is 0 to 255 characters. For enabling/disabling the "Configuration Audit" function, please configure it in the **Option** page (**System > Device Management > Option**), refer to the Configuration Audit.

Expand Protection, configure the corresponding options.

Option	Description
Antivirus	Specifies an antivirus profile. The combination of security policy rule and antivirus profile enables the devices to implement fine-grained application layer policy control.
IPS	Specifies an IPS profile. The combination of security policy rule

Option	Description
	and IPS profile enables the devices to implement fine-grained application layer policy control.
Antispam	Specifies an anti-spam profile. The combination of security policy rule and anti-spam profile enables the devices to implement fine-grained application layer policy control.
URL Filtering	Specifies a URL filter profile. The combination of security policy rule and URL filter profile enables the devices to implement fine-grained application layer policy control.
Sandbox	Specifies a sandbox profile. The combination of security policy rule and sandbox profile enables the devices to implement fine-grained application layer policy control.
Botnet Prevention	Specifies a botnet prevention profile. The combination of security policy rule and botnet prevention profile enables the devices to implement fine-grained application layer policy control.

Expand Data Security, configure the corresponding options.

Option	Description
File Filter	Specifies a file filter profile. The combination of security policy rule and file filter profile enables the devices to implement fine-grained application layer policy control.
File Content Filter	Specifies a file content filter profile. The combination of security policy rule and file content filter profile enables the devices to implement fine-grained application layer policy control.
File Content Filter	Specifies a file content filter profile. The combination of security policy rule and file content filter profile enables the devices to

Option	Description
	implement fine-grained application layer policy control.
Web Content	Specifies a web content profile. The combination of security policy rule and Web Content profile enables the devices to implement fine-grained application layer policy control.
Web Posting	Specifies a web posting profile. The combination of security policy rule and web posting profile enables the devices to implement fine-grained application layer policy control.
Email Filter	Specifies an email filter profile. The combination of security policy rule and email filter profile enables the devices to implement fine-grained application layer policy control.
APP Behavior Control	Specifies an app behavior control profile. The combination of security policy rule and app behavior control profile enables the devices to implement fine-grained application layer policy control.
Network Behavior Record	Specifies a NBR profile. The combination of security policy rule and NBR profile enables the devices to implement fine-grained application layer policy control.

Expand Options, configure the corresponding options.

Option	Description
Schedule	Specifies a schedule when the security policy rule takes effect. Select a desired schedule from the **Schedule** dialog. This option supports fuzzy search. After selecting the desired schedules, click the blank area in this page to complete the schedule configuration. To create a new schedule, click ⊕ icon.

Option	Description
Start Time	Specifies the time when the security policy rule takes effect. To do this, click to specify the time from the drop-down menu. You can also click "Now" in the lower-left corner to use the current system time as the start time of the effective period.
Expire Time	Specifies the time when the security policy rule expires. To do this, click to specify the time from the drop-down menu. You can also click "Now" in the lower-left corner to use the current system time as the end time of the effective period.
Session Timeout	Specifies the session timeout period of the policy rule. The session timeout period indicates the aging period of session in the policy rule. After the timeout period is reached, the session is disconnected. Valid values: 1 to 65535 seconds or 1 to 1000 days.
Log	You can log policy rule matching in the system logs according to your needs. • For the policy rules of Permit, logs will be generated in two conditions: the traffic that is matched to the policy rules starts and ends its session. • For the policy rules of Deny, logs will be generated when the traffic that is matched to the policy rules is denied. Select one or more check boxes to enable the corresponding log types. • Deny - Generates logs when the traffic that is matched to the policy rules is denied.

Option	Description
	• Session start - Generates logs when the traffic that is matched to the policy rules starts its session. • Session end - Generates logs when the traffic that is matched to the policy rules ends its session.
SSL Proxy	Specifies a SSL proxy profile. The combination of security policy rule and SSL proxy profile enables the devices to decrypt the HTTPS traffic.
Policy Assistant	Click the **Enable** button to enable policy assistant. After enabling the policy assistant, you can specify the policy ID as the traffic hit policy. System can analyze the traffic data hit the specified policy ID, and aggregate the traffic list according to the user-defined aggregation rules, and finally the security policy rules that meet your expectations can be generated. For how to use policy assistant, see Configuring the Policy Assitant.
ACL	Click the **Enable** button to enable the access control function and select the ACL profile. With the combination of security policy and ACL rules, system can achieve accurate access controlling.
Aggregate Policy	Click the Aggregate Policy drop-down menu, and select the aggregate policy to be added to the aggregate policy to which you want to add.
Position	Select a rule position from the Position drop-down list. Each policy rule is labeled with a unique ID or name. When traffic flows into a device, the device will query for the policy rules by

Option	Description
	turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed in policy rule list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name.
Description	Type descriptions into the **Description** box.

Click Userdefined Attribute and enter the corresponding configuration.

Option	Description
User-defined Attributes 1-8	Specifies the custom attribute content of the policy, which can be up to 31 characters in length. **Note**: This option is displayed and available for configuration only after you have configured the policy custom attributes mapping. For more information, see Configuring Policy User-defined Attributes Mapping.

3. Click **OK** to save your settings.

For more information, refer to the **Policy** > **Security Policy** > **Configuring a Security Policy Rule** section in *StoneOS_WebUI_User_Guide*. FR 40345

CLI

Configuring a Policy Rule

You can configure a policy rule via CLI to control the traffic destined to the device. The configuration includes:

- Entering the policy configuration mode
- Switching to the multi-zone mode
- Creating a policy rule
- Editing a policy rule
- Enabling/Disabling a policy rule
- Configuring the service
- Specifying the default action
- Configuring Policy User-defined Attributes
- Specifying That the Policy Matches the Post-DNAT Destination Address
- Configuring the start time of the policy rule
- Configuring the expire time of the policy rule

Configuring the Start Time of the Policy Rule

The system supports to configure the time when a single policy rule takes effect. To do this, in policy rule configuration mode, use the following command:

start-time *time_value*

- *time_value* - Specifies the start time of the policy rule, which needs to be in the "MM/DD/YYYY HH:MM:SS" format. Example: 06/07/2024 17:49:32.

Configuring the Expire Time of the Policy Rule

The system supports to configure the time when a single policy rule expires. To do this, in policy rule configuration mode, use the following command:

expire-time *time_value*

- *time_value* - Specifies the expire time of the policy rule, which needs to be in the "MM/DD/YYYY HH:MM:SS" format. Example: 06/07/2024 17:49:32.

For more information, refer to the **Policy** > **Security Policy** > **Configuring a Policy Rule** section in *StoneOS_CLI_User_Guide*. FR 40345

VPN Supports for Configuring Route Priority and the Same Pre-shared Key, and Displaying the Peer ID and Proxy ID

WebUI

Configuring Dial-up VPN

Dial-up VPN indicates configuring only one VPN tunnel on the central device, after which multiple remote dial-up endpoints can access the central device through the VPN tunnel. Remote dial-up endpoints need to configure an IKE VPN corresponding to the central device's VPN tunnel for data protection. At the same time, the central device authenticates the identity of the dial-up end-points using pre-shared keys or certificate authentication methods, thereby establishing a VPN tun-nel with the dial-up endpoints.

The configuration of dial-up VPN includes the following two parts:

- Configure center device
    - Configure P1 proposal
    - Configure the peer end
    - Configure P2 proposal
    - Configure tunnel
- Configure the dial-up (similar to the configuration of the central device)

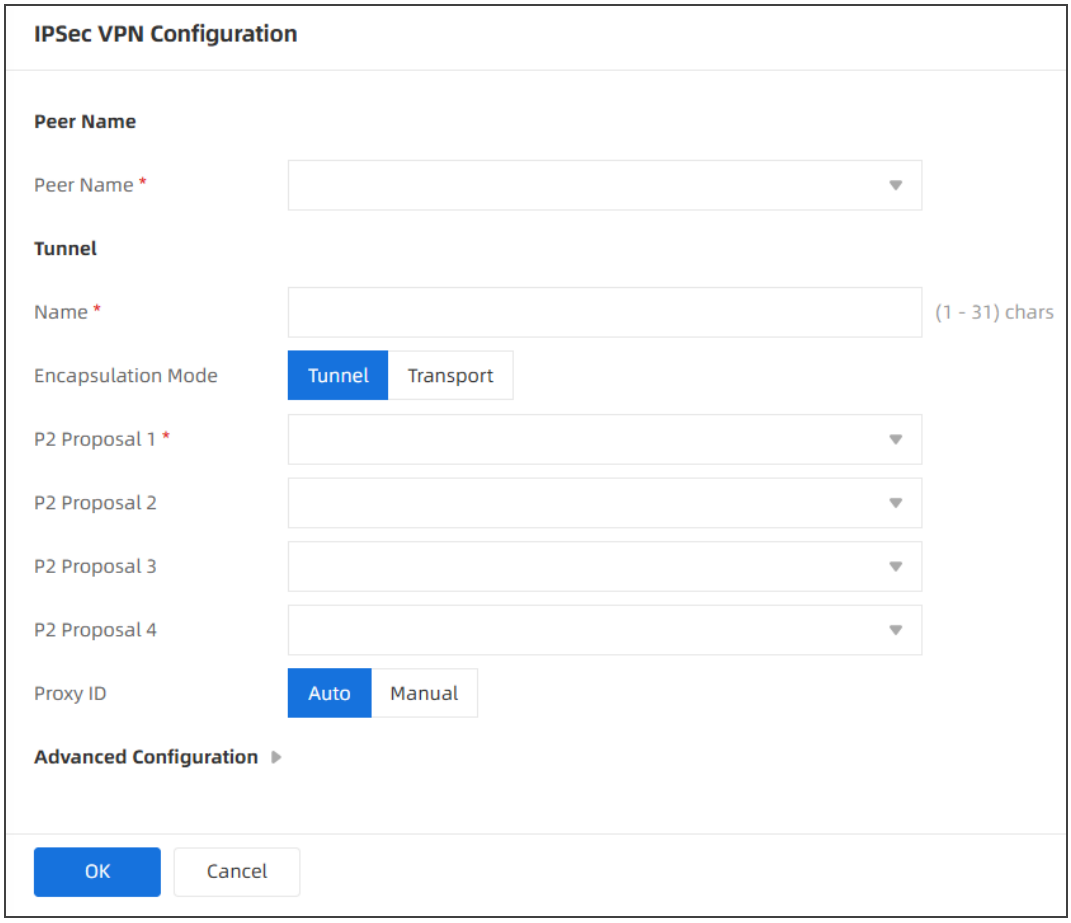
Configuring the Central Device

To configure the dial-up VPN for the center device, take the following steps:

1. Select **Network** > **VPN** > **IPSec VPN** to enter the IPSec VPN page.

2. Select the **IPSec VPN** tab.

3. Click **New** to open the **IPSec VPN Configuration** page.



On the **IPSec VPN Configuration** page, configure the following options:

Option	Description
Peer Name	
Peer Name	From the **Peer Name** drop-down list, select the ISAKMP gateway. For more information about how to configure the peer, see the Configuring VPN Peer section.

Option	Description
Tunnel	
Tunnel	Enter the relevant information in the **Tunnel** section. For more information, see the **VPN** > **IPSec VPN** > **Configuring IPSec VPN** topic.
Advanced Configuration	
Commit Bit	Click the button to set the commit bit for the corresponding party, which prevents packet loss and time differences. However, setting the commit bit may slow down the response speed.
Auto connect	Configure the automatic connection function. By default, this function is disabled; click the button to enable it. The device provides two methods for triggering SA establishment: automatic mode and traffic-triggered mode. In automatic mode, the device checks the SA status every 60 seconds, and if the SA is not established, it automatically initiates a negotiation request. In traffic-triggered mode, the tunnel only initiates a negotiation request when there is data traffic that needs to be transmitted through the tunnel. By default, the system uses the traffic-triggered method.
Accept-all-proxy-ID	This function needs to be configured on the responding device during IKE tunnel negotiation. After enabling, the responding device will accept the Phase 2 ID configuration from the peer (the initiating party), and simultaneously set its own Phase 2 ID to correspond with the peer, thus allowing both ends of the IKE tunnel to negotiate successfully. It is commonly used in scenarios where the responding device cannot perceive or is not interested in the Phase 2 ID of the initiator.

Option	Description
	Notes: When multiple Phase 2 IDs are configured on the responding device (i.e., configuring multiple IKE tunnels), this function needs to be disabled; otherwise, only one tunnel can be negotiated.
Enable Idle Time	Configure the idle time function. By default, this function is disabled. Click the button to enable it. After enabling, this function allows the tunnel to maintain its connection state in the absence of traffic for the maximum duration specified. Once the idle time is exceeded, the SA will be cleared.
DF-Bit	Specifies whether the forwarding device is allowed to fragment the packet. Options include: • Copy – Directly copy the DF option of IP packets from the sending end. This option is the system default. • Clear – Allows the forwarding device to fragment packets. • Set - Do not allow the forwarding device to fragment packets.
Anti-Replay	Replay protection indicates preventing malicious users from attacking by resending captured data packets, i.e., the receiver will reject old or duplicate packets. By default, the replay protection function is disabled. • Close - Disable the anti-replay function. This option is the system default.

Option	Description
	• 32 – Specifies the anti-replay window as 32. • 64 – Specifies the anti-replay window as 64. • 128 – Specifies the anti-replay window as 128. • 256 – Specifies the anti-replay window as 256. • 512 – Specifies the anti-replay window as 512.
UDP Checksum	Enable the UDP packet checksum function, which indicates the device will recalculate the UDP checksum after the UDP packet header has been modified. By default, this function is disabled.
Check ID	By default, this function is disabled. The ID check function is used for traffic distribution and rate limiting of IPSec VPN traffic. Before enabling it, ensure that the Phase 2 ID has been configured and the Phase 2 negotiation of the IKE tunnel is successful. After enabling, the device will filter the traffic entering and exiting the IKE tunnel based on the configuration of the Phase 2 ID, then distribute and limit the traffic; traffic that does not match the Phase 2 ID will be discarded. Specifically: • Traffic diversion: The device, based on the configuration of the Phase 2 ID, diverts traffic entering the IKE tunnel at the IKE tunnel entrance. If the source IP address, destination IP address, and type (service) of the traffic match a certain Phase 2 ID configuration, the traffic enters the corresponding IKE tunnel for encapsulation and transmission. If there is no matching Phase 2 ID, the traffic is discarded. • Traffic limiting: The device performs traffic limiting on the decapsulated traffic at the IKE tunnel exit based on

Option	Description
	the configuration of the Phase 2 ID. If the source IP address, destination IP address, and type (service) of the decapsulated traffic match the configuration of a certain Phase 2 ID, the traffic is further processed by the receiving device; if the traffic does not match any Phase 2 ID configuration, it is discarded.
Tunnel State Notify	Click the button to enable the VPN tunnel status notification function. After enabling this function, if the VPN is route-based, the system will immediately notify the routing module of the interrupted VPN tunnel information and perform tunnel route update processing once it detects an interrupted VPN tunnel; if the VPN is policy-based, the system will immediately notify the policy module of the interrupted VPN tunnel information and perform tunnel policy update processing once it detects an interrupted VPN tunnel.
VPN Track	Click the button to enable the VPN tunnel monitoring function. The device can monitor whether the specified VPN tunnel is connected and can achieve backup or load balancing for two or more VPN tunnels. This function is effective for both route-based and policy-based VPNs. Options include: • Track Interval – Specifies the time interval for sending Ping monitoring packets. • Threshold – Specifies the threshold for determining monitoring failure. If the system does not receive the specified number of response packets consecutively, it determines

Option	Description
	that the monitoring has failed, indicating that the target tunnel is down. • Source Address – Specifies the source IP address for sending Ping monitoring packets. • Destination Address – Specifies the IP address of the monitoring target.
Intelligent Routing	Select the intelligent routing rule from the **Intelligent Routing** drop-down list. For more information about how to configure intelligent routing rules, see Configure Intelligent Routing. Intelligent routing and VPN tunnel monitoring cannot be configured simultaneously. **Notes:** This function is supported only when the peer option type is static IP.
DNS1	Specifies the primary DNS server IP address that the PnPVPN server deploys to the client.
DNS2	Specifies the backup DNS server IP address for the PnPVPN server to deploy to the client.
DNS3	Specifies the backup DNS server IP address for the PnPVPN server to deploy to the client.
DNS4	Specifies the backup DNS server IP address for the PnPVPN server to deploy to the client.
WINS1	Specifies the primary WINS server IP address for the PnPVPN server to deploy to the client.

Option	Description
WINS2	Specifies the backup WINS server IP address for the PnPVPN server to deploy to the client.
Tunnel Route	This option needs to be modified after completing the IKE VPN configuration. Click Edit to open the **Tunnel Route Configuration** dialog box. In this dialog box, add one or more tunnel routes. The system allows a maximum of 128 tunnel routes.
Route Priority	Notes: • Before configuring route priority, you need to enable the route generation function first; otherwise, the route priority configuration will not take effect. For more information about how to enable the route generation function, see the Configuring VPN Peer section. • This function only takes effect for VPNs that comply with the IKE1 protocol standard. • If this end is the responder, the route priority is primarily determined by the initiator. • If the initiator configures route priority, and the responder does not support the route priority function, it will result in a failed VPN connection. (Route priority is supported only in StoneOS R10P9 and later versions, R11P3 and later versions, R12 and later versions, R10P9M5 and later

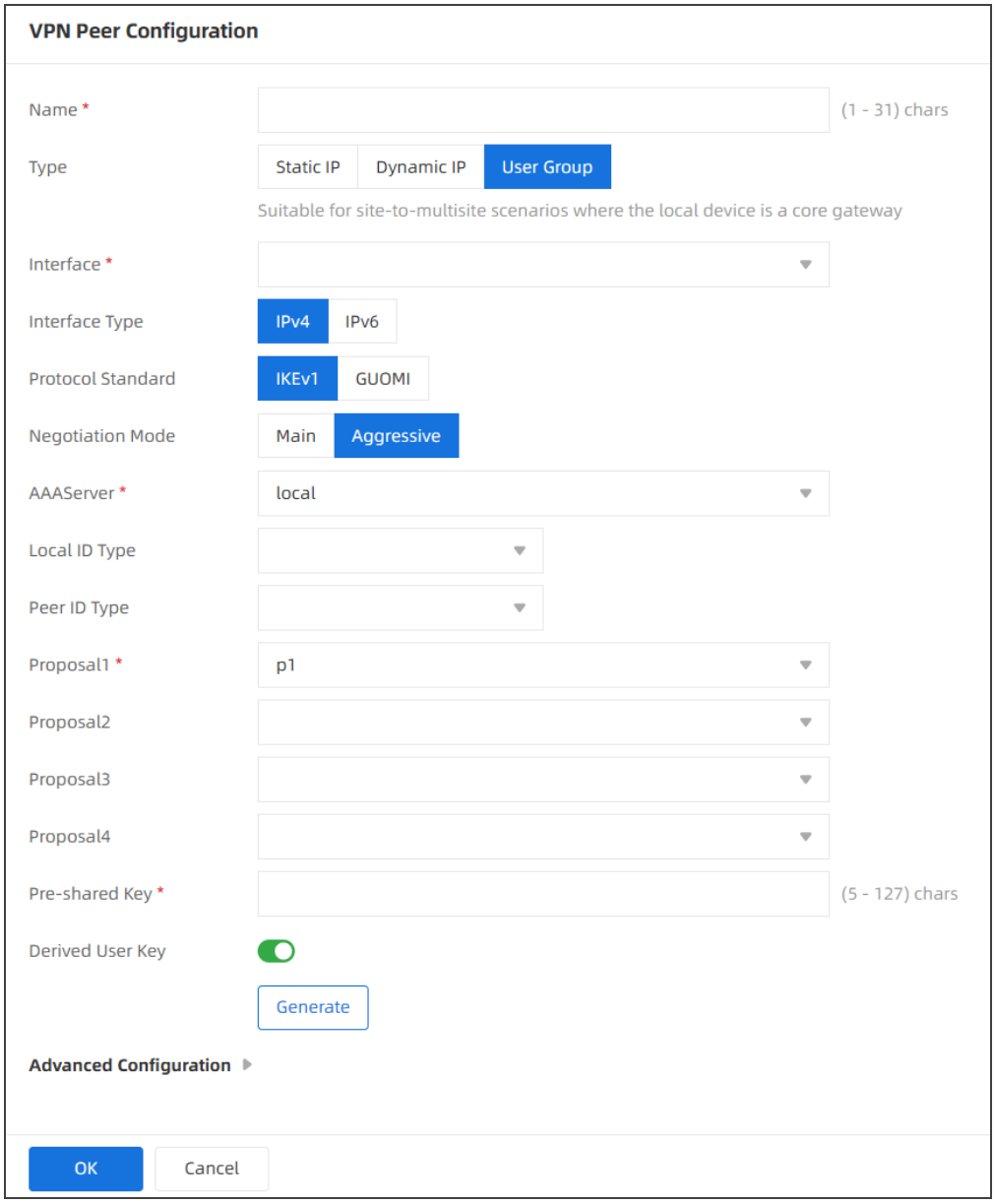
Option	Description
	versions, R11F3 and later versions.) You can specify the priority of routes, allowing for more flexible management of VPNs. For example, for VPNs reaching the same destination address, if you need to set up primary and backup VPNs, you can specify different route priorities to achieve this; if you need to implement load balancing, you can specify the same route priority. The higher the specified route priority number, the lower the priority, with a value range of 1-255. If no route priority is specified, the default value is 1.
Description	Enter a description for the tunnel being created in the text box.

4. Click **OK**.

Configuring the VPN Peer

To configure the dial-up VPN peer parameters, take the following steps:

1. Click **Network** > **VPN** > **IPSec VPN** to enter the IPSec VPN page.
2. Select the **IPSec VPN** tab.
3. Click New to open the **IPSec VPN Configuration** page.
4. Click the **Peer Name** drop-down list, click ⊕, and open the **VPN Peer Configuration** panel.



In the VPN Peer Configuration panel, configure the following options:

Basic Configuration	
Name	Specify the name of the ISAKMP gateway.
Type	Specify the type of the peer IP address. The central device of a dial-up VPN needs to select the "User Group" type.

Basic Configuration	
	• If the peer IP address type is static, select **Static IP**, and then enter the peer's IP address in the **Peer Address** field; • If the peer IP address type is user group, select **User Group** and choose the required authentication server name from the subsequent **AAAServer** drop-down list. • If the peer IP address is a dynamic IP address, select **Dynamic IP**.
Interface	Specifies the interface bound to the ISAKMP gateway.
Interface Type	Specify the interface type, including IPv4 and IPv6. This option is only applicable to the IPv6 version.
Protocol Standard	Specifies the negotiation protocol standard, which can be IKEv1, IKEv2, and National Cryptography Standard (GUOMI). By default, the system uses the international standard IKEv1 as the negotiation protocol standard. If you choose the GUOMI standard, specify the national cryptography standard version number in the version field: • v1.0: For the GM 1.0 version. • v1.1: For the GM 1.1 version. • Default: If the "Default" option is configured, both GM v1.0 and v1.1 protocol versions can be negotiated. **Notes:** If a specific version number v1.0 or v1.1 is specified, the two devices involved in the negotiation need to be of the same version number to successfully

Basic Configuration	
	negotiate; otherwise, the negotiation will fail.
Negotiation Mode	Specifies the IKE negotiation mode. There are two negotiation modes for IKE: Main mode and Aggressive mode. Main mode is the default system mode. IKE Aggressive mode does not provide identity protection, and it can only be used in the following cases: the IP address of the central device is a fixed assigned address, while the client device's IP address is dynamically obtained. This option is only applicable to IKEv1 and National Cryptography versions.
Local ID Type	Specify the local ID. The system supports FQDN, U-FQDN, ASD1-DN (only for certificate usage), KEY-ID, and IP type IDs. Select the radio button for the desired ID type, and then enter the specific content of the ID or IP in the Local ID or Local IP text box.
Peer ID	Specifies the peer ID. The system supports FQDN, U-FQDN, ASD1-DN (only for certificate usage), KEY-ID, and IP type IDs. Select the radio button for the desired ID type, then enter the specific content of the ID or IP in the Peer ID or Local IP text box. If using a Radius server for authentication, select the **Wildcard** checkbox.
Proposal1	Specifies P1 proposals for the ISAKMP gateway. You can specify up to 4 proposals. To configure P1 proposals, refer to Configuring P1 Proposals.
Proposal2	Specifies P1 proposals for the ISAKMP gateway. You can specify up to 4 proposals.
Proposal3	Specifies P1 proposals for the ISAKMP gateway. You can specify up to 4 proposals.

Basic Configuration	
Proposal4	Specifies P1 proposals for the ISAKMP gateway. You can specify up to 4 proposals.
Pre-shared Key	If using pre-shared key authentication, specify the pre-shared key through this option.
Modify Pre-shared Key	When editing the peer configuration of the VPN, you can see the pre-shared key function. After enabling it, the pre-shared key input box will be displayed. To modify it, enter the new pre-shared key and save the configuration.
Derived User Key	（丢失或坏的片段）
Generate User Key	Click **Generate**. In the **Generate the User Key** panel, enter the pre-shared key of the central device and the IKE ID of the dial-up. Then click **Generate**. The generated user key will be displayed in the **Generate Result** text box. For IKE ID configuration, see the **Object** > **User** > **Configuring User** section.
Signature Trust Domain	If using DSA Signature, RSA Signature, ECDSA Signature and GM-DE (National Cryptography Data Envelope) authentication methods, specify the trust domain through this option.
Peer Trust Domain	Configure the trust domain where the peer certificate is located. The peer certificate is generally used for data encryption and authentication during negotiation and need to be imported by the end initiating the VPN connection. This option is only applicable to GM 1.0 version.
Encryption Trust Domain	Configure the trust domain where the encryption certificate is located. The encryption certificate is generally used for data encryption during negotiation. This option is only applicable to GM 1.1 version, and the system needs to be configured with dual certificates.

Basic Configuration	
Advanced Configuration	
Connection type	Specify the connection type for the ISAKMP gateway. Select the appropriate type. • Bidirectional – Specifies that the ISAKMP gateway acts as both the initiator and the responder. This option is the system default. • Initiator – Specifies that this ISAKMP gateway is only the initiating party. • Responder – Specifies that this ISAKMP gateway is only a responder.
NAT Traversal	In an IPSec or IKE-built VPN tunnel, if there is a NAT gateway device that performs NAT conversion on the VPN data, the NAT traversal function of IPSec or IKE needs to be enabled. By default, the NAT traversal function is disabled. This option applies only to IKEv1 and national cryptography versions.
Any Peer ID	Allows the created ISAKMP gateway to accept any peer ID, without performing peer ID checks. This option is only applicable to IKEv1 and national cryptography versions.
Generate Route	Configure the auto-generated route function. By default, this function is disabled. This function allows the device to automatically add route entries from the central device to branch offices, thus avoiding issues associated with manual route configuration.
DPD	Configure the DPD (Dead Peer Detection) function. By default, this function is disabled; click the button to enable it. Once

<table>
<tr><th colspan="2">Basic Configuration</th></tr>
<tr><td></td><td>enabled, the system will periodically send request packets to the peer at specified intervals to check if the ISAKMP gateway exists.
• DPD Mode – Specifies the DPD detection mode, which can be either periodic or on-demand:
• periodic: After enabling this mode, the system will send DPD detection packets to the peer at specified time intervals continuously. If no response packet is received from the peer within one DPD period, the peer is considered inactive. Calculation method: DPD detection period = DPD interval time * DPD retry count.
• on-demand: After enabling this mode, the system will determine whether to send DPD (Dead Peer Detection) probe messages based on whether the device receives IPSec traffic. If the device does not receive IPSec traffic, no DPD probe messages are sent; if the device receives IPSec traffic and needs to forward it, the system checks the time interval since the last IPSec packet was received from the peer and compares it with the DPD probe period: ① If the current time interval since the last IPSec packet from the peer is less than the DPD probe period, it indicates that packets from the peer were</td></tr>
</table>

	received within the DPD probe period, indicating that the peer ISAKMP gateway is active, and the device does not send a DPD probe message; ② If the current time interval since the last IPSec packet from the peer exceeds the DPD probe period, it indicates uncertainty about the status of the peer ISAKMP gateway, and the device sends a DPD probe message to check the peer ISAKMP gateway. If no packets from the peer are received within one DPD probe period, it is determined that the peer ISAKMP gateway has failed. The system will age the SA (Security Association) information for both phases and re-initiate new IPSec negotiations. • DPD Interval – Specifies the time interval for sending DPD query requests to the peer, in seconds. The value range is 1 to 10 seconds, with a default value of 10 seconds. • DPD Retries – Specifies the number of times DPD query requests are sent to the peer. After sending a query request to the peer, if no message from the peer is received within the specified time interval, the system will send the query request again, repeating this process until the number of times specified by this parameter is

Basic Configuration	
	reached. If no message from the peer is still received after the specified number of queries, the peer ISAKMP gateway is considered to be down. The range of query request counts is 1 to 10, with a default value of 3.
Description	Enter a description for the ISAKMP gateway being created in the text box.
XAUTH Server	Select the button to enable the XAUTH server on the device. After enabling the XAUTH server, the device can authenticate users attempting to access the IPSec VPN network using the configured authentication servers (RADIUS and local AAA servers). This option is only applicable to IKEv1 and national cryptography versions. You can select an existing IPSec-XAUTH address pool from the "Address Pool" drop-down menu, which is an optional configuration. When the client successfully connects to the XAUTH server, the device will assign an IP address from the address pool along with other relevant parameters (such as DNS server addresses and WINS server addresses) to the user. For more information about the IPSec-XAUTH address pool, see the **VPN** > **IPSec VPN** > **Configuring IPSec-XAUTH Address Pool** section.

5. Click **OK**.

Configuring the Dial-up

The dial-up needs to configure P1 proposal, P2 proposal, ISAKMP gateway, and tunnel corresponding to the central device. The configuration process is basically the same as that of the central device.

When configuring the ISAKMP gateway for the dial-up, if the central device uses a pre-shared key and has enabled the derived user key function, the pre-shared key specified by the dial-up end is the

corresponding user key generated by the central device; if the derived user key function is not enabled, the pre-shared key specified by the dial-up is the pre-shared key of the central device.

In the derived key method, configuring the pre-shared key for the dial-up

（丢失或坏的片段）

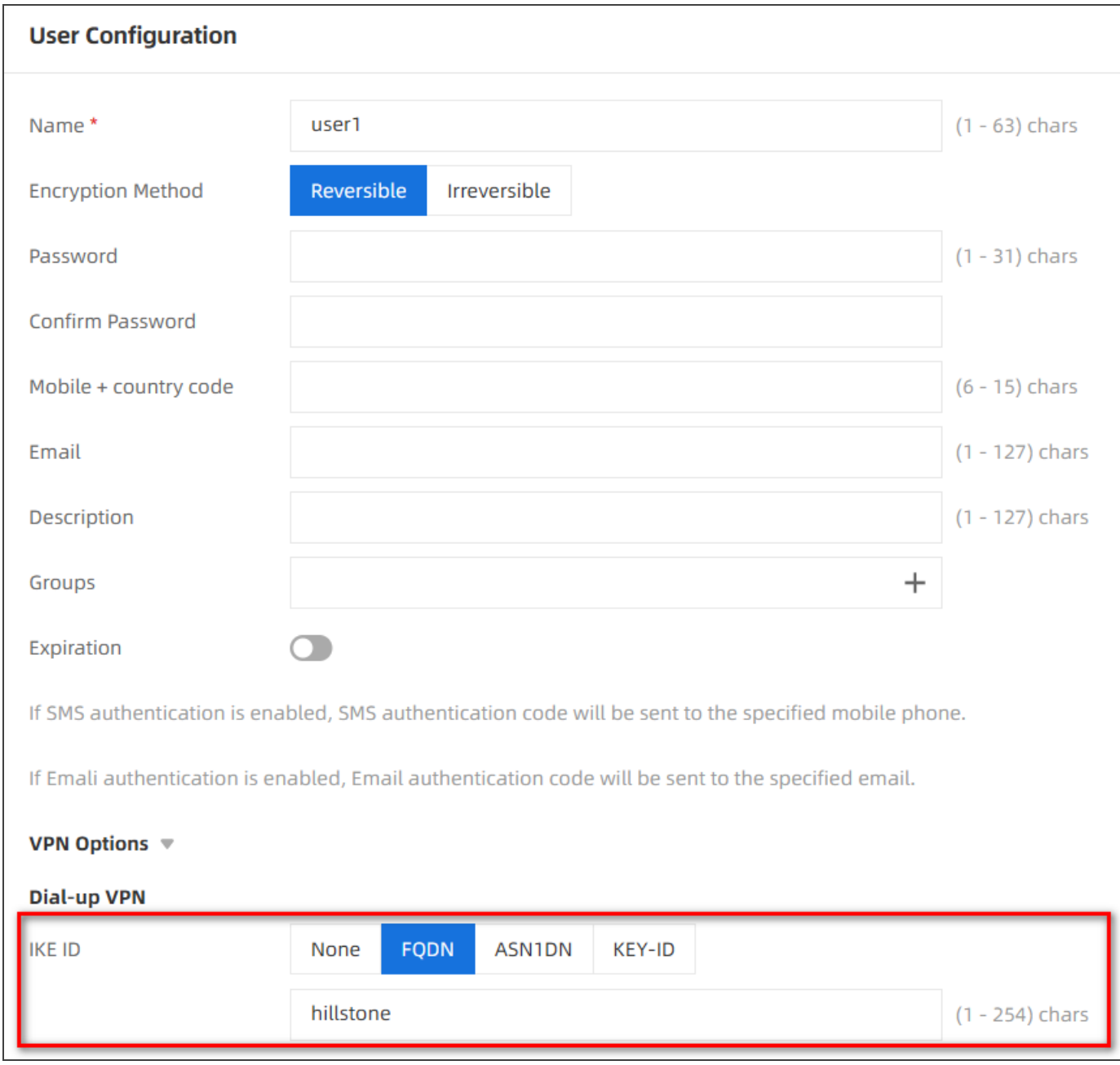
The configuration steps for the central device are as follows:

1. Configure the IKE ID for dial-up user
2. Enable the derived user key function (default is enabled)
3. Generate user key

Step 1: Configure the IKE ID for the dial-up user

1. Click **Object** > **User** > **Local User**.
2. Click **New**, select **User** from the drop-down list, and open the **User Configuration** page.
3. Enter the user name. In the **IKE ID** field, select the ID type and enter the IKE ID of the dial-up (it needs to match the local ID of the dial-up). The system supports FQDN, ASD1-DN (only for certificate usage), and KEY-ID types of IKE ID. As shown in the figure, select

the FQDN type and enter the IKE ID as "hillstone".



4. Click **OK**.

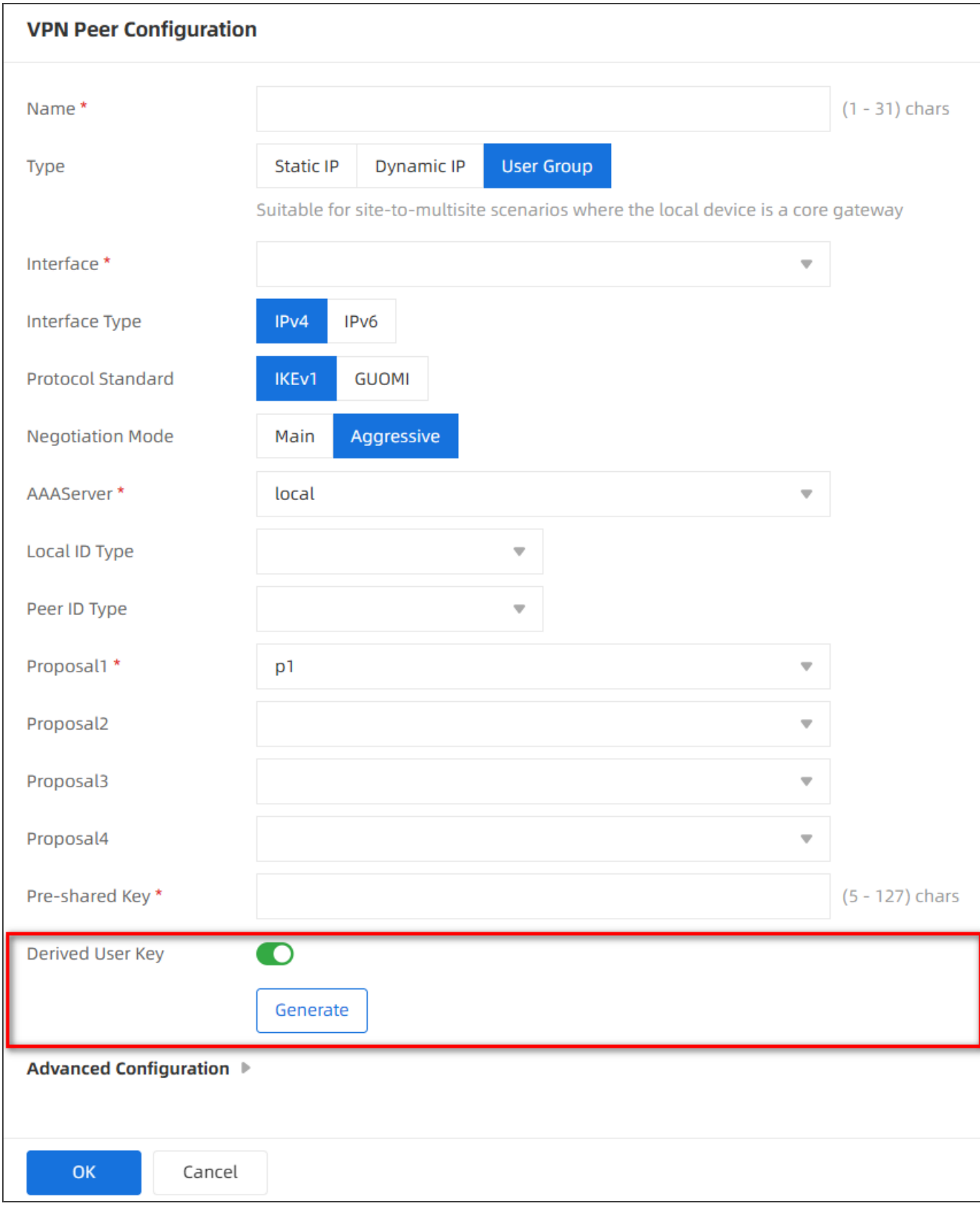
Step 2 & Step 3: Enable derived user key function & Generate user key

1. Click **Network** > **VPN** > **IPSec VPN** to enter the **IPSec VPN** page.

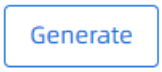
2. Select the **IPSec VPN** tab.

3. Click **New** to open the **IPSec VPN** page.

4. Click the **Peer Name** drop-down list, click the button, and open the **VPN Peer Configuration** page.


VPN Peer Configuration
Name *
(1 - 31) chars
Type
Static IP
Dynamic IP
User Group
Suitable for site-to-multisite scenarios where the local device is a core gateway
Interface *
Interface Type
IPv4
IPv6
Protocol Standard
IKEv1
GUOMI
Negotiation Mode
Main
Aggressive
AAAServer *
local
Local ID Type
Peer ID Type
Proposal1 *
p1
Proposal2
Proposal3
Proposal4
Pre-shared Key *
(5 - 127) chars
Derived User Key
Generate
Advanced Configuration
OK
Cancel

5. Click  to enable the derived user key function. This function is enabled by default.

6. Click 

to open the **Generate the User Key** panel.

7. As shown in the figure, enter the IKE ID of the dial-up end user in the "IKE ID" text box, and enter the pre-shared key of the central device in the "Pre-shared Key" text box. Click **Generate**, and the generated user key will be displayed in the **Generate Result** text box. The pre-shared key corresponding to the dial-up needs to be filled with this user key.



8. Click **Disable** to return to the **VPN Peer Configuration** panel. Click **OK**.

The configuration steps for the dial-up are as follows:

1. Go to the corresponding **VPN Peer Configuration** page, and enter the user key generated by the central device in the "Pre-shared Key" text box.

2. Click **OK**.

In non-derived key mode, configuring the pre-shared key for the dial-up

（丢失或坏的片段）

The configuration steps for the central device are as follows:

1. Go to the corresponding **VPN Peer Configuration** page, click  after "Derived User Key" to disable the derived user key function. This function is enabled by default.
2. Click **OK**.

The configuration steps for the dial-up end are as follows:

1. Enter the corresponding **VPN Peer Configuration** page, and enter the pre-shared key of the central device in the "Pre-shared Key" text box.
2. Click **OK**.

Viewing IPSec VPN Monitoring Information

IPSec VPN monitoring mainly lists the results of phase 1 SA negotiation, phase 2 SA negotiation, and statistics of dial-up users through the ISAKMP SA list, IPSec SA list, and dial-up user list, respectively.

To check the VPN monitoring results, take the following steps:

1. Click **Network** > **VPN** > **IPSec VPN** to enter the IPSec VPN page.
2. Click **IPSec VPN Monitor** in the upper-right corner of the page. You can view IPSec VPN monitoring information on the ISAKMP SA, IPSec SA, and Dial-up User tabs.
    - On the ISAKMP SA tab, you can specify the peer name in the "Peer" drop-down list to filter monitoring information by peer name;
    - On the IPSec SA tab, you can specify a VPN name in the "VPN Name" drop-down list to filter monitoring information by VPN name;
    - On the Dial-up User tab, you can specify the peer name in the "Peer Name" drop-down list to filter monitoring information by peer name, click 

, specify the

IKE ID, dial-in username, or private IP to view monitoring information with the specified filter conditions.

The specific options on each monitoring page are described as follows:

ISAKMP SA list

Option	Description
Peer	Displays the peer name, which is the name of the ISAKMP gateway.
Cookie	Displays negotiated Cookies used to match the first phase SA.
Protocol Standard	Displays the protocol standard being negotiated.
Status	Displays the status of the first phase SA.
Peer Address	Displays the peer IP address.
Port	Displays the port number used to establish the first phase SA. 500 indicates that no NAT traversal was detected during the establishment of the first phase SA, and 4500 indicates that NAT traversal was detected.
Algorithm	Displays the algorithms used for the first phase SA negotiation, including authentication method, encryption algorithm, and verification algorithm.
Lifetime	Displays the lifetime of the first phase SA, in seconds.

IPSec SA list

Option	Description
ID	Displays the number automatically assigned by the system to the created tunnel.
VPN Name	Displays the name of the VPN.
Protocol Standard	Displays the protocol standard being negotiated.

Option	Description
Peer Name	Displays the peer name.
Peer ID	Displays the peer's IKE ID.
Proxy ID	Displays the subnet of the peer.
Direction	Displays the direction of the VPN.
Peer Address	Displays the peer IP address.
Port	Displays the port number used for the Phase 2 SA negotiation.
Algorithm	Displays the algorithms used by the tunnel. This includes protocol type, encryption algorithm, authentication algorithm, and compression algorithm.
SPI	Display local SPI and remote SPI. The inbound direction corresponds to the local SPI, and the outbound direction corresponds to the remote SPI.
CPI	Displays the compression parameter index used in the Phase 2 SA negotiation.
Lifetime	Displays the lifetime of the phase two SA, measured in seconds, i.e., after X seconds, the phase two SA will renegotiate the key.
Lifesize	Displays the lifetime of the Phase 2 SA, measured in KB, i.e., after X bytes of traffic, the Phase 2 SA will renegotiate the key.
Status	Displays the status of the Phase 2 SA.
Traffic	Displays the cumulative values of traffic received and sent through the tunnel.
Duration (second)	Displays the duration since the last successful negotiation of the Phase 2 SA to the current time, measured in seconds.

Option	Description
Sending/Receiving Rate (KB/s)	Displays the real-time send/receive rate of tunnel packets. The outbound direction corresponds to the send rate, and the inbound direction corresponds to the receive rate. Measured in KB/s.
Last Setup Time	Displays the time of the most recent successful negotiation for the Phase 2 SA.
Last Teardown Time	Displays the time of the most recent teardown for the Phase 2 SA.
Teardown Reason	Display the reason for the most recent teardown of the phase two SA. Teardown reasons include: • a disconnection request is received from the peer • an idle connection timeout occurred • configuration changed • VPN is manually cleared • a DPD timeout occurred • VPN track failed • an SPI inconsistency error occurred • a lifetime timeout occurred
Teardowns Today	Displays the number of SA teardowns in the Phase 2 from midnight of the current day to the current time. The maximum count is from midnight of the current day to midnight of the next day, after which the counted number resets to 0.

Dial-up user list

Option	Description
IKE ID	Displays the user's IKE ID.
Dial-in User	Displays the username of the dial-up user.
Public IP	Displays the public IP address of the dial-up user.
Private IP	Displays the private IP address of the dial-up user.
Proxy ID	Displays the subnet of the peer.
Encrypted Packets	Displays the number of encrypted packets transmitted through the tunnel.
Encrypted Bytes	Displays the number of encrypted bytes transmitted through the tunnel.
Decrypted Packets	Displays the number of decrypted packets transmitted through the tunnel.
Decrypted Bytes	Displays the number of decrypted bytes transmitted through the tunnel.

For more information, refer to the **VPN** > **IPSec VPN** > **Configuring IPSec VPN** section in the *StoneOS WebUI User Guide*. FR 44013/44015/44019

CLI

Configuring ISAKMP Gateway

After creating an ISAKMP gateway, you can specify the authentication server of the ISAKMP gateway, IKE negotiation mode, IP address and type of the ISAKMP gateway, IKE security proposal, pre-shared key, PKI trust domain, local ID, ISAKMP gateway ID, ISAKMP gateway connection method, and whether to enable NAT traversal for the ISAKMP gateway, etc.

.....

Enabling/Disabling Derived User Key Function

In "Aggressive Mode," the central device defaults to enabling the "Derived User Key" function. At this point, after configuring the pre-shared key for the central device, you need to generate different user keys one by one as the pre-shared keys for the dial-up. This method is more secure but less convenient, so you can also disable this function and use the pre-shared key of the central device as the pre-shared key for the dial-up end. For more information about how to generate user key configuration, refer to the **VPN > Dial-up VPN > Dial-up VPN Configuration > Generating Dial-up End User Pre-shared Key** section.

If this function is enabled, the pre-shared key on the dial-up needs to be filled with the generated user key; if this function is disabled, the pre-shared key on the dial-up only needs to be filled with the pre-shared key of the central device. This function is enabled by default.

To enable/disable the derived user key function, in ISAKMP gateway configuration mode, use the following commands:

- Enable: **derived-user-key**
- Disable: **noderived-user-key**

Configuring Route Priority

Before you start:

- Before configuring route priority, you need to enable the auto-generated route function first; otherwise, the route priority configuration will not take effect. For more information about the auto-generated route function, refer to the **VPN > Dial-up VPN > Dial-up VPN Configuration > Configuring Auto-Generated Route Function** section.

Notes:

- This function only takes effect for VPNs that comply with the IKE1 protocol standard.

- If this end is the responder, the route priority is primarily determined by the initiator.
- If the initiator configures route priority, and the responder does not support the route priority function, it will result in a failed VPN connection. (Route priority is supported only in StoneOS R10P9 and later versions, R11P3 and later versions, R12 and later versions, R10P9M5 and later versions, R11F3 and later versions.)

You can specify the priority of routes, allowing for more flexible management of VPNs. For example, for VPNs reaching the same destination address, if you need to set up primary and backup VPNs, you can specify different route priorities to achieve this; if you need to implement load balancing, you can specify the same route priority. The higher the specified route priority number, the lower the priority, with a value range of 1-255. If no route priority is specified, it defaults to 1.

To configure route priority, in IKE tunnel configuration mode, use the following command:

route-priority*number*

number - Specifies the priority of the route, with a value range of 1-255, defaulting to 1.

In IKE tunnel configuration mode, use the **noroute-priority** command to restore the default route priority.

Dial-up Configuration

The dial-up needs to configure P1 proposal, P2 proposal, ISAKMP gateway, and tunnel corresponding to the central device. The configuration process is basically the same as that of the central device.

When configuring the ISAKMP gateway for the dial-up, if the central device uses a pre-shared key and has enabled the derived user key function, the pre-shared key specified by the dial-up is the corresponding user key generated by the central device; if the derived user key function is not enabled, the pre-shared key specified by the dial-up is the pre-shared key of the central device.

For more information, refer to the **VPN** > **Dial-up VPN** > **Dial-up VPN Configuration** section in the *StoneOS CLI User Guide*. FR 44013/44015/44019

Certain Synchronous Modes of Twin-mode Support Synchronizing SNAT/DNAT/VRouter Configuration

CLI

Twin-mode HA Synchronization

To ensure the backup device can take over the work of the master data center when it fails, the master data center will synchronize its information with the backup data center. In different deployment modes, the system supports different synchronization modes and synchronization information types.

In twin-mode HA A/P mode, the types of information that can be synchronized include:

- IPv4 configuration information
- IPv4/IPv6 session information
- IPv4 ARP table
- IPv4 pinhole
- IPv4 track information
- IPv4/IPv6 dynamic route information
- IPv4 NTP information
- IPv4 signature file
- IPv6 ND neighbor information
- IPv6 PMTU entries

In twin-mode HA A/A mode, the system supports two synchronous modes: Partial synchronization and No synchronization. Take the following steps: refer to Specifying the deployment mode and synchronization mode. The types of information that can be synchronized include:

- configuration information: Policy/Service Book/Address Book/IPS/AV/URL/Schedule/SNAT/DNAT/VRouter (in which the configuration information of SNAT/DNAT/VRouter is not synchronized by default, and you need to enable synchronization manually)
- session information
- pinhole
- signature file

You can manually enable the SNAT configuration synchronization function, DNAT configuration synchronization function, and VRouter configuration synchronization function. After enabling, when the twin mode is A/A deployment mode and the synchronization method is partial synchronization, the two data centers can synchronize the corresponding configuration information.

> **Notes:** The synchronization configuration function can only be enabled when the twin mode is in the disabled state.

Synchronizing SNAT Configuration

By default, the SNAT configuration synchronization function is disabled. To enable the SNAT configuration synchronization function, use the following command in global configuration mode:

twin-mode-part-sync-config snat

In global configuration mode, use the **no twin-mode-part-sync-config snat** command to disable the SNAT configuration synchronization function.

Synchronizing DNAT Configuration

By default, the DNAT configuration synchronization function is disabled. To enable the DNAT synchronization configuration function, use the following command in global configuration mode:

twin-mode-part-sync-config dnat

In global configuration mode, use the **no twin-mode-part-sync-config dnat** command to disable the DNAT configuration synchronization function.

Synchronizing VRouter Configuration

By default, the VRouter configuration synchronization function is disabled. To enable the VRouter configuration synchronization function, use the following command in global configuration mode:

twin-mode-part-sync-config vrouter

In global configuration mode, use the **no twin-mode-part-sync-config vrouter** command to disable the VRouter configuration synchronization function.

Viewing Twin Mode Configuration

The system provides corresponding show commands to view the configuration information of the twin mode.

Viewing the Configuration Information of the Twin Mode

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

showtwin-modeconfiguration [**difference**]

- **difference** – Check if there are any inconsistencies in the synchronized configuration information between the two data centers.

Viewing Twin Mode Connection Information

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

show twin-mode link

Viewing the Status Information of the Peer in Twin Mode

To view the status information of the peer in twin mode, in any mode, use the following command:

show twin-mode peer

Viewing Twin Mode Status Information

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

show twin-mode status

Viewing the Number of Data Packets Transmitted in Twin Mode

To view the number of transmitted data packets in twin mode, in any mode, use the following command:

show twin-mode-counter

Viewing the Synchronization Status of SNAT/DNAT/VRouter Configurations

To check the synchronization status of SNAT/DNAT/VRouter configurations, in any mode, use the following command:

show twin-mode-part-sync-config

The following is an example of a return result. If the return result is empty, it indicates that the system will not synchronize SNAT/DNAT/VRouter configuration information.

```
hostname# show twin-mode-part-sync-config
twin-mode-part-sync dnat (System synchronizes DNAT configuration information)
twin-mode-part-sync vrouter (System synchronizes VRouter configuration information)
twin-mode-part-sync snat  (System synchronizes SNAT configuration information)
```

For more information, refer to the **High Availability (HA)** > **Twin-mode HA** > **Twin-mode HA Synchronization** section in *StoneOS CLI User Guide*. FR 42872

Supporting to Enable Algorithms Disabled by the OpenSSH Library

CLI

Managing SSH Algorithms

SSH connections use multiple SSH algorithms during the negotiation phase. To guard against potential security risks, when a certain SSH algorithm has a security vulnerability, you can proactively disable that algorithm to prevent adverse effects on your services.The OpenSSH library

defaults to disabling some insecure algorithms to provide a relatively secure connection environment even with default configurations. SSH algorithms that have been manually disabled or are disabled by default will not be used during the key exchange phase,and if vulnerabilities are later fixed, you can re-enable these SSH algorithms as needed. Currently, the system supports managing the following types of SSH algorithms: key exchange algorithms (kex algorithms), server host key algorithms, encryption algorithms, and message authentication code (MAC) algorithms. You can manage these SSH algorithms based on your actual needs to enhance the security and stability of the SSH connection process.

Managing SSH algorithms includes:

- Disable specified SSH algorithms
- Re-enable SSH algorithm
- View disabled SSH algorithms

Disabling Specified SSH Algorithms

To disable the specified SSH algorithm, in global configuration mode, use the following command:

no ssh server algorithms type {**encryption** | **kex** | **mac** | **server-host -key**} *algorithm-name*

- *algorithm-name* - Specifies the specific name of the SSH algorithm to be disabled. You can press the Tab key after the {**encryption** | **kex** | **mac** | **server-host -key**} parameter to view all SSH algorithm names available for the current type.

Re-enabling SSH Algorithms

Notes: The algorithms disabled by default in the OpenSSH library pose certain security risks. If you enable these algorithms on your own, it may lead to risks in SSH connections. Please proceed with caution!

The algorithms disabled by default in the OpenSSH library used in the current firewall version are as follows:

- kex_algorithms: Diffie-hellman-group1-sha1, Diffie-hellman-group14-sha1, Diffie-hellman-group-exchange-sha1, sntrup4591761x25519-sha512@tinyssh.org
- encryption_algorithms: 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, Rijndael-cbc@lysator.liu.se
- mac_algorithms: hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-sha1-96-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-md5-etm@openssh.-com
- server_host_key_algorithms: ssh-dss

To re-enable the SSH algorithm, in global configuration mode, use the following command:

ssh server algorithms type {**encryption** | **kex** | **mac** | **server-host -key**} *algorithm-name*

- *algorithm-name* - Specifies the specific name of the SSH algorithm to be re-enabled. You can press the Tab key after the {**encryption** | **kex** | **mac** | **server-host-key**} parameter to view the names of SSH algorithms that can be re-enabled for the current type.

Viewing Disabled SSH Algorithms

To view the disabled SSH algorithms, in any mode, use the following command:

show ssh server algorithms disable

The following is an example of the return result:

```
hostname#show ssh server algorithms disable
kex_algroithms: diffie-hellman-group14-sha256
server_host_key_algorithms: rsa-sha2-512
encryption_algorithms: aes128-ctr
mac_algorithms: umac-64-etm@openssh.com
```

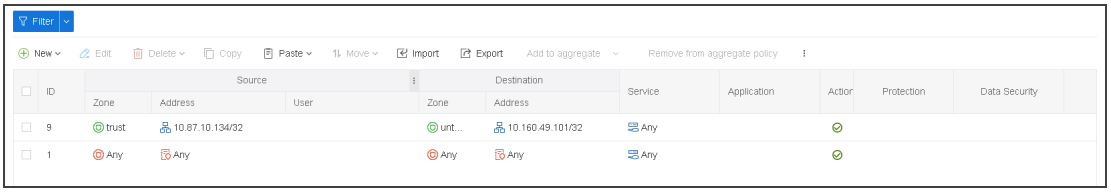
For more information, refer to the **System Management** > **Managing SSH Algorithms** section in the *StoneOS CLI User Guide*. FR 44988

Adding the Schedule Column in the Policy List and Supporting Filtering by Schedule Name

WebUI

Viewing the Policy/ Policy Group/ Mini Policy

View the security policy rules in the policy rule list.

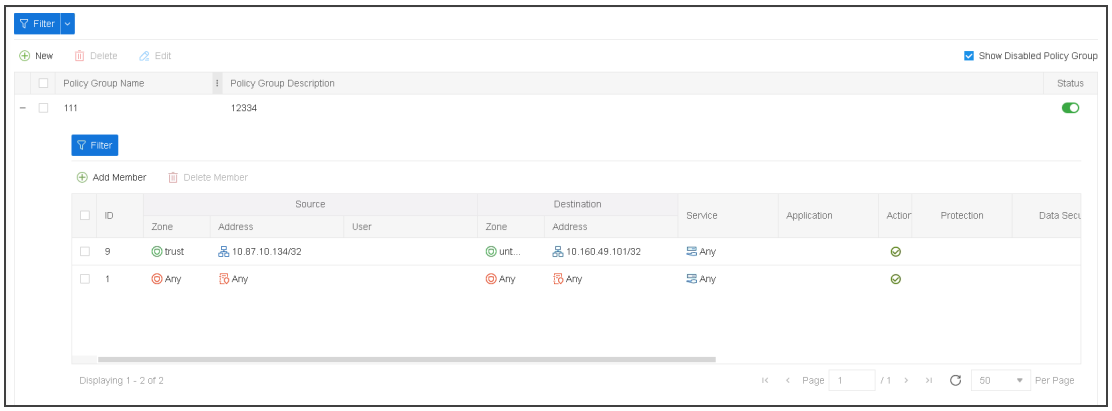


- Each column displays the corresponding configurations.
- Click icon under the Session Detail column in the Policy list to open then the **Session Detail** page. You can view the current session status of the selected policy.
  - You can also click Filter button to add filtering conditions and search out the filtered sessions.
  - The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. You can select Long Session to view the status of persistent sessions. For more information, see Session Timeout.
  - Select one or more sessions and click **Clear** to clear them. You can select at most all sessions on the current page and clear them.
- To provide you with a clearer view of the schedule and status of policies, the system displays the schedule in a separate column. The display includes an icon and the schedule name. The icons indicate different schedule statuses: indicates active, indicates inactive, and

indicates expired. Each policy can display up to 8 schedules. If there are more than 8 schedules, a "More" option will appear. You can click **More** to view all schedules for this policy.

- Hover over your mouse on the configuration in a certain column. Then based on the configuration type, the WebUI displays either ⋮ icon or the detailed configurations.
    - You can view the detailed configurations directly.
    - You can click ⋮ icon. Based on the configuration type, the WebUI displays **Add Filter** or **Details**.
        - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.
        - Click **Add Filter**, the filter condition of the configuration you are hovering over with your mouse appears on the top of the list, and then you can filter the policy according to the filter condition. For detailed information of filtering policy rules, see Searching Security Policy Rules/ Policy Groups.

View the policy groups in the policy group list.



- Each column displays the corresponding configurations.
- You can view the current policy group status in **Status** column. The enabled state is displayed as , and the disabled state is displayed as .

View the mini policy rules in the policy group list.



- Each column displays the corresponding configurations.
- The **ID** column shows the ID automatically assigned by the system for the mini policy. The ID must be unique in the entire system. The starting ID of the mini policy is 1000001, and the ID range varies according to different device platforms.

Searching for Security Policy Rules/ Policy Groups/ Mini Policy

Use the Filter to search for the policy rules/ policy groups/ mini policy that match the filter conditions.

1. Click **Policy > Security Policy > Policy**, **Policy > Security Policy > Policy Group** or **Policy > Security Policy > Mini Policy**.
2. On the Policy/ Policy Group/ Mini Policy page, click **Filter** in the upper-left corner, select a filter condition from the drop-down menu, and enter a value. Filter conditions include Aggregate/ Authorization Policy or Not, Aggregate Policy, Reference Schedule, Schedule Status, Name, ID, Source Zone, Source Address, User, Destination Zone, Destination Address, Service, Application, VLAN ID, Action, Schedule, and Description.
   When filtering policies by User, Schedule, or custom attributes, you can perform precise or fuzzy query to search policies that match the filter condition. Precise query is the default query method.

- Fuzzy: Fuzzy query is performed by specifying the keyword of the user name / user group name/ role name/ schedule name/ custom attribute keyword. By fuzzy matching the specified keyword, a list of all policies that contain this keyword in their user name/ user group name/ role name/ schedule/ custom attribute will be returned.
    - Select **User** from the **Filter** drop-down list and select **Fuzzy**. Enter the keyword of the user name/ user group name/ role name in the text box. Click **Enter** to search for the policy rules that matches the filter conditions.
    - Select **Schedule** from the **Filter** drop-down list and select **Fuzzy**. Enter the keyword of the schedule name in the text box. Click **Enter** to search for the policy rules that matches the filter conditions.
    - Select **Custom Attribute** from the **Filter** drop-down list and select **Fuzzy**. Enter the keyword of the custom attribute in the text box. Click **Enter** to search for the policy rules that matches the filter conditions.
- Precise: Precise query is performed by specifying a precise user name/ user group name/ schedule name/ custom attribute. By precise matching the specified user name/ user group name/ schedule name/ custom attribute, a list of all policies that have the same user name/ user group name/ schedule name/ custom attribute will be returned. If a policy rule contains the specified field, this policy will also be listed in the search results.
    - Select **User** from the **Filter** drop-down list and select **Precise**. From the drop-down list, select the AAA server where user/ user group resides. Then, click **Select User** or **Select User Group** from the drop-down list and select existing user name/ user group name. Click **Enter** to search for the policy rules that matches the filter conditions. You can also select **Input User** or **Input Usergroup** and specify the user name/ user group name in the text box.

- Select **Schedule** from the **Filter** drop-down list and select **Precise**. From the drop-down list, select an existing schedule name to filter all policy rules that match the filter conditions.
- Select **Custom Attribute** from the **Filter** drop-down list and select **Precise**. Enter the keyword of the schedule name in the text box. From the drop-down list, select an existing schedule name to filter all policy rules that match the filter conditions. Click **Enter** to search for the policy rules that matches the filter conditions.

Notes:

- Policy group and mini policy do not support the **User** and **Schedule** filter conditions.
- **Fuzzy** and **Precise** are mutually exclusive and cannot be selected at the same time.
- When **Precise** is specified, you need to specify the AAA server. In this case, the AAA server can only be Local server, AD server, and LDAP server. If AD server or LDAP server is specified, and **Input User** or **Input Usergroup** is specified, only policies that have the same user name/ user group name will be searched. If a policy's user group contains the specified user name/ user group name, this policy cannot be searched.

3. Click **Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the policy rules that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.

6. To delete a filter condition, hover your mouse on that condition and then click ×Remove All icon.

   To close the filter, click × icon on the right side of the row.



Save the filter conditions.

1. After adding the filter conditions, click ⌄ in Filter ⌄, in the drop-down menu, click **Save Filters**.
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.
4. To use the saved filter condition, double click the name of the saved filter condition.
5. To delete the saved filter condition, click × on the right side of the filter condition.

Notes:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

For more information, refer to the **Policy** > **Security Policy** > **Viewing and Searching for Security Policy Rules/ Policy Groups/ Mini Policy** section in *StoneOS WebUI User Guide*. FR 40264

CLI

Viewing Policy Rule Information

You can view the detailed information of all policy rules or a specified policy rule. And also you can view the detailed information of the policy matching the five-tuple filtering conditions (including

source IP address, destination IP address, protocol, source port and destination port).

To view the detailed information of the policy rules, in any mode, use the following command:

show policy [**id***id*] [**from***src-zone*] [**to***dst-zone*] [**src-addr***src-addr*] [**dst-addr***dst-addr*] [**protocol** | **service***service-name*] [**application***application-name*] [**description***description*] [**name***name*] [**name-filter***filter-name*] [**user** {**filter-fuzzy***filter-name* | **filter-precise***aaa-server-namefilter-name*}] [**user-group** {**filter-fuzzy***filter-name* | **filter-precise***aaa-server-namefilter-name*}] [**role filter-fuzzy***filter-name*] [**family** {*ipv4* | *ipv6*}] [**schedule-name***schedule-name*] [**schedule-name-filter***filter-schedule-name*]

- **id***id* - Shows the detailed information of the specified policy rule.
- **from***src-zone* - Shows the detailed information of the policy rule whose source security zone is the specified zone.
- **to***dst-zone* - Shows the detailed information of the policy rule whose destination security zone is the specified zone.
- **src-addr***src-addr* – Shows the detailed information of the specified source address of the IP range type.
- **dst-addr***dst-addr* – Shows the detailed information of the specified the destination address of the address entry type.
- **protocol** | **service***service-name* - Shows the detailed information of the specified protocol (**protocol**) or service (**service***service-name*).
- **service***service-name* – Shows the detailed information of the specified service type.
- **application***application-name* – Shows the detailed information of the specified application type.
- **description***description* – Shows the detailed information of the specified name rule.
- **name***name* – Shows the detailed information of the specified name rule.

- **name-filter***filter-name* − Shows the detailed information of all rules whose name includes the specified keyword.

  user − Shows policy rules with the specified user name.

- **user-group** − Shows policy rules with the specified user group name.

- **role** − Shows policy rules with specified role name.

- **filter-fuzzy***filter-name* | **filter-precise***aaa-server-namefilter-name* − Specifies the query method is fuzzy query (**filter-fuzzy**) or precise query (**filter-precise**).

  - **filter-fuzzy***filter-name* − Specifies the query method is fuzzy query. Fuzzy query is performed by specifying the keyword of the user name / user group name/ role name. By fuzzy matching the specified keyword, a list of all policies that contain this keyword in their user name/ user group name/ role name will be returned.

  - **filter-precise***aaa-server-namefilter-name* − Specifies the query method is precise query. Precise query is performed by specifying a precise user name/ user group name. By precise matching the specified user name/ user group name, a list of all policies that have the same user name/ user group name will be returned. If a policy's user group contains the specified user name/ user group name, this policy will also be listed in the search results.

- **family** {**ipv4** | **ipv6**} − Shows the detailed information of the IPv4 or IPv6 policy rules. Note: This keyword is available only when the system version is IPv6.

- [**schedule-name***schedule-name*] − Shows the detailed information about the rule with the specified schedule name.

- [**schedule-name-filter***filter-schedule-name*] − Shows the detailed information about all rules whose schedule name contains the specified keyword.

Notes:

- Fuzzy query and precise query are mutually exclusive and cannot be selected at the same time.
- If the filter condition User is selected together with other filter conditions (relationship between each filter condition is **AND**), filter condition User should be placed last.

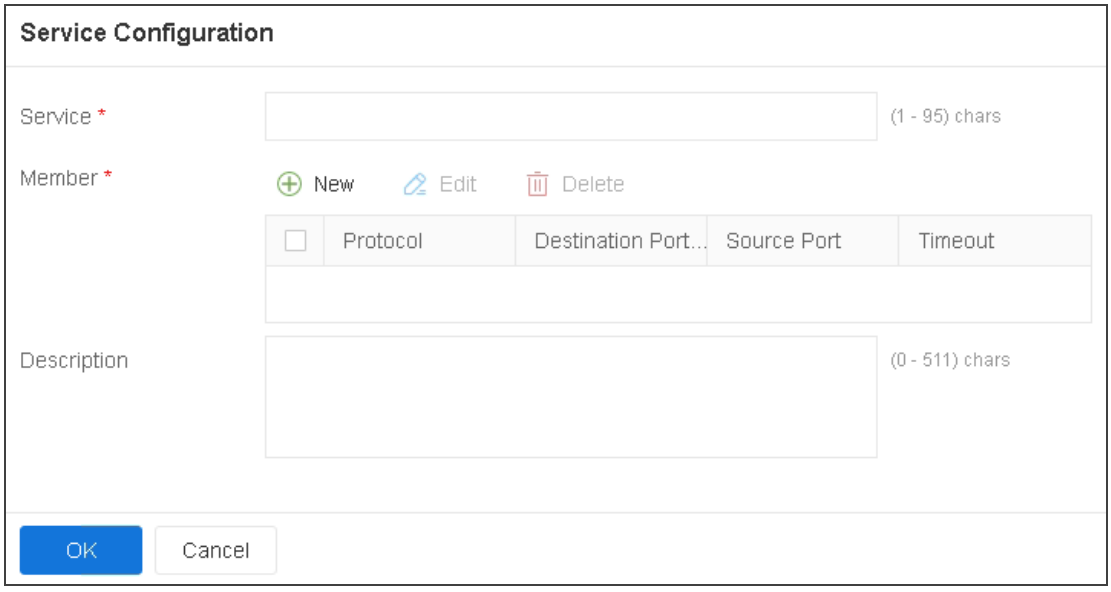
For more information, refer to the **Policy** > **Security Policy** > **Viewing Policy Rule Information** section in *StoneOS CLI User Guide*. FR 40264

Support to Set Timeout Values for Custom Services Based on an Hourly Configuration.

WebUI

Configuring a User-defined Service

1. Select **Object** > **Service Book** > **Service**.
2. Click **New**.



Service Configuration	
Service	Type the name for the user-defined service into the textbox.
Member	Specify a protocol type for the user-defined service. The available options include TCP, UDP, ICMP, ICMPv6 and All. If needed, you can add multiple service items. Click **New** and the parameters for the protocol types are described as follows:
	TCP/UDP Destination port: • Min - Specifies the minimum port number of the specified service entry. • Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535. Source port:

Service Configuration		
		• Min - Specifies the minimum port number of the specified service entry. • Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535. **Notes:** • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. • Timeout: When the policy references a service or application, the system will establish a session and

		retrieve the timeout period once traffic matches the referenced entry. If the session exceeds the timeout, it will be closed to prevent idle sessions from consuming too many system resources, which could impact performance. The system prioritizes the timeout period in the following order: service > application > protocol. It will use the default timeout period for service, application, or protocols as the timeout period of the session. This configuration is used to specify the timeout period for services. The system supports configuration in three time units:

		seconds, hours, and days. The configuration ranges are 1 to 65,535 seconds, 1 to 24,000 hours, and 1 to 1,000 days, respectively. The default value is 0, which indicates that the service's timeout is not effective, and the system will use the application timeout as the session timeout based on priority. For timeout periods equal to or greater than 24 hours, the session is considered a long-duration session. In such cases, the system sets the session timeout based on the proportion of long-duration sessions to total sessions on the device. The default proportion is 0, which indicates that no long-duration sessions can

Service Configuration		
		be created. Before configuring the timeout for long-duration sessions, the session proportion needs to be set. For more information, see Global Network Parameters. • If the session proportion is not reached, the system will use the service's timeout as the session timeout. • Once the session proportion is reached, the system will apply the protocol's default timeout as the session timeout.
	ICMP	• Type: Specifies an ICMP type for the service entry. The value range is 0（Echp-Reply）, 3（Destin-

<table>
<tr><th colspan="3">Service Configuration</th></tr>
<tr><td></td><td></td><td>ation-Unreachable），4（Source Quench），5（Redirect），8（Echo），11（Time Exceeded），12（Parameter Problem），13（Timestamp），14（Timestamp Reply），15（Information Request），16（Information Reply），17（Address Mask Request），18（Address Mask Reply），30（Traceroute），31（Datagram Conversion Error），32（Mobile Host Redirect），33（IPv6 Where-Are-You），34（IPv6 I-Am-Here），35（Mobile Registration Request），36（Mobile Registration Reply）.
• Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 15, the default value is : min code - 0, max code - 15.
Notes:
• The minimum port number cannot exceed the maximum port number.
• The "Min" of the des-</td></tr>
</table>

		tination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. • Timeout: When the policy references a service or application, the system will establish a session and retrieve the timeout period once traffic matches the referenced entry. If the session exceeds the timeout, it will be closed to prevent idle sessions from consuming too many system resources, which could impact performance. The system prioritizes the timeout period in the following order: service >

		application > protocol. It will use the default timeout period for service, application, or protocols as the timeout period of the session. This configuration is used to specify the timeout period for services. The system supports configuration in three time units: seconds, hours, and days. The configuration ranges are 1 to 65,535 seconds, 1 to 24,000 hours, and 1 to 1,000 days, respectively. The default value is 0, which indicates that the service's timeout is not effective, and the system will use the application timeout as the session timeout based on priority. For timeout periods equal

		to or greater than 24 hours, the session is considered a long-duration session. In such cases, the system sets the session timeout based on the proportion of long-duration sessions to total sessions on the device. The default proportion is 0, which indicates that no long-duration sessions can be created. Before configuring the timeout for long-duration sessions, the session proportion needs to be set. For more information, see Global Network Parameters. • If the session proportion is not reached, the system will use the service's timeout as the session timeout.

Service Configuration		
		• Once the session proportion is reached, the system will apply the protocol's default timeout as the session timeout.
	ICMPv6	• Type: Specifies an ICMPv6 type for the service entry. The value range is 1（Dest-Unreachable）, 2（Packet Too Big）, 3（Time Exceeded）, 4（Parameter Problem）, 5-99 (Unallocated Error message), 100（Private experimentation）, 101（Private experimentation）, 102-126 (Unallocated Error message), 127（Reserved for expansion of ICMPv6 error message）, 128（Echo Request）, 129（Echo Reply）, 130（Multicast Listener Query）, 131（Multicast Listener Report）, 132（Multicast Listener Done）, 133（Router Solicitation）, 134（Router Advertisement）, 135（Neighbor Solicitation）, 136（Neighbor

Service Configuration		
		Advertisement）, 137（Redirect Message）, 138（Router Renumbering）, 139（ICMP Node Information Query）, 140（ICMP Node Information Response）, 141（Inverse Neighbor Discovery Solicitation Message）, 142（Inverse Neighbor Discovery Advertisement Message）, 143（Version 2 Multicast Listener Report）, 144（Home Agent Address Discovery Request Massage）, 145（Home Agent Address Discovery Reply Massage）, 146（Mobile Prefix Solicitation）, 147（Mobile Prefix Advertisement ）, 148（Certification Path Solicitation Message）, 149（Certification Path Advertisement Message）, 150（ICMP message utilized by experimental mobility protocols such as Seamoby）, 151（Multicast Router Advertisement）, 152（Multicast Router Solicitation ）, 153（Multicast Router Termination）, 154（FMIPv6 Messages）, 200（Private experimentation）, 201（Private experimentation）and

- Code: Specifies a minimum value and maximum value for ICMPv6 code. The value range is 0 to 255, the default value is : min code - 0, max code - 255.

Notes:

- The minimum code cannot exceed the maximum code.
- If "Max " is not configured, system will use "Min" as the single code.
- Timeout: When the policy references a service or application, the system will establish a session and retrieve the timeout period once traffic matches the referenced entry. If the session exceeds the timeout, it will be closed to prevent idle sessions from con-

		suming too many system resources, which could impact performance. The system prioritizes the timeout period in the following order: service > application > protocol. It will use the default timeout period for service, application, or protocols as the timeout period of the session. This configuration is used to specify the timeout period for services. The system supports configuration in three time units: seconds, hours, and days. The configuration ranges are 1 to 65,535 seconds, 1 to 24,000 hours, and 1 to 1,000 days, respectively. The default value is 0,

		which indicates that the service's timeout is not effective, and the system will use the application timeout as the session timeout based on priority. For timeout periods equal to or greater than 24 hours, the session is considered a long-duration session. In such cases, the system sets the session timeout based on the proportion of long-duration sessions to total sessions on the device. The default proportion is 0, which indicates that no long-duration sessions can be created. Before configuring the timeout for long-duration sessions, the session proportion needs to be set. For more information, see Global Network

Service Configuration		
		Parameters. • If the session proportion is not reached, the system will use the service's timeout as the session timeout. • Once the session proportion is reached, the system will apply the protocol's default timeout as the session timeout.
	All	• Protocol: Specifies a protocol number for the service entry. The value range is 1 to 255. • Timeout: When the policy references a service or application, the system will establish a session and retrieve the timeout period once traffic matches the referenced entry. If the

		session exceeds the timeout, it will be closed to prevent idle sessions from consuming too many system resources, which could impact performance. The system prioritizes the timeout period in the following order: service > application > protocol. It will use the default timeout period for service, application, or protocols as the timeout period of the session. This configuration is used to specify the timeout period for services. The system supports configuration in three time units: seconds, hours, and days. The configuration ranges are 1 to 65,535 seconds, 1 to 24,000 hours, and 1 to 1,000 days, respectively. The default value is 0, which indicates that the service's timeout is not effective, and the system will use the application timeout as the session timeout based on priority. For timeout periods equal to or greater than 24 hours, the session is

Service Configuration		
		considered a long-duration session. In such cases, the system sets the session timeout based on the proportion of long-duration sessions to total sessions on the device. The default proportion is 0, which indicates that no long-duration sessions can be created. Before configuring the timeout for long-duration sessions, the session proportion needs to be set. For more information, see Global Network Parameters. • If the session proportion is not reached, the system will use the service's timeout as the session timeout. • Once the session proportion is reached, the system will apply the protocol's default timeout as the session timeout.
Description	If it's needed, type the description for the service into the text box.	

3. Click **OK**.

For more information, refer to the **Object** > **Service Book** > **Configuring a Service Book** > **Configuring a User-defined Service** section in *StoneOS WebUI User Guide*. FR 40517

CLI

Adding/Deleting a User-defined Service Entry

The command that is used to add a service entry may vary from different protocol types of the service entries.

To add a service entry of TCP or UDP type, in the service configuration mode, use the following command:

{**tcp** | **udp**} **dst-port***min-port* [*max-port*] [**src-port***min-port* [*max-port*]] [**timeout***time-out-value* | **timeout-hour***time-out-value* | **timeout-day***time-out-value*]

- **dst-port***min-port* [*max-port*] – Specifies the destination port number of the user-defined service. If the destination port number is a number range, then *min-port* is the minimum destination port number, and *max-port* is the maximum destination port number. The value range is 0 to 65535, and the destination port number should not be a single 0. For example, the destination port number can be 0 to 20, but cannot only be 0.
- **src-port***min-port* [*max-port*] – Specifies the source port number of the user-defined service. If the source port number is a number range, then *min-port* is the minimum source port number, and *max-port* is the maximum source port number. The value range is 0 to 65535.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-hour***time-out-value* – Specify the timeout value. The unit is hour. The value varies from 1 to 24000. The connection will disconnect after the timeout. For timeout periods equal to or greater than 24 hours, the session is considered a persistent session. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent

sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.

- **timeout-day***time-out-value* – Specify the timeout value. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.

To add a service entry of ICMP type, in the service configuration mode, use the following command:

icmp type*type-value* [**code***min-code* [*max-code*]] [**timeout***time-out-value* | **timeout-hour***time-out-value* | **timeout-day***time-out-value*]

- *type-value* – Specifies the ICMP type value of the user-defined service. The value range is 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp), 15 (Information) and any (all the above type values).
- **code** *min-code* [*max-code*] – Specifies the ICMP code value for the user-defined service. The value range is 0 to 5.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-hour***time-out-value* – Specify the timeout value. The unit is hour. The value varies from 1 to 24000. The connection will disconnect after the timeout. For timeout periods equal to or greater than 24 hours, the session is considered a persistent session. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.
- **timeout-day***time-out-value* – Specify the timeout value. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. To configure the timeout value of

persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.

To add a service entry of other types, in the service configuration mode, use the following command:

protocol*protocol-number* [**timeout***time-out-value* | **timeout-hour***time-out-value* | **timeout-day***time-out-value*]

- *protocol-number* – Specifies the protocol number of the user-defined service. The value range is 1 to 255.
- **timeout** *time-out-value* – Specify the timeout value. The unit is second. The value varies from 1 to 65525. The connection will disconnect after the timeout.
- **timeout-hour***time-out-value* – Specify the timeout value. The unit is hour. The value varies from 1 to 24000. The connection will disconnect after the timeout. For timeout periods equal to or greater than 24 hours, the session is considered a persistent session. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.
- **timeout-day***time-out-value* – Specify the timeout value. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.

To delete the specified service entry, use one of the following commands. The service entries can only be deleted but cannot be edited.

- **no** {**tcp** | **udp**} **dst-port***min-port* [*max-port*] [**src-port***min-port* [*max-port*]]
- **no icmp type***type-value* [**code***min-code* [*max-code*]]
- **no protocol***protocol-number*

For more information, refer to the **Firewall** > **Service and Application** > **Service Overview** > **User-defined Service** topic in *StoneOS CLI User Guide*. FR 40517

Configuring an IPv6 Service

StoneOS includes some new predefined services in the service book to support IPv6 service; besides it also supports IPv6 ports for some network applications. To view all the supported predefined services and service groups, use the command **show service predefined** and **show servgroup predefined** respectively. A service group can contain both IPv4 and IPv6 services. You can also create a user-defined IPv6 service (ICMPv6) as needed.

Tips: For more information about the configuration of IPv4 service book, see "Application and Service" of "Firewall".

For more information about how to create a user-defined ICMPv6 service, see the section below:

To create a user-defined service and enter the user-defined service configuration mode, in the global configuration mode, use the following command:

service*service-name*

If the specified service already exists, the system will directly enter the user-defined service configuration mode.

To add an ICMPv6 service, in the user-defined configuration mode, use the following command:

icmpv6 type*type-value* [**code** *min-code* [*max-code*]] [**timeout***time-out-value* | **timeout-hour***time-out-value* | **timeout-day***time-out-value*]

- *type-value* – Specifies the ICMPv6 type value. For more information about the value range, see Appendix 1: ICMPv6 Type and Code. The default value is Any, which indicates all the ICMPv6 type values.
- **code** *min-code* [*max-code*] – Specifies the minimum code value (*min-code*) and maximum code value (*max-code*) for ICMPv6. The value range is 0 to 6 and Any (any ICMPv6 code value). If the code value is not specified, by default the system will use the code value that

corresponds to the Type value (defined in RFC); if the maximum code value is not specified, by default the system will use the minimum code value as the maximum code value.

- **timeout** *time-out-value* – Specifies the timeout value. The unit is second. Valid values: 1 to 65535. The connection will disconnect after the timeout.
- **timeout-hour***time-out-value* – Specify the timeout value. The unit is hour. The value varies from 1 to 24000. The connection will disconnect after the timeout. For timeout periods equal to or greater than 24 hours, the session is considered a persistent session. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.
- **timeout-day***time-out-value* – Specify the timeout value. The unit is day. The value varies from 1 to 1000. The connection will disconnect after the timeout. To configure the timeout value of persistent sessions, you need to configure the session proportion of persistent sessions in global configuration mode first. For more information, see Creating/Deleting a User-defined Service.

To delete the specified ICMPv6 service, in the user-defined configuration mode, use the following command:

no icmpv6 type*type-value* [**code** *min-code* [*max-code*]][**timeout** *timeout-value*]

For more information, refer to the **IPv6 > Configuring an IPv6 Policy Rule** topic in *StoneOS CLI User Guide*. FR 40517

Adding Session List for Displaying Session Information and Supporting to Filter the Show/Clear Session Information Command by Protocol

WebUI

Session List

Select **Monitor** > **Device Monitor** > **Session List**. To better understand the device's current session information, you can view detailed statistics for all current sessions on this page.

- For X-series devices and K9180 and K6580 devices, you can select a slot from the **Slot** drop-down list to view the current session information about different modules.
- Select a slot from the **Slot** drop-down list to view the current session information about different modules.
- Click 

to add filter conditions, and information matching the filter conditions will be displayed in the session list.
- Click the policy ID of a specific session to configure the policy for this session. For more information, see Configuring the Policy Rule.
- Click the SNAT ID of a specific session to configure SNAT for this session. For more information, see Configuring SNAT. By default, the SNAT ID column is hidden. To display a specified column, refer to the Conventions > Common Controls section.
- Click the DNAT ID of a specific session to configure DNAT for this session. For more information, see Configuring the Advanced Configurations of the NAT Rule. To display a specified column, refer to the Conventions > Common Controls section.

For more information, refer to the **Monitor** > **Monitor** > **Device Monitor** topic in *StoneOS WebUI User Guide*. FR 40272

Showing Session Information

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

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

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

show session [**id***number* [*end-id*]] [**src-ip***A.B.C.D* [*netmask* | *wildcard*]] [**dst-ip***A.B.C.D* [*netmask* | *wildcard*]] [**protocol** {**icmp** | **icmpv6** | **sctp** | **tcp** | **udp** | *protocol-number*}] [**src-port***port-number* [*port-number*]] [**dst-port***port-number* [*port-number*]] [**src-mac***src-mac-address*] [**dst-mac***dst-mac-address*] [**src-zone***zone-name*] [**dst-zone***zone-name*] [**application***name*] [**policy***policy-id*] [**vrouter***vrouter-name*] [**vsys***vsys-name*] [{**flow0-interface** | **flow1-interface**} *interface-name*] [**cpu***cpu-number*] [**slot***slot-number*] [**ipv4**] [**ipv6**] [**snat-rule***id*] [**dnat-rule***id*] [**bnat-rule***id*] [**detail**] [**tcp-state-3handshake**] [**tcp-state-established**] [**tcp-state-closing**]

- **id** *number* [*end-id*] – Shows the session information of the specified ID. To show the session information of a specified range of IDs, continue entering the end ID of the range.
- **src-ip***A.B.C.D* – Shows the session information of the specified source IP address or specified range of IP addresses.
- **dst-ip***A.B.C.D* – Shows the session information of the specified destination IP address or specified range of IP addresses.
- *netmask* | *wildcard* – Specifies the netmask or the wildcard mask.
- **protocol** {**icmp** | **icmpv6** | **sctp** | **tcp** | **udp** | *protocol-number*} – Shows the session information of the specified protocol. The session information can be filtered by ICMP (icmp),

ICMPv6 (icmpv6), SCTP (sctp), TCP (tcp), UDP (udp), and protocol numbers. The protocol number ranges from 1 to 255. You can specify the ICMPv6 protocol only for the IPv6 version.

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

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

Clearing Session Information

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

clear session [**h323**] [**id***number* [*end-id*]] [**src-ip***A.B.C.D* [*netmask* | *wildcard*]] [**dst-ip***A.B.C.D* [*netmask* | *wildcard*]] [**protocol** {**icmp** | **icmpv6** | **sctp** | **tcp** | **udp** | *protocol-number*}] [**src-port***port-number* [*port-number*]] [**dst-port***port-number* [*port-number*]] [**vrouter***vrouter-name*] [**vsys***vsys-name*] [**cpu***cpu-number*] [**slot***slot-number*] [**ipv4**] [**ipv6**] [**detail**]

- **h323** – Clears the H323 session information.
- **id***number* [*end-id*] – Clears the session information of the specified ID. To show the session information of a specified range of IDs, continue entering the end ID of the range.

- **src-ip***A.B.C.D* – Clears the session information of the specified source IP address or specified range of IP addresses.
- **dst-ip***A.B.C.D* – Clears the session information of the specified destination IP address or specified range of IP addresses.
- *netmask* | *wildcard* – Clears the netmask or the wildcard mask.
- **protocol** {**icmp** | **icmpv6** | **sctp** | **tcp** | **udp** | *protocol-number*} – Clears the session information of the specified protocol. The session information can be filtered by ICMP (icmp), ICMPv6 (icmpv6), SCTP (sctp), TCP (tcp), UDP (udp), and protocol numbers. The protocol number ranges from 1 to 255. You can specify the ICMPv6 protocol only for the IPv6 version.
- **src-port***port-number* [*port-number*] – Clears the session information of the specified source port or specified range of port.
- **dst-port***port-number* [*port-number*] – Clears the session information of the specified destination port or specified range of port.
- **vrouter***vrouter-name* – Clears the session information of the specified virtual router.
- **vsys***vsys-name* – Clears the session information of the specified VSYS.
- **slot***slot-number* – Clears the session information of the specified slot.
- **cpu***cpu-number* – Clears the session information of the specified CPU.
- **ipv4** – Clears the session information of the IPv4 protocol.
- **ipv6** – Clears the session information of the IPv6 protocol.
- **detail** – Clears the detail session information.

For more information, refer to the **Firewall** > **StoneOS Architecture** topic in *StoneOS CLI User Guide*. FR 40272

The Backup Device Supports to Execute the Main and Backup Switching Command

CLI

Manually Switching Main and Backup Device Status of HA

To switch main and backup device status of HA manually, in any mode, use the following command:

exec ha master switch-over

Notes:

- For certain Hillstone devices (SG-6000-K9180/K20803, and X series), this command can be executed only on the master SCM.
- Only devices in the master and backup statuses can execute this command.
- This command is only supported in Active-Passive (A/P) mode.
- Regardless of the priority values set for the master and backup devices before the switchover, after the switchover, the system will set the master device's **priority** to 100 and the backup device's **priority** to 150.
- As the switching operation executes, this device is executing batch synchronization or some Hillstone devices (SG-6000-K9180/K20803, and X series) are executing batch synchronization of SCM, which will result in failed switching of HA main and backup device status.

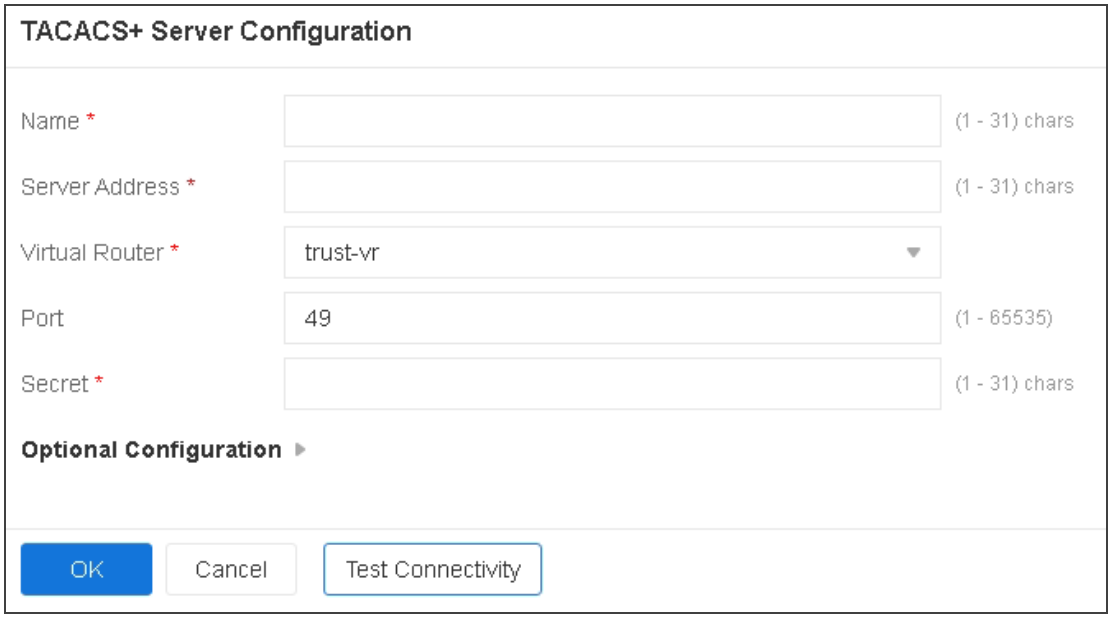
For more information, refer to the **High Availability (HA)** > **Configuring HA** topic in *StoneOS CLI User Guide*. FR 40185

Supporting to Send Operation Commands on the CLI to the TACACS+ Server

WebUI

Configuring TACACS+ Server

1. Select **Object > AAA Server**.
2. Click **New > TACACS+ Server**, and the **TACACS+ Server Configuration** page opens.



Configure the following.

Basic Configuration	
Server Name	Enter a name for the TACACS+ server.
Server Address	Specify the IPv4 address, IPv6 address, or domain name for the TACACS+ server.
Virtual Router	Specify the VRouter of TACACS+ server.

Port	Enter port number for the TACACS+ server. The default value is 49. The value range is 1 to 65535.
Secret	Enter the shared secret to connect the TACACS+ server.
Optional	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role mapping rule	Select a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup Server 1 (2)	Enter the IPv4 address, IPv6 address, or domain name for the backup TACACS+ server 1(or 2). The types of backup server and primary server are the same, which are TACACS+ servers. When the authentication fails via the primary server, the

	authentication is performed by using the backup server 1 and 2 in sequence.
Virtual Router 1 (2)	Select the VRouter for the backup server.
Command Line Audit	When you configure the device via command lines, incorrect operations may cause network issues. Once the Command Line Audit function is enabled, the system sends information about the executed commands to the corresponding TACACS+ server. You can review these command logs to troubleshoot network issues. Click the button to enable the Command Line Audit function, which is disabled by default. **Notes:** The Command Line Audit function only applies to users authenticated via the TACACS+ server.

For more information, refer to the **Object** > **AAA Server** > **Configuring TACACS+ Server** section in *StoneOS WebUI User Guide*. FR 39803

CLI

Configuring TACACS+ Authentication Server

In global configuration mode, use the command **aaa-server***aaa-server-name***type tacacs+** to enter TACACS+ server configuration mode.

Configuration of TACACS+ server includes:

- Configuring IP or Domain Name of Primary Authentication Server
- Configuring IP or Domain Name of Backup Server 1
- Configuring IP or Domain Name of Backup Server 2
- Configuring Port of TACACS+ Server
- Configuring Secret of TACACS+ Server
- Specifying User Name Format
- Configuring Role Mapping Rule
- Configuring the Brute-force Cracking Defense
- Configuring Command Line Audit

Enabling/Disabling Command Line Audit

> **Notes:** The Command Line Audit function only applies to users authenticated via the TACACS+ server.

When you configure the device via command lines, incorrect operations may cause network issues. Once the Command Line Audit function is enabled, the system sends information about the executed commands to the corresponding TACACS+ server. You can review these command logs to troubleshoot network issues. By default, this function is disabled.

To enable/disable the Command Line Audit function, in TACACS+ server configuration mode, use the following command:

- Enable: **accounting-cmd enable**
- Disable: **no accounting-cmd enable**

For more information, refer to the **User Authentication** > **Authentication, Authorization and Accounting** > **Configuring an AAA Server** > **Configuring TACACS+ Authentication Server** topic in *StoneOS CLI User Guide*. FR 39803

The 100GE Interface of Firewall Supports to Configure the FEC Function

WebUI

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network > Interface**.
2. Select the interface you want to edit from the interface list and click **Edit**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the interface.
Description	Enter descriptions for the interface.
Binding Zone	Specifies the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. You can also specify the firewall information (firewall's IPv4 or IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP

Option	Description
	mode and this interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block; • The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, you should also select an aggregate interface/redundant interface: • Aggregate Interface: The interface you specified belongs to a aggregate interface. • Interface: Choose an aggregate interface which the aggregate interface belongs to from Interface drop-down list. • Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the

Option	Description
	members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority. • Port timeout mode: The LACP timeout refers to the time interval for the members The system supports **Fast** (1 second) and **Slow** (30 seconds, the default value) waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. • Redundant Interface: This interface belongs to a redundant interface. Select that redundant interface from the Interface drop-down list. • None: This interface does not belong to any object.
Aggregate mode	• Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally. • Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are:

Option	Description
	• System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be. • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby. • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface needs to be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.

Option	Description
	Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.

DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.

Password: Specifies PPPoE user's password.

Confirm Password: Enter the password again to confirm.

Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet</td></tr>
</table>

Option	Description	
	access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.	
	Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.	
	Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.	
	Advanced	Access concentrator: Specifies a name for the concentrator.
		Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.
		Netmask: Specifies a netmask for the IP address obtained via PPPoE.
		Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Service: Specifies allowed service. The specified service needs to be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td colspan="2">WebAuth</td></tr>
<tr><td>Auth Service</td><td>Click the Enable， Close or Global Default radio button as needed.
Enable：Enable the WebAuth function of the specified interface.
Close：Disable the WebAuth function of the specified</td></tr>
</table>

Option	Description
	interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authen-

Option	Description
	tication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "StoneOS 5.5R11F3" on Page 3

5. Expand Interface Properties, configure properties for the interface.

Property	Description
Duplex	Specifies a duplex working mode for the interface. Options include auto, full duplex, and half duplex. Auto is the default working mode, in which the system will select the most appropriate duplex working mode automatically. 1000M half duplex is not supported.
Rate	Specifies a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported. For 1GE(SFP) optical port of certain A-series devices, you can set the data rate to 100 Mbps or 1,000 Mbps. The default data rate is 1000 Mbps. When you set the data rate to 100 Mbps, the optical port can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers. **Note**: Only the following devices allow you to backward switch the data rate of 1GE(SFP) optical port: SG-6000-A5500, A5200, A5100, A3800, A3700, A3600, A3000, A2800, and A2700.

Property	Description
Channel-Speed	Converts the data rate of 10GE (SFP+) optical interfaces. • 1G: Convert the data rate of 10GE (SFP+) optical interfaces from 10Gbps to 1Gbps. • Close: Do not convert the data rate of the 10GE (SFP+) optical interface, which is 10Gbps by default.
Optical Interface to Electrical Interface	This option applies to the X8180 devices' 10GE (SFP+) optical port, and by default, Optical Interface to Electrical Interface function is disabled. To enable this function, take the following steps: 1. Insert a copper SFP module. 2. Channel-Speed option is configured to "1G". 3. Click the **Enable** button, convert optical port to electrical port.
FEC	**Device Supported:** : This function is only applicable to the following models with 100GE (QSFP28) interfaces. • A series some models: SG-6000-A7600/A6800 • K series some models: SG-6000-K9180 • X series some models: SG-6000-X20812/X20803/X9180/X8180 FEC (Forward Error Correction) is an error correction tech-

Property	Description

	nique used for data transmission. It processes the original data with encoding at the sender's end, adding error correction information. At the receiver, this error correction information is used to correct errors that occur during data packet transmission, restoring the original data and thus improving signal quality.
	The FEC modes that you can configure are as follows:
	• Automatic: Set the FEC function to automatic mode, which is the default mode. The system will automatically set the FEC mode of the interface based on different transceiver modules, as follows:
	  • TRAN-LR4-QSFP28: Automatically set to off mode.
	  • The remaining Hillstone Networks transceiver modules: automatically set to RS mode.
	• RS: Specify the FEC function as RS mode. RS mode has a more complex encoding rule, providing strong error correction capabilities but may also cause packet delay. Suitable for 100GE interfaces, and 25GE interfaces split from 100GE interfaces.
	• Base-R: Specifies the FEC function as Base-R mode. The encoding rules of Base-R mode are relatively simple, with weaker error correction capability and lower computational complexity. It is only applicable to 25GE inter-

Property	Description
	faces split from 100GE interfaces. • Off: Disable the FEC function. Note: • 100GE interface converted to 40GE interface cannot configure FEC function. • The FEC mode of the interfaces at both ends of the link needs to be consistent; otherwise, the link will not be able to connect and operate normally.
Combo type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: • Auto: The above default scenario. • Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this option configured, the device will migrate the traffic on the copper port to the fiber port automatically without reboot.

Property	Description
MTU	The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.

Property	Description
MAC clone	The system clones a MAC address to the Ethernet sub-interface. If the user clicks "Restore Default MAC," the Ethernet sub-interface will restore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of the HA master device forwards traffic with the virtual MAC address provided by the system. You can configure a custom HA MAC address. In the HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. Note: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Band-	Specifies the maximum value of the down bandwidth of the inter-

Property	Description
width	face.

6. "StoneOS 5.5R11F3" on Page 3

> **Notes:** Non-root VSYS does not support this configuration.

7. "StoneOS 5.5R11F3" on Page 3
8. "StoneOS 5.5R11F3" on Page 3
9. "StoneOS 5.5R11F3" on Page 3
10. "StoneOS 5.5R11F3" on Page 3
11. Click **OK**.

Notes:

- Before deleting an aggregate/redundant interface, you must cancel other interfaces' bindings to it, aggregate/redundant sub-interface's configuration, its IP address configuration, and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.
- When a VSwitch interface is deleted, the corresponding VSwitch will be deleted as well.
- The HA interface cannot bind the track object.

For more information, refer to the **Network** > **Interface** > **Configuring an Interface** topic in *StoneOS WebUI User Guide*. FR 39672

Configuring the FEC Mode of the Interface

Device Supported: :

This function is only applicable to the 100GE (QSFP28) interfaces.

- A series some models: SG-6000-A7600/A6800
- K series some models: SG-6000-K9180
- X series some models: SG-6000-X25812/X25803/X9180/X8180

FEC (Forward Error Correction) is an error correction technique used for data transmission. It processes the original data with encoding at the sender, adding error correction information. At the receiver, this error correction information is used to correct errors that occur during data packet transmission, restoring the original data and thus improving signal quality.

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

fec-mode {**auto** | **base-r-enable** | **rs-enable** | **disable**}

- **auto** – Specifies the FEC function to operate in auto mode, which is the default mode. The system automatically sets the FEC mode of the interface based on different transceiver modules, as follows:
  - TRAN-LR4-QSFP28: Automatically set to off mode.
  - Other Hillstone Networks transceiver modules: Automatically set to RS mode.

- **base-r-enable** – Specifies the FEC function to operate in Base-R mode. The encoding rules of Base-R mode are relatively simple, with weaker error correction capabilities and lower computational complexity. It is only applicable to 25GE interfaces split from 100GE interfaces.
- **rs-enable** – Specifies the FEC function as RS mode. The encoding rules of RS mode are more complex, providing stronger error correction capabilities, but may also cause packet delay. Suitable for 100GE interfaces, and 25GE interfaces split from 100GE interfaces.
- **disable** – Specifies that the FEC function is in the disabled state.

In interface configuration mode, use the **nofec-mode** command to restore the FEC function to its default mode.

Notes:

- 100GE interface converted to 40GE interface cannot configure FEC function.
- The FEC mode of the interfaces at both ends of the link need to be consistent; otherwise, the link will fail to connect properly.

For more information, refer to the **Firewall** > **Interface** > **Switching Interface Work Mode** section in *StoneOS CLI User Guide*. FR 39672

MIB

HILLSTONE-IF-MIB

The following tables is the parsing results of HILLSTONE-IF-MIB.

Name	OID	Value
hillstoneWanIfNumber	.1.3.6.1.4.1.28557.2.6.1.1	Data type: Integer32 Description: Number of interfaces

Name	OID	Value
		bound to WAN Zone
hillstoneLanIfNumber	.1.3.6.1.4.1.28557.2.6.1.2	Data type: Integer32 Description: Number of interfaces bound to other zones (LAN)
hillstoneIfAttriTable: Attributes of all interfaces		
hillstoneIfIndex	.1.3.6.1.4.1.28557.2.6.1.3.1.1	Data type: Integer Description: Interface index, the same as the type of IfIndex node (.1.3.6.1.2.1.2.2.1.1) in IF-MIB (public MIB)
hillstoneIfName	.1.3.6.1.4.1.28557.2.6.1.3.1.2	Data type: String Description: Interface name
hillstoneIfAttribute	.1.3.6.1.4.1.28557.2.6.1.3.1.3	Data type: Integer Description: Type of the binding zone • 0 – Not bound • 1 - LAN Zone • 2 - WAN Zone
hillstoneIfNetAddress	.1.3.6.1.4.1.28557.2.6.1.3.1.4	Data type: IP

Name	OID	Value
		Address Description: Interface IP address
hillstoneIfNetMask	.1.3.6.1.4.1.28557.2.6.1.3.1.5	Data type: IP Address Description: Netmask of the interface IP address
hillstoneIfManageIp	.1.3.6.1.4.1.28557.2.6.1.3.1.6	Data type: IP Address Description: Management IP of the interface (if no management IP is configured, the interface IP will be shown).
hillstoneIfSecIpAddress0	.1.3.6.1.4.1.28557.2.6.1.3.1.7	Data type: IP Address Description: Secondary IP address 0 of the interface
hillstoneIfSecNetMask0	.1.3.6.1.4.1.28557.2.6.1.3.1.8	Data type: IP Address Description: Netmask of secondary IP address 0 of the interface
hillstoneIfSecIpAddress1	.1.3.6.1.4.1.28557.2.6.1.3.1.9	Data type: IP

Name	OID	Value
		Address Description: Secondary IP address 1 of the interface
hillstoneIfSecNetMask1	.1.3.6.1.4.1.28557.2.6.1.3.1.10	Data type: IP Address Description: Netmask of secondary IP address 1 of the interface
hillstoneIfSecIpAddress2	.1.3.6.1.4.1.28557.2.6.1.3.1.11	Data type: IP Address Description: Secondary IP address 2 of the interface
hillstoneIfSecNetMask2	.1.3.6.1.4.1.28557.2.6.1.3.1.12	Data type: IP Address Description: Netmask of the secondary IP address 2 of the interface
hillstoneIfSecIpAddress3	.1.3.6.1.4.1.28557.2.6.1.3.1.13	Data type: IP Address Description: Secondary IP address 3 of the interface
hillstoneIfSecNetMask3	.1.3.6.1.4.1.28557.2.6.1.3.1.14	Data type: IP Address Description: Net-

Name	OID	Value
		mask of secondary IP address 3 of the interface
hillstoneIfSecIpAddress4	.1.3.6.1.4.1.28557.2.6.1.3.1.15	Data type: IP Address Description: Secondary IP address 4 of the interface
hillstoneIfSecNetMask4	.1.3.6.1.4.1.28557.2.6.1.3.1.16	Data type: IP Address Description: Netmask of secondary IP address 4 of the interface
hillstoneIfSecIpAddress5	.1.3.6.1.4.1.28557.2.6.1.3.1.17	Data type: IP Address Description: Secondary IP address 5 of the interface
hillstoneIfSecNetMask5	.1.3.6.1.4.1.28557.2.6.1.3.1.18	Data type: IP Address Description: Netmask of secondary IP address 5 of the interface
HillstoneIfInRate	.1.3.6.1.4.1.28557.2.6.1.3.1.19	Data type: Counter64 Description: Real-time ingress inter-

Name	OID	Value
		face rate. Unit: bps
hillstoneOutRate	.1.3.6.1.4.1.28557.2.6.1.3.1.20	Data type: Counter64 Description: Real-time egress interface rate. Unit: bps
hillstoneInPps	.1.3.6.1.4.1.28557.2.6.1.3.1.21	Data type: Counter64 Description: Real-time packets per second the interface received. Unit: pps
hillstoneOutPps	.1.3.6.1.4.1.28557.2.6.1.3.1.22	Data type: Counter64 Description: Real-time packets per second the interface sent. Unit: pps
hillstoneIfDiscards	.1.3.6.1.4.1.28557.2.6.1.3.1.23	Data type: Counter64 Description: Hardware packet loss data of the physical interface.
hillstoneIfInRateIPv4	.1.3.6.1.4.1.28557.2.6.1.3.1.24	Data type: Counter64 Description: IPv4 traffic rate of ingress interface

Name	OID	Value
hillstoneIfInRateIPv6	.1.3.6.1.4.1.28557.2.6.1.3.1.25	Data type: Counter64 Description: IPv6 traffic rate of inbound traffic
hillstoneIfOutRateIPv4	.1.3.6.1.4.1.28557.2.6.1.3.1.26	Data type: Counter64 Description: IPv4 traffic rate of egress interface
hillstoneIfOutRateIPv6	.1.3.6.1.4.1.28557.2.6.1.3.1.27	Data type: Counter64 Description: IPv6 traffic rate of egress interface
hillstoneIfSfpModuleTemperature	.1.3.6.1.4.1.28557.2.6.1.3.1.28	Data type: DisplayString Description: Current temperature of the transceiver module.
hillstoneIfSfpTxSupplyVoltage	.1.3.6.1.4.1.28557.2.6.1.3.1.29	Data type: DisplayString Description: The supply voltage of the transmitting transceiver module.
hillstoneIfSfpTxBiasCurrent	.1.3.6.1.4.1.28557.2.6.1.3.1.30	Data type: DisplayString

Name	OID	Value
		Description: The bias current of the transmitting transceiver module.
hillstoneIfTxOpticalPower	.1.3.6.1.4.1.28557.2.6.1.3.1.31	Data type: DisplayString Description: The optical power of the transmitting transceiver module
hillstoneIfRxOpticalPower	.1.3.6.1.4.1.28557.2.6.1.3.1.32	Data type: DisplayString Description: The optical power of the receiving transceiver module
hillstoneIfFecmode	.1.3.6.1.4.1.28557.2.6.1.3.1.56	Data type: Integer Description: The FEC mode of the interface Supported platform: A7600, A6800, K9180, X25812, X25803, X9180, X8180

For more information, refer to *StoneOS SNMP Private MIB Reference Guide*. FR 39672

Supporting to Enable or Disable the Logging Function for Policies Globally

WebUI

Policy Global Configuration

The global configuration of policies includes:

- Switching between multi-zone and single-zone
- Security Policy Matching Destination Addresses After DNAT
- Enabling/Disabling traffic statistics of policies
- Enabling/Disabling the Delay Address Update Time Function
- Enabling/Disabling Logging in Policy Global Configuration

Enabling/Disabling Logging in Policy Global Configuration

Before you start:

- Before using this function, ensure that the system's traffic log function is enabled, i.e., session logs, NAT logs, and URL logs need to be enabled on the **Monitor** > **Log** > **Log Management** page.

The system can log the matching conditions of traffic against policy rules via the log function in individual policies. However, due to potential human oversight, some policies may have logging enabled or disabled incorrectly. To avoid such issues, the system supports to enable logging in policy global configuration, which allows you to enable or disable logging for all policies. The logging in policy global configuration function consists of the following three functions: Policy Deny, Session Start, and Session End. By default, the logging in policy global configuration function is disabled.

- Policy Deny: For deny-type policy rules, logs the information when traffic matching the policy rule is denied.
- Session Start: For allow-type policy rules, logs the information when traffic matching the policy rule establishes a session.
- Session End: For allow-type policy rules, logs the information when traffic matching the policy rule ends a session.

To enable/disable logging in policy global configuration, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click . From the drop-down list, select **Policy Global Config**.
3. Under "Log", there are three logging options: Deny, Session start, and Session end. After clicking the Enable button for the corresponding function, the logging configuration for all policies will be overridden by the global configuration, and the logging configuration for individual policies will no longer take effect. You will also need to specify whether the mode is Loging or No Loging, with the default being Loging:
   - Loging: Enables the Logging function to log the corresponding information.
   - No Logging: Disables the Logging function.

   To disable the logging in policy global configuration function, click the Enable button again for the corresponding function. This way, logging will follow the configuration in individual policies.
4. Click **OK**.

Notes: The logging in policy global configuration function has a higher priority than the logging function in individual and mini policies. That is, once logging is enabled in the global policy configuration, the corresponding logging configuration in individual or mini policies

will not take effect.

For example, if "Session start" logging is enabled in an individual policy, but the corresponding global logging function is enabled and set to No Logging, then the "Session Start" logging configuration in that individual policy will not take effect, and the system will not log the corresponding information.

For more information, refer to the **Policy** > **Security Policy** > **Policy Global Configuration** section in *StoneOS WebUI User Guide*. FR 40268

CLI

Configuring a Policy Rule

You can configure a policy rule via CLI to control the traffic destined to the device. The configuration includes:

- Switching to the multi-zone mode
- Creating a policy rule
- Editing a policy rule
- Specifying the default action

  ...
- Configuring Policy User-defined Attributes
- Specifying That the Policy Matches the Post-DNAT Destination Address
- Configuring Logging in Policy Global Configuration

Configuring Logging in Policy Global Configuration

Before you start:

- Before using this function, ensure that the system's traffic log function is enabled, i.e., the **logging traffic on** command is executed in global configuration mode.

The system can log the matching conditions of traffic against policy rules via the log function in individual policies. However, due to potential human oversight, some policies may have logging enabled or disabled incorrectly. To avoid such issues, the system supports to enable logging in policy global configuration, which allows you to enable or disable logging for all policies. By default, this function is disabled.

To configure the logging in policy global configuration function, in policy rule configuration mode, use the following command:

global-policy-log {**session-start** | **session-end** | **policy-deny**} {**on** | **off**}

- **session-start** – Applies to permit-type policy rules. It enables the system to generate log information when a session is established.
- **session-end** – Applies to permit-type policy rules. It enables the system to generate log information when a session ends.
- **policy-deny** – Applies to deny-type policy rules. It enables the system to generate log information when traffic is denied by the rule.
- **on** – Specifies the logging in policy global configuration function to be in Logging mode.
- **off** – Specifies the logging in policy global configuration function to be in No Logging mode.

To cancel the configuration of the logging in policy global configuration function, use the **noglobal-policy-log** {**session-start** | **session-end** | **policy-deny**} command.

Notes: The logging in policy global configuration function has a higher priority than the logging function in individual and mini policies. That is, once logging is enabled in the global policy configuration, the corresponding logging configuration in individual or mini policies will not take effect.

For example, if **session-start** logging is enabled in an individual policy, but the

corresponding global logging function is enabled and set to No Logging, then the **session-start** logging configuration in that individual policy will not take effect, and the system will not log the corresponding information.

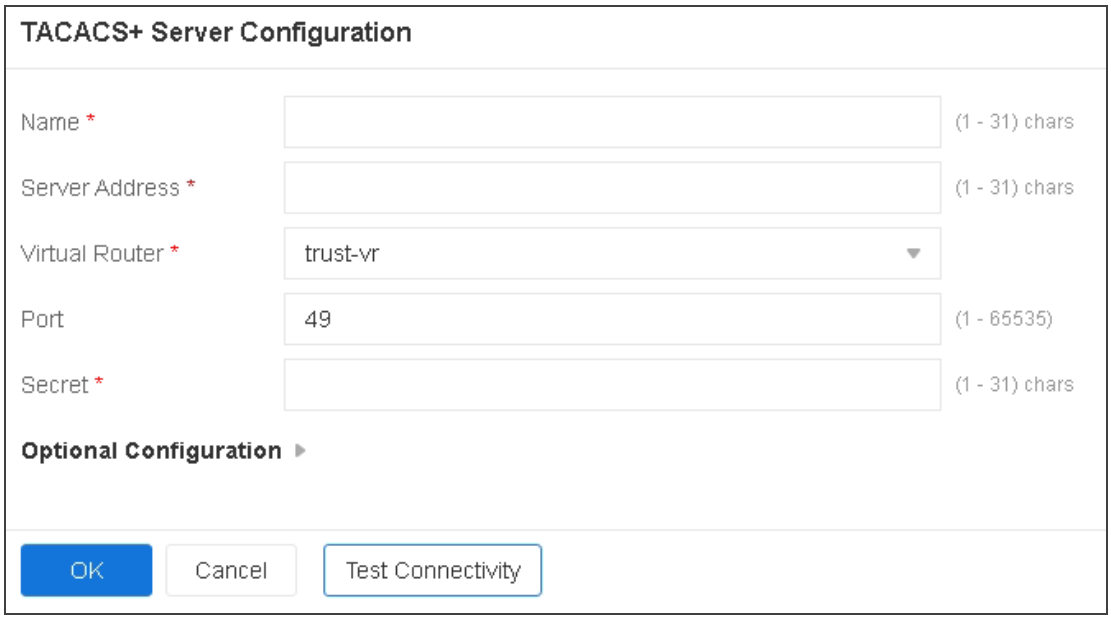
For more information, refer to the **Policy** > **Security Policy** > **Configuring a Policy Rule** section in *StoneOS CLI User Guide*. FR 40268

Supporting to Perform Command Line Authentication for Users Authenticated via the TACACS+ Server

WebUI

Configuring TACACS+ Server

1. Select **Object** > **AAA Server**.
2. Click **New** > **TACACS+ Server**, and the **TACACS+ Server Configuration** page opens.



Configure the following.

Basic Configuration	
Server Name	Enter a name for the TACACS+ server.
Server Address	Specify the IPv4 address, IPv6 address, or domain name for the TACACS+ server.
Virtual Router	Specify the VRouter of TACACS+ server.
Port	Enter port number for the TACACS+ server. The default value is 49. The value range is 1 to 65535.
Secret	Enter the shared secret to connect the TACACS+ server.
Optional	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role mapping rule	Select a role mapping rule for the server. With this option selected, system will allocate a role for the users who have

	been authenticated to the server according to the specified role mapping rule.
Backup Server 1 (2)	Enter the IPv4 address, IPv6 address, or domain name for the backup TACACS+ server 1(or 2). The types of backup server and primary server are the same, which are TACACS+ servers. When the authentication fails via the primary server, the authentication is performed by using the backup server 1 and 2 in sequence.
Virtual Router 1 (2)	Select the VRouter for the backup server.
Command Line Authentication	To enhance the security of command-line operations and impose stricter control over users, the Command Line Authentication function can be configured. Once this function is enabled, every command entered by a user authenticated via the TACACS+ server requires authentication from the TACACS+ server. Commands can only be executed if authenticated by the server; otherwise, they cannot be executed. Click the button to enable the this function, which is disabled by default.
Escape Mode Time	After enabling command line authentication, you can configure the escape mode timeout. When the TACACS+ server is unreachable due to network issues, server failure, or other reasons, the system enters escape mode. In this mode, a timer (escape mode timeout) is

	set, starting from the moment the user first attempts to execute a command and the server is unreachable. During the escape mode timeout, commands entered by the user can be executed without authentication from the TACACS+ server, preventing operational delays caused by authentication service interruptions. Once the escape mode timeout expires, the system returns to the normal authentication process. If the server remains unreachable, the system re-enters the escape mode until the server recovers or the issue is resolved. Enter the escape mode timeout in the text box. Valid values: 0 to 3600 seconds. Default value: 0 seconds, which indicates to disable the escape mode. For example, setting the escape mode timeout to 100 seconds indicates that commands entered by the user within that time frame can be executed without authentication.

For more information, refer to the **Object** > **AAA Server** > **Configuring TACACS+ Server** section in *StoneOS WebUI User Guide*. FR 40143

CLI

Configuring TACACS+ Authentication Server

In global configuration mode, use the command **aaa-server***aaa-server-name***type tacacs+** to enter TACACS+ server configuration mode.

Configuration of TACACS+ server includes:

- Configuring IP or Domain Name of Primary Authentication Server
- Configuring IP or Domain Name of Backup Server 1

- Configuring IP or Domain Name of Backup Server 2
- Configuring Port of TACACS+ Server
- Configuring Secret of TACACS+ Server
- Specifying User Name Format
- Configuring Role Mapping Rule
- Configuring the Brute-force Cracking Defense
- Configuring Command Line Authentication

Configuring Command Line Authentication

To enhance the security of command-line operations and impose stricter control over users, you can configure the Command Line Authentication function. Once this function is enabled, every command entered by a user authenticated via the TACACS+ server requires authentication from the TACACS+ server. Commands can only be executed if authenticated by the server; otherwise, they cannot be executed. The configurations of the Command Line Authentication function include:

- Enabling/Disabling the Command Line Authentication function
- Configuring the Escape Mode time

Enabling/Disabling the Command Line Authentication Function

By default, the Command Line Authentication function is disabled. To enable/disable this function, in TACACS+ server configuration mode, use the following command:

- Enable: **authentication-cmd enable**
- Disable: **no authentication-cmd enable**

Configuring the Escape Mode Time

When the TACACS+ server is unreachable due to network issues, server failure, or other reasons, the system enters escape mode. In this mode, a timer (escape mode time) is set, starting from the moment the user first attempts to execute a command and the server is unreachable. During the escape mode time, commands entered by the user can be executed without authentication from the TACACS+ server, preventing operational delays caused by authentication service interruptions. Once the escape mode time expires, the system returns to the normal authentication process. If the server remains unreachable, the system re-enters the escape mode until the server recovers or the issue is resolved.

To configure the escape mode time, in TACACS+ server configuration mode, use the following command:

authentication-cmd-escape-mode-time*time*

- *time* – Specifies the escape mode time. Valid values: 0 to 3600 seconds. Default value: 0 seconds, which indicates to disable the escape mode.

For more information, refer to the **User Authentication > Authentication, Authorization and Accounting > Configuring an AAA Server > Configuring TACACS+ Authentication Server** topic in *StoneOS CLI User Guide*. FR 40143

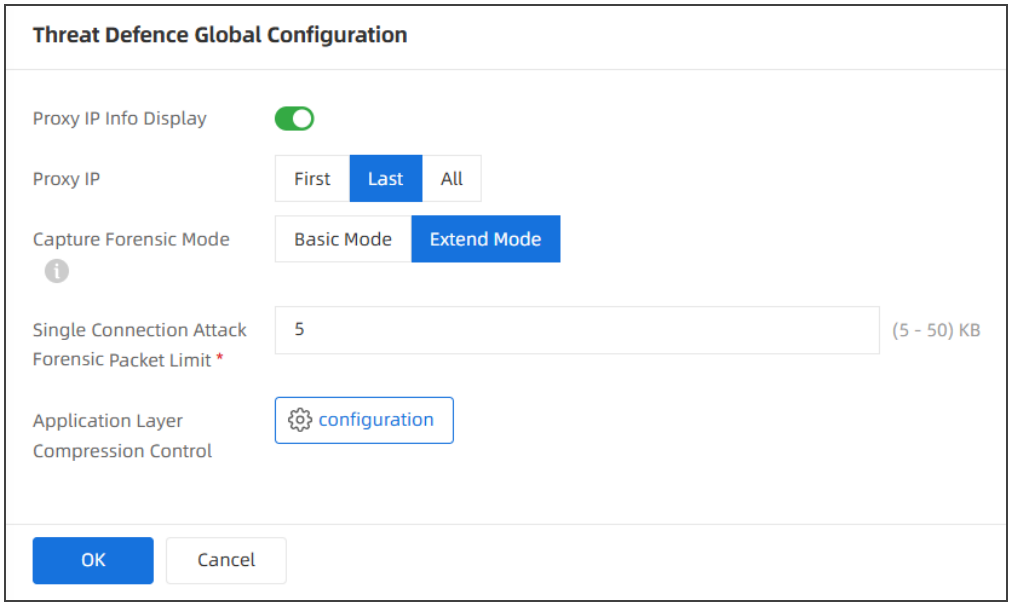
Intrusion Prevention System and Botnet Prevention Support Capture Forensic

WebUI

Configuring The Threat Protection Global Parameters

Configure the global parameters for threat protection, Take the following steps:

1. Click **Object > Threat Detection Template > Threat Defence Global Configuration**, to open the Global Threat Prevention Configuration page.



On the Threat Defence Global Configuration page, configure the parameter information.

Option	Description
Proxy IP Info Display	Click the **Enable** button to enable the proxy IP information display function. Enabling this function allows the system to record proxy IP information in HTTP traffic when a threat event is detected in an HTTP proxy deployment environment. You can view the proxy IP addresses in the threat logs and threat events. This function is enabled by default. **Note:** The proxy IP information display function operates independently and does not affect the recording of HTTP proxy IP functionality or the X-Forwarded-For configuration in CC protection.
Proxy IP	You can choose to record the first, last, or all IP information in the proxy IP. By default, it records all proxy IP

Option	Description
	information. **Note:** After choosing to record all proxy IP information, the system will record and display a maximum of the first 5 proxy IP addresses.
Capture Forensic Mode	Specify the packet capture mode, you can choose Basic Mode or Extended Mode, default is Basic Mode. • Basic mode: The system can capture packets when a threat is detected. For the HTTP protocol, the system will capture request and response packets. • Extended mode: The system can capture packet data before and after a threat is detected. The upper limit of captured packet data can be configured through the "Number of Packets per Connection for Forensics". For the HTTP protocol in botnet detection and intrusion detection functions, the system will capture request and response packets. Note: Packet capture forensics mode only takes effect for Intrusion Prevention System and Botnet Prevention.
Single Connection Attack Forensic Packet Limit	After selecting the extended mode, you need to configure the upper limit of single connection forensic message volume. Once the limit is reached, the earliest captured packet data will be discarded. Specify the upper limit of the amount of data captured each time, with a range of 5-50KB, defaulting to 5KB.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Application Layer Compression Control</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Decompression</td><td>Click/Do not click the "Enable" button to enable/disable the decompression function.</td></tr>
<tr><td>Maximum Compression Layers</td><td>By default, the system can scan up to 5 layers of nested compressed files (up to 20 layers). You need to configure the number of compressions layers that can be scanned using this option. Select the desired number of layers from the drop-down list. The range is 1-20 layers.</td></tr>
<tr><td>Option</td><td>Specify the action to take for compressed files that exceed the maximum compression layer limit. You can choose:
Log Only - Generates only the relevant log information. This behavior is the system default.
Reset Connection - Reset the compressed file connection.</td></tr>
</table>
</td></tr>
</table>

2. Click OK.

For more information, refer to the **Threat Protection** topic in *StoneOS CLI User Guide*. FR 43747

Packet Capture Forensic

Introduction

When threat traffic passes through the device, the system captures relevant threat packets, and you can view or download the captured packets in the corresponding threat logs. You can also enable the cloud platform connection function to upload threat packet data to the cloud, helping you quickly complete threat analysis and handling.

Usage Restrictions and Precautions

General

- For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to Cloud · Jing. Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

Packet capture and evidence collection mode related

- Pcap evidence collection mode only takes effect for the intrusion detection and botnet defense functions.
- When the packet capture mode is set to extended mode, it supports capturing up to 100 packets.

- If the packet capture mode is set to extended, if the threat message data exceeds the configured "maximum number of packets per connection" or exceeds 100 packets, the captured threat message data may be incomplete.
- If the memory used by the packet capture and evidence collection function exceeds one-tenth of the total DP (data plane) memory, regardless of whether the system-configured packet capture and evidence collection mode is basic or extended, the subsequent packet capture and evidence collection mode used when the system detects threats will be basic. (You can use the **show memory detail** command to check the system DP memory usage)

Intrusion Prevention System Function Related

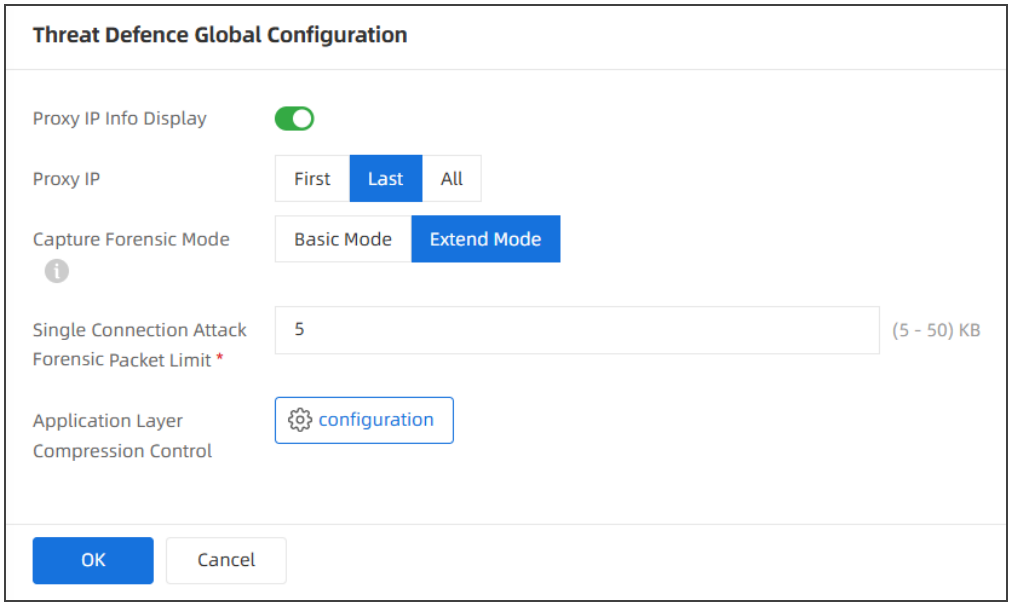
- Bounce shell detection only supports capturing the single packet that detects the threat.
- Weak password detection and HTTP plaintext password detection do not support sending evidence packets to the cloud.

Botnet Prevention Function Related

- TCP protocol detection only supports capturing a single packet that detects a threat.
- Sinkhole malicious IP logs do not support packet capture for evidence.

Configuring Packet Capture Forensic

1. Global Configuration for Packet Capture and Evidence Mode.
    a. Click **Object** > **Threat Prevention Template** > **Threat Prevention Global Configuration** to open the Threat Prevention Global Configuration page.



b. Configure the packet capture mode, you can choose between Basic Mode or Extend Mode. The default is Basic Mode.

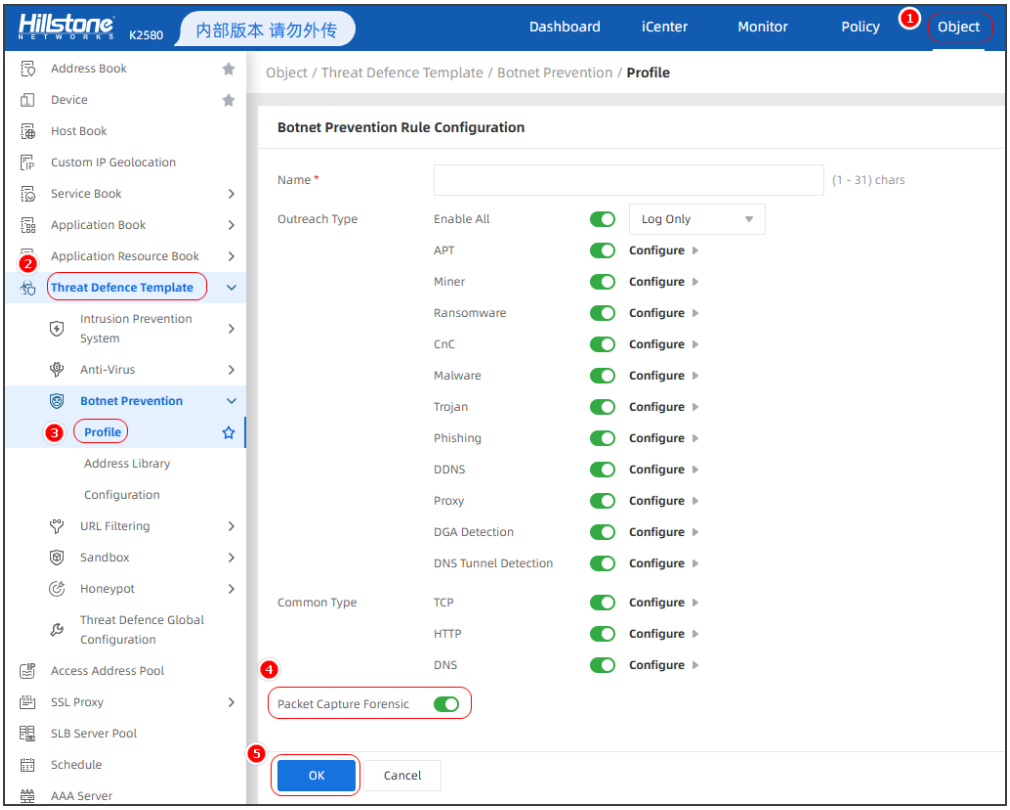
- Basic mode: The system can capture packets when a threat is detected. For the HTTP protocol, the system will capture request and response packets.
- Extend mode: The system can capture packet data both when a threat is detected and before the threat is detected. The upper limit of captured packet data can be configured through the "Packet Quantity for Single Connection Forensics". For the HTTP protocol in botnet detection functions and intrusion detection functions, the system will capture request and response packets. Compared to basic mode, extended mode can capture more packet data, providing you with more comprehensive evidence for in-depth analysis and accurate judgment.

c. If you select the extend mode, you need to configure the maximum number of single connection trace packets. Once the limit is reached, the earliest captured packet data will be discarded. The range is 5-50KB, with a default of 5KB.

d. Click **OK**.

2. **Configure the Intrusion Prevention SystemTemplate/Botnet Prevention Template, and enable the packet capture switch.**

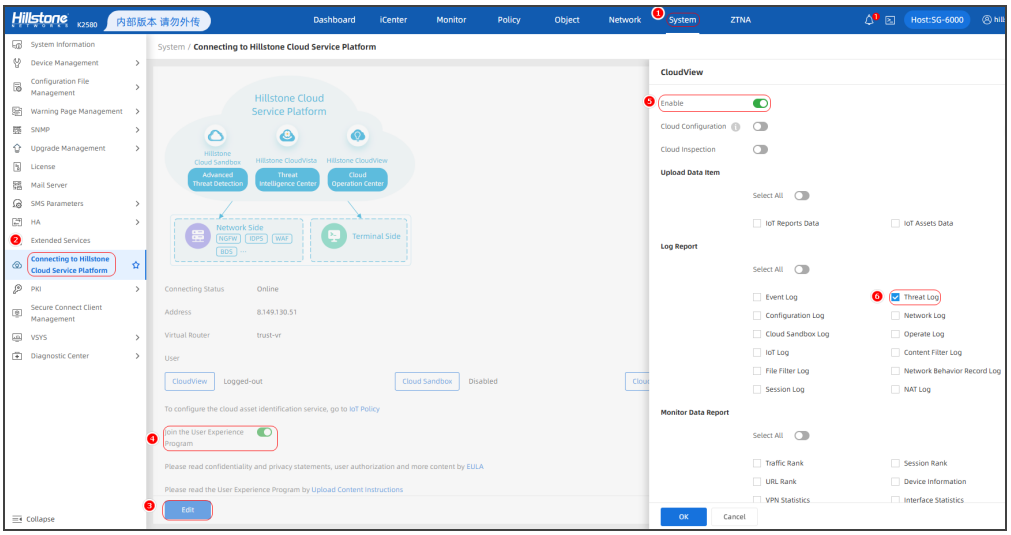
   Using the Botnet Defense Template as an example:



3. **(Optional) Connect to the cloud platform, enable the Join User Experience Program and CloudView.**

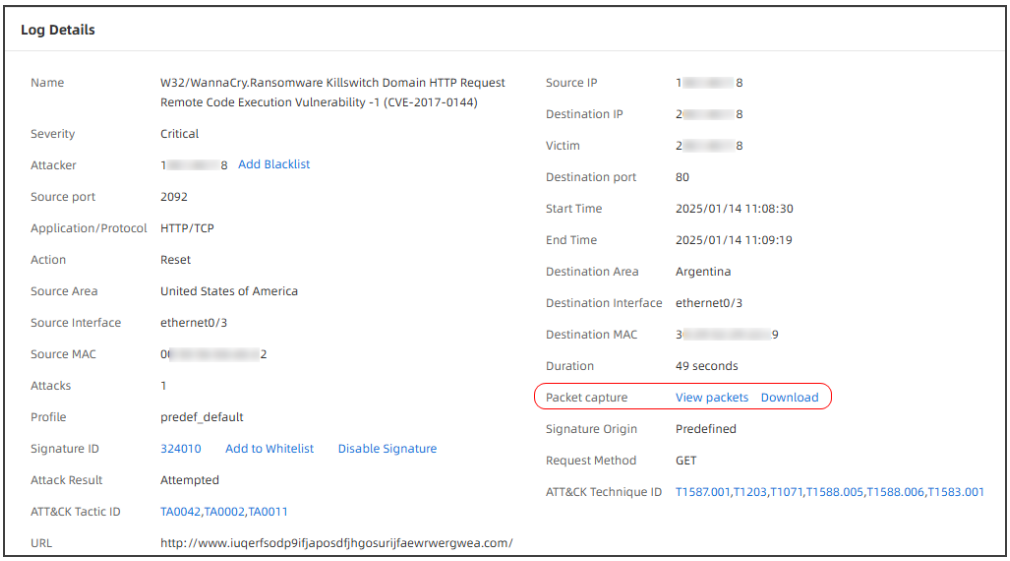
   When enabled, when the device detects a threat, it will capture packets and send the captured threat packet data and threat log information to Cloud · Jing. You can log in to Cloud · Jing to view and handle this information. The configuration process is shown in the following fig-

ure:



4. **View Threat Evidence Information.**

When threat traffic passes through the device, it detects threats and captures packets. You can view or download the captured threat packet data information on the WebUI.



Configuring a Botnet Prevention Rule

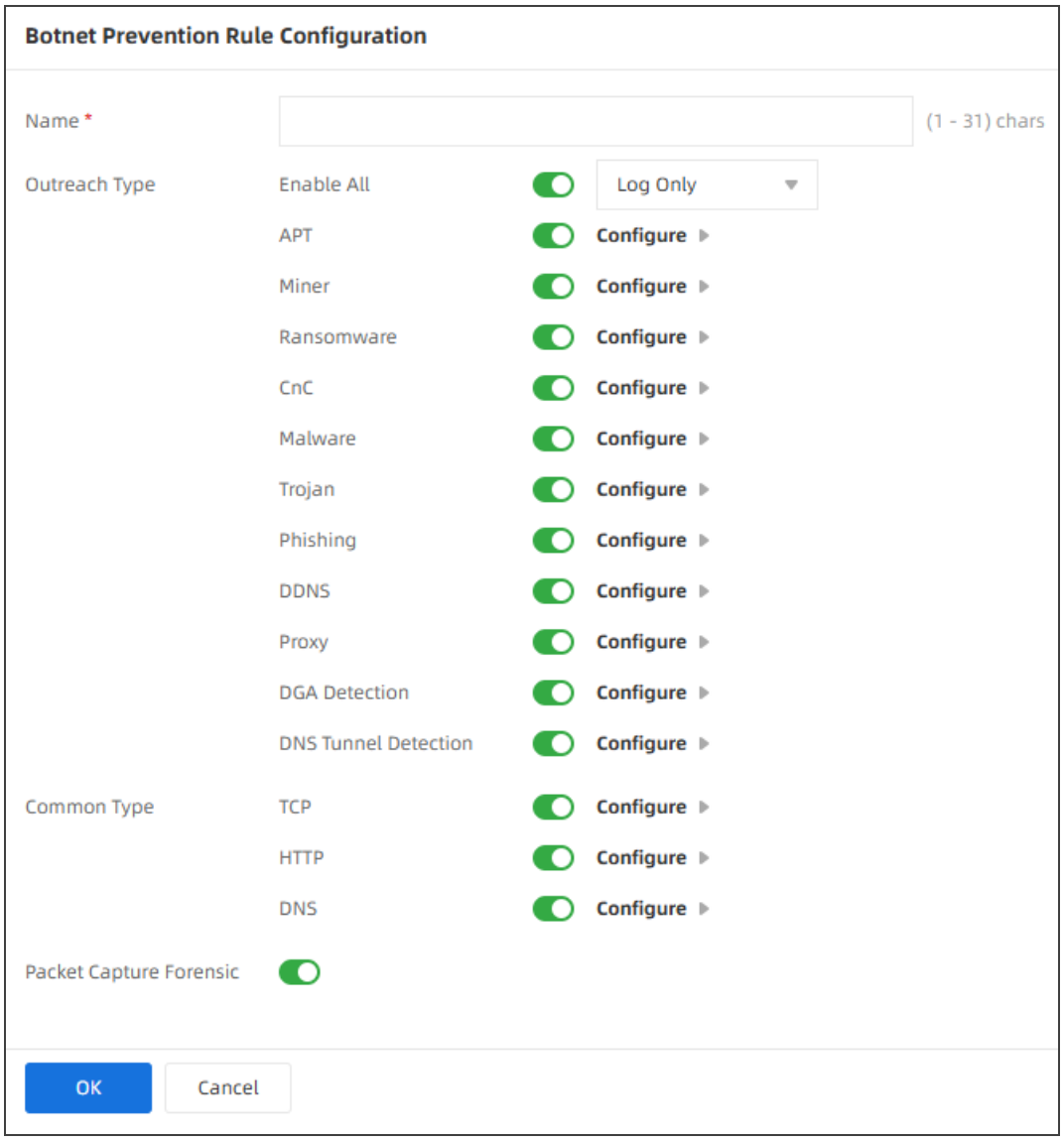
You can use default botnet prevention rules or create custom rules. The system provides 3 default botnet prevention rules: predef_critical, predef_default, and no-botnet-c2-prevention.

- **predef_critical** - The strict botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, malicious connection is reset and threat logs will be recorded.
- **predef_default** - The loose botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, traffic is allowed and the system only records threat logs.
- **no-botnet-c2-prevention** – This rule does not implement any botnet prevention check.

To configure a Botnet Prevention rule, take the following steps:

1. Click **Object** > **Threat Defence Template** > **Botnet Prevention**> **Profile**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
Outreach Type	Specifies the outreach type (i.e., IOC tag type) that needs to be protected and specifies the corresponding action. After enabled, when traffic hits the predefined/custom blocking list

Option	Description
	or cloud query cache blocklist, the IOC tag of the traffic data will be detected and processed based on the specified outreach type and the corresponding action; if not enabled, traffic will be detected and processed based on the protocol configuration of the common type. • Enable All: Turn on the switch to enable the protection for all outreach types. Select an action to be taken from the drop-down list. The action can be Log Only or Reset Connection. • Turn on the switch next to a specified outreach type to enable the protection for this type. • Click **Configure** to enable scan of different protocols (TCP, HTTP, DNS) for the selected outreach type and select the corresponding action. • Local Intelligent Algorithm: For the DGA Detection type and DNS Tunnel Detection type, the Local Intelligent Algorithm function is enabled by default. You can use this function to improve the accuracy rate of detection and reduce the false positive rate. Note: • The priority of the outreach type is higher than that of the common type. • The priority of each IOC tag type in the outreach type is

Option	Description
	ranked in ascending order based on the order displayed on the page.
Common Type	Specifies the protocol types (TCP, HTTP, DNS) that the system will scan and specifies the action the system will take after the bot-net is found. • Log Only - Only generates log. • Reset Connection - If botnets has been detected, system will reset connections to the files. • Sinkhole-Replace - When the protocol type is DNS, you can specify the processing action as "Sinkhole Address Replacement". After the threat is discovered, the system will replace the IP address in the DNS response packet with the Sinkhole IP address.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.

3. Click **OK**.

Notes: For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView

Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

For more information, refer to the **Threat Prevention**> **Botnet Prevention** > **Configuring Botnet Prevention** in *StoneOS WebUI User Guide*. FR 43747

Configuring an IPS Rule

System has three default IPS rules: **predef_default** , **predef_loose** and **predef_critical**.

- The **predef_default** rule is configured with IPS signatures of medium and high confidence levels, this rule can be used to detect threats and perform the default rule action.
- The **predef_loose** rule is configured with all the IPS signatures and its default action is log only.
- The **predef_critical** rule is configured with IPS signatures of the latest high-risk attacks and its default action is reset.

The system supports up to 64 user-defined IPS rules and each non-root VSYS supports up to 4 user-defined IPS rules.

To configure an IPS rule, take the following steps:

1. Select **Object > Intrusion Prevention System > Profile**.
2. Click **New** to create a new IPS rule. To edit an existing one, select the check box of this rule and then click **Edit**. To view it, click the name of this rule.



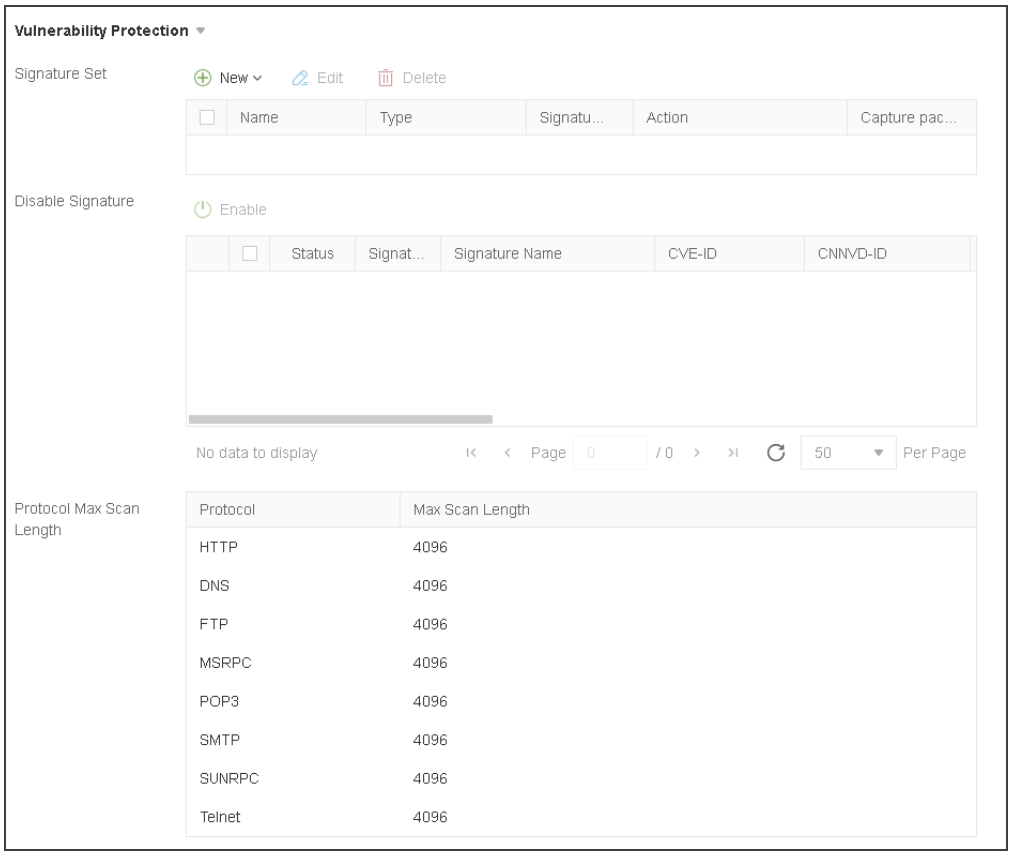
Note: A navigation bar is located on the right side of the **IPS Configuration** page. You can click any option to go to the corresponding section.

3. Configure the basic information of the profile:

Option	Description
Name	In the Name text box, enter the name of the newly-created IPS IDS profile. If you just configure the name and click **OK**, this profile will not take effect.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. **Notes:** For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet

Option	Description
	capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.
Description	Type the description information into the **Description** text box.

4. In the **Vulnerability Protection** section, click ▸ next to Vulnerability Protection to expand this section, including **Signature Set** and **Protocol Max Scan Length**.



5. In the signature configuration area, configure signature set rules and disable signatures.

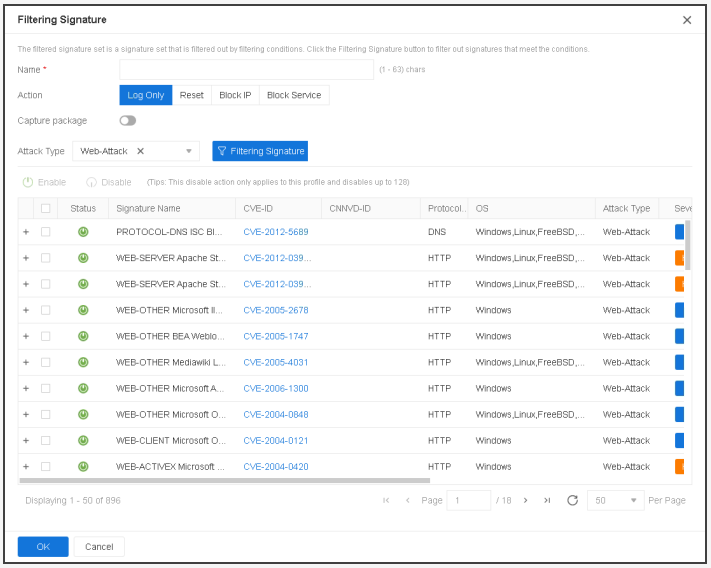
    i. In the **Signature Set** area, the existing signature sets and their settings will be displayed in the table. Select the desired signature sets. You can also manage the signature sets, including **New**, **Edit**, and **Delete**. When creating a new signature set rule, you can select **Filtering Signature** or **Selection Signature** as needed to filter and retrieve the signature database to select the desired signature sets.

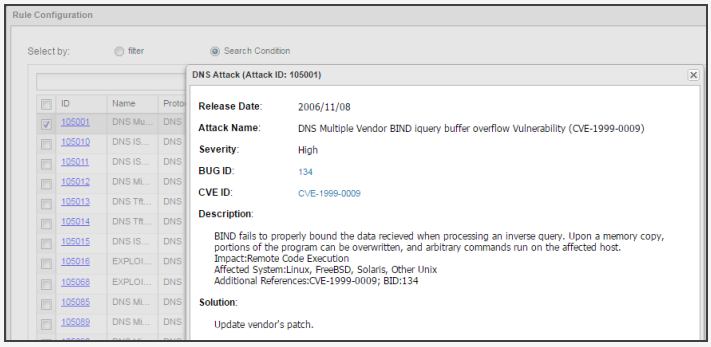
    - Filtering Signature: Filter signature sets by certain filter conditions. Click the **Filter Signature** button to search for the signatures you want. In this way, you can quickly select the signatures that have been classified by system.
    - Selection Signature: Select a particular signature set from the signature database. In this way, you can quickly select a particular signature.

    ii. **Click New and select Filtering Signature or Selection Signature to create a new signature set rule.**

Option	Description
Name	Specify the name of signature.
Action	Specify the action performed on the abnormal traffic that matches the signature set. • Log Only: Record a log. • Reset: Reset connections (TCP) or send destination unreachable packets (UDP) and also generate logs. • Block IP: Block the IP address of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a

Option	Description
	longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. • Default: Excute the action specifiled in the signature rule.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
Filtering Signature	If **Filtering Signature** is selected: System categorizes the signatures according to the following aspects (aka main categories): affected OS, attack type, protocol, severity, confidence, released year, affected application, and bulletin board. A signature can be in several subcategories of one main category. For example, the signature of ID 200211 is in the Linux subcategory, the FreeBSD subcategory, and Other Linux subcategory at the same time.

Option	Description
	Note: By default, **Filtering Signature** filters signatures based on all subcategories of severity. You can select other dimensions for filtering. You can view the detailed information of the signature by clicking the signature ID, and you can select one or more signatures. Click the Disable or Enable button to disable or re-enable the signature. **Note**: The enabled/disabled state here is only for the current profile, but the global state is not affected.  When selecting main category and subcategory, note the following matters: • You can select multiple subcategories of one main category. The logic relation between them is OR. • The logic relation between each main category is AND.

Option	Description
	• For example, you have selected Windows and Linux in OS and select HIGH in Severity. The chosen signatures are those whose severity is high and meanwhile whose affected operating system is either Windows or Linux.
Selection Signature	If **Selection Signature** is selected: Type the signature information into the **Keyword** text box, and system will perform fuzzy search in the following fields: signature ID, signature name, and description.  After the matched signature is found, select the signature, and it will be added to the Selected Signatures tab, indicating the signature is included in the signature set. After the matched signature is found, select the signature, and then click the Enable or Disable button to disable or re-enable the signature. The enabled/disabled state here is only for the current profile, but the global state is not affected.
Note: You create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the	

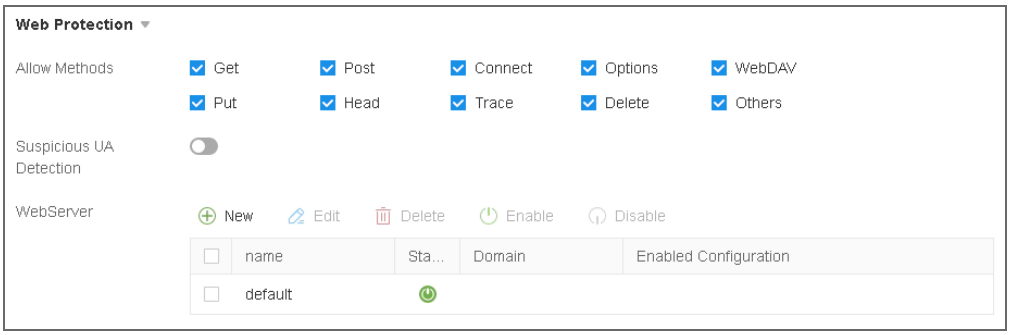
Option	Description
	attack matches this particular signature , system will adopt the following rules: • Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only > Deault. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s. • If one signature set is configured with Capture Packet, system will capture the packets. • The action of the signature set created by Selection Signature has higher priority than the action of the signature set created by Filter.

iii. Click **OK** to complete signature set configurations.

iv. In the Disable Signature section, the signatures that are Disabled in the template will be shown. Select one or more signatures, and then click the **Enable** button to re-enable the signature.

6. In the **Protocol Max Scan Length** section of **Vulnerability Protection**, click the max scan length of any protocol in the table to modify it. You can configure the max scan length of the HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet protocols. Default max scan length: 4096 bytes. Valid values: 0 to 65535 bytes, in which 0 indicates no limits.

7. In the Web Protection section, click ▸ next to Web Protection to expand this section.



Option	Description
Allow Methods	Specify the HTTP method that is allowed, including Get, Post, Connet, Options, WebDAV, Put, Head, Trace, Delete, and Others.
Suspicious UA Detection	Turn on the switch to enable the Suspicious UA Detection function. With this function enabled, the system detects User-Agent in HTTP Request messages. When User-Agent is detected as abnormal in HTTP messages, you can specify the action to handle User-Agent.
	Action: Specify the action to be performed when suspicious UA is detected. • Log Only: Record a log. • Block IP: Block the IP address of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration

Option	Description
	unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

To protect the Web server, configure Web Server in the HTTP tab.

Protecting the Web server means system can detect the following attacks: Sensitive File Scan, High Frequency Access Control, SQL injection, XSS injection, external link check, hotlinking check, iframe attack, ACL, and HTTP request flood and take actions when detecting them.

A pre-defined Web server protection rule named **default** is built in. The **default** rule supports only the following protection functions: Sensitive File Scan, SQL injection protection, XSS injection detection, iframe check, ACL, and HTTP request flood protection. By default, this protection rule is enabled and cannot be disabled or deleted. Each IPS rule can configure at most 32 Web server protection rules, excluding the **default** rule.

Configure the following settings to protect the Web server:

Option	Description
Name	Specify the name of the Web server protection rule.

Option	Description
Configure Domain	Specify domains protected by this rule. Click the link and the Configure Domain page will appear. Enter the domain names in the **Domain** text box. At most 5 domains can be configured. The traffic to these domains will be checked by the protection rule. The domain name of the Web server follows the longest match rule from the back to the front. The traffic that does not match any rules will match the default Web server. For example, you have configured two protection rules: **rule1 and rule2**. The domain name in rule1 is abc.com. The domain name in rule2 is email.abc.com. The traffic that visits news.abc.com will match rule1, the traffic that visits www.email.abc.com will match rule2, and the traffic that visits www.abc.com.cn will match the default protection rule.
High Frequency Access Control	Click the Enable button to enable the High Frequency Access Control feature. When this function is enabled, system will block the traffic of this IP address， whose access frequency exceeds the threshold. • Threshold: Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, system will block the flow of the IP. The value ranges from 1 to 65535 times per minute. • URL Path: Click the link and the URL Page Configuration

Option	Description
	page appears. Click **New** and enter the URL path in the **Path** text box. After the configuration, all paths that contain the name of the path are also counted. System accesses the frequency statistics for HTTP requests that access these paths. If the access frequency of the HTTP request exceeds the threshold, the source IP of the request is blocked, and the IP will not be able to access the Web server. For example: configure'/home/ab', system will perform a frequency check on the 'access/home/ab/login' and '/home/BC/login' HTTP requests. URL path does not support the path format which contains the host name or domain name, for example: you can not configure www.baidu.com/home/login.html, you should configure '/home / login.html', and 'www.baidu.com' should be configured in the corresponding Web server domain name settings. You can configure up to 32 URL paths. The length of each path is in the range of 1-255 characters. **Note**: Non-root VSYS does not support the High Frequency Access Control.
Sensitive File Scan	Select Enable to enable the Sensitive File Scan function for Web servers. In Sensitive File Scan attacks, an attacker traverses the sites in the Web server by using a file scanning tool. This way, the attacker can obtain sensitive information of the Web server, such as the dir-

Option	Description
	ectory structure, background files, and backup files. If an attacker attempts to scan sensitive files on the Web server, the Web server returns a large number of response packets with the status code "404". In this case, the system counts the number of 404 responses returned by the Web server per minute. ① If the number is greater than 10, the system parses the URLs in all HTTP requests and matches them with the built-in sensitive file dictionary. If the number of times that the parsed URL matches the sensitive file dictionary exceeds the specified threshold, the system performs the user-specified protection actions. The specified actions can be Log Only, Reset, Block IP, or Block Service. ②If the number is equal to or greater than 100, the system determines the behavior as a sensitive file scanning attack and performs the specified protection action. • Threshold: Specifies the threshold for the system to defend against sensitive file scanning attacks. If the number of times that URL paths match sensitive file dictionaries per minute exceeds the threshold, the system performs the user-specified protection actions. Default value: 10. Valid values: 10 to 100. Unit: times/min. • Action: Specifies the protection action for the system to defend against sensitive file scanning attacks: Log Only, Block IP, or Block Service.

Option	Description
	• Log Only: record a log. • Reset: Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. • Block IP: Block the IP address of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the attacker's IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
SQL Injection Protection	Click the Enable button to enable SQL injection check. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only - Record a log. Rest - Reset connections

Option	Description
	(TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Check point: Specifies the check point for the SQL injection check. It can be Cookie, Cookie2, Post, Referer or URI.
XSS Injection Protection	Click the Enable button box to enable XSS injection check for the HTTP protocol. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Check point: Specifies the check point for the XSS injection check. It can be Cookie, Cookie2, Post, Referer or URI.
External Link	Click the Enable button to enable external link check for the Web

Option	Description
Check	server. This function controls the resource reference from the external sites. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • External link exception: Click this link, and the External Link Exception Configuration page will appear. All the URLs configured on this page can be linked by the Web sever. At most 32 URLs can be specified for one Web server. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
Hotlinking Check	Click the Enable button to enable Hotlinking Check. System checks the headers of the HTTP packets and obtains the source site of the HTTP request. If the source site is in the Hotlinking Exception list, system will release it; otherwise, log or reset the connection. Thus controlling the Web site from other sites and to prevent chain of CSRF (Cross Site Request Forgery cross-site request spoofing) attacks occur. • Hotlinking Exception: Click the 'Hotlinking Exception ' to open the <Hotlinking Exception Configuration> page,

Option	Description
	where the configured URL can refer to the other Web site. Each Web server can be configured with up to 32 URLs. • Action: Specify the action for the HTTP request for the chaining behavior, either "Log only" or "Reset". “
Iframe check	Click the Enable button to enable iframe checking. System will identify if there are hidden iframe HTML pages by this function, then log it or reset its link. After iframe checking is enabled, system checks the iframe in the HTML page based on the specified iframe height and width, and when any height and width is less than or equal to the qualified value, system will identify as a hidden iframe attack, record, or reset connection that occurred. • Height: Specifies the height value for the iframe, range from 0 to 4096. • Width: Specifies the width value of the iframe, range from 0 to 4096. • Action: Specify the action for the HTTP request that hides iframe behavior, which is 'Only logged' or 'Reset'. Log Only - Record a log. Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
ACL	Click the Enable button to enable access control for the Web

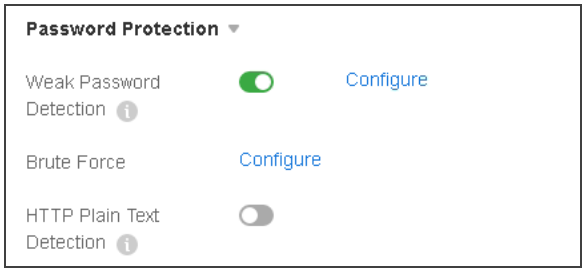
Option	Description
	server. The access control function checks the upload paths of the websites to prevent the malicious code uploading from attackers. • ACL: Click this link, the ACL Configuration page appears. Specify websites and the properties on this page. "Static" means the URI can be accessed statically only as the static resource (images and text), otherwise, the access will handle as the action specified (log only/reset); "Block" means the resource of the website is not allowed to access. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
HTTP Request Flood Protection	Select the Enable check box to enable the HTTP request flood protection. Both IPv4 and IPv6 address are supported. • Request threshold: Specifies the request threshold. For the protected domain name, when the number of HTTP connecting request per second reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack, and will enable the HTTP request flood protection. • When the number of HTTP connecting request per second by the object reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack by this object, and will enable the HTTP request flood pro-

Option	Description
	tection. • x-forwarded-for: Select None, system will not use the value in x-forwarded-for as the statistic object. Select First, system will use the first value of the x-forwarded-for field as the statistic object. Select Last, system will use the last value of the x-forwarded-for field as the statistic object. Select All, system will use all values in x-forwarded-for as the statistic object. • x-real-ip: Select whether to use the value in the x-real-ip field as the statistic field. When the HTTP request flood attack is discovered, you can make the system take the following actions: • Authentication: Specifies the authentication method. System judges the legality of the HTTP request on the source IP through the authentication. If a source IP fails on the authentication, the current request from the source IP will be blocked. The available authentication methods are: • No Authentication: The system does not authenticate the source IP of the HTTP request. • Auto (JS Cookie): The Web browser will finish the authentication process automatically. • Auto (Redirect): The Web browser will finish the

Option	Description
	authentication process automatically. • Manual (Access Configuration): The initiator of the HTTP request must confirm by clicking OK on the returned page to finish the authentication process. • Manual (CAPTCHA): The initiator of the HTTP request must be confirmed by entering the authentication code on the returned page to finish the authentication process. • Crawler-friendly: When the authentication method is selected as **Auto (JS Cookie)**, **Auto (Redirect)**, **Manual (Access Configuration)** or **Manual (CAPTCHA)**, you can enable the Crawler-friendly function. If this button is clicked, system will not authenticate to the crawler. • Request limit: Specifies the request limit for the HTTP request flood protection. After configuring the request limit, system will limit the request rate of each source IP. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enable button. • Proxy limit: Specifies the proxy limit for the HTTP request flood protection. After configuring the proxy limit, system

Option	Description
	will check whether each source belongs to the each source IP proxy server. If belongs to, according to configuration to limit the request rate. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enbale button. • Allow List: Specifies the allow list for the HTTP request flood protection. The source IP added to the allow list will not check the HTTP request flood protection. **Note**: Non-root VSYS does not support the HTTP Request Flood Protection.

8. In the Password Protection section, click ▸ next to **Password Protection** to expand this section, including Weak Password Detection, Brute Force, HTTP Plain Text Detection, and HTTP Password Protect Configuration.



   i. Turn on the **Weak Password Detection** switch to enable this function. Then, the system checks the strength of the plaintext password which is set under the FTP/Telnet/POP3/IMAP/SMTP/HTTP protocols in this profile. The password is detected as weak if it meets the conditions configured in the Weak Password Detection

section. In this case, the system issues an alarm log to prevent potential security risks caused by a weak password. Click Configure to configure the detection parameters of the weak password.

Note: When SSL proxy is configured in the policy, you can detect weak password for encrypted protocols such as HTTP.

Configure the detection parameters of the weak password.

Option	Description
Password Length	Specify the length criterion of the password. If a password is shorter than the length criterion, it will be detected as a weak password. The default length criterion is 6 characters. You can specify the password length criterion from 6 characters to 50 characters.
Password Character Type	Specify how many character types should be covered in the password. There are four types of characters: digits, uppercase letters, lowercase letters, and symbols. If the character types covered in a password are less than the specified number, the password will be detected as a weak password. By default, the system will detect the password containing less than 2 character types as a weak password and you can specify up to 4 character types for the detection of the password character type.
Other situations:	In the following situations, the password will be detected as a weak password: User Name Equals Password, Continuous Character Detection, FTP Anonymous Login Detection. • **User Name Equals Password**: The password that equals the user name will be detected as a weak pass-

Option	Description
	word after the detection function is enabled. • **Continuous Character Detection**: After this detection is enabled, a password that has less than 10 characters, among which at least 8 characters are the same or in consecutive sequence, will be detected as a weak password, such as 1aaaaaaaa, 1abcdefgh, a87654321. • **FTP Anonymous Login Detection**: When you log in anonymously through FTP, the system identifies your password as a weak password.
Specify Weak Password	You can specify the weak passwords. If a password matches the specified weak password, the system will consider the password as a weak one. You can specify up to 100 weak passwords.

ii. Click **Configure** next to **Brute Force** to go to the **Brute Force** panel. You can configure to block the brute force attacks under the FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP/HTTP protocol.
Note: The blocklist of brute-force attack IP does not take effect after the system is restarted.

To configure the protocol, click the Enable button behind the protocol. To enable/disable all protocols, click Enable All or Disable All.

Option	Description
FTP/MSRPC/ POP3/SMTP/ SUNRPC/Telnet/ IMAP/SSH/ LDAP/SMB/ VNC/RDP	**Action for Brute-force**: If the login attempts per 5 minutes fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Click the **Enable** button to enable brute-force. • Login Threshold per 5 Mins: Specifies a permitted authentication/login failure count per 5 minutes. • Action: Block the IP address of the attacker • Block Time: Specifies the block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. • Time Unit: If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address or the service of the attacker.

iii. Turn on the **HTTP Plain Text Detection** switch to enable this function. Then, the system checks the password field in the HTTP packet. If the password is not encrypted, an alarm log is generated.

Note: When the login is successful, the system performs plaintext detection only against the password in the HTTP packet but not the HTTPs packet because the HTTPS protocol is not transmitted in plaintext by default.

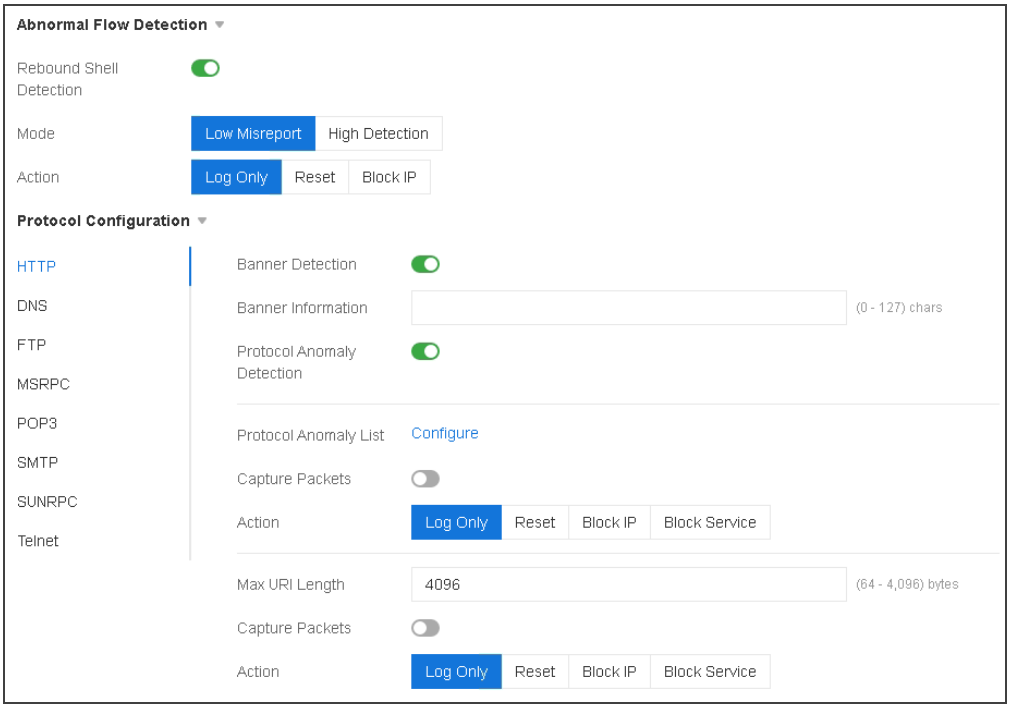
iv. In the **HTTP Password Protect Configuration** section, you can configure the username field , password field, success-login response code, success-login field, fail-login response code, and fail-login field in the HTTP login packet. The system can determine whether the login password is weak and whether there is brute-force attack by parsing the username, password, and login results contained in the HTTP login packet. The system is configured with a list of default username field, password field, and login result fields. However, the content of the HTTP protocol depends on the negotiation between the client and the server, therefore, to avoid false negatives, you can customize fields that tell information about the username, password, successful login, and failed login in the actual HTTP packet. This way, the system detects weak password and brute-force attacks and perform corresponding actions according to the configured rules.

Configure the following options in the HTTP Password Protect Configuration.

Option	Description
Username Field(s)	Specifies the username field in the HTTP login packet. The username field is case insensitive. Multiple fields can be separated with a semicolon. For example, username;user;usrname;j_username.
Password Field(s)	Specifies the password field in the HTTP login packet. The password field is case insensitive. Multiple fields can be separated with a semicolon. For example, password;passwd;pass;pwd;j_password.
Success-login Response	Specifies the success-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semi-

Option	Description
Code(s)	colon. For example, 200;302;201.
Success-login Field(s)	Specifies the success-login field in the HTTP login packet. The success-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, login-success;login-success.
Fail-login Response Code(s)	Specifies the fail-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semicolon. For example, 200;302;201;303.
Fail-login Field(s)	Specifies the fail-login field in the HTTP login packet. The fail-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, loginerror;login-error;loginerr.

9. In the **Abnormal Flow Detection** section, click ▸ next to **Abnormal Flow Detection** to expand this section, including **Rebound Shell Detection and Protocol Configuration**.



i. Turn on the switch next to Rebound Shell Detection and configure this function.

Option	Description
Action	Specifies the defend action against the rebound shell attacks. • Log Only - The system only generate logs when it detects the rebound shell attacks. • Reset - When a rebound shell attack is detected, the system resets connection (TCP) or sends destination unreachable packets (UDP), and then generates logs. • Block IP - Block the IP address of the rebound shell attacker and configure the block time. • Block Time: The default value is 60 seconds. The value range is from 60 to 3600 seconds. If longer block duration is needed, you can select bigger time unit, such as Hour or Day. You can also block the attacker IP permanently.
Mode	Specifies the detect and defend mode for the rebound shell attacks. • Low Misreport: When the system scans to detect keywords of the rebound shell attack, logs are reported only when the keywords are hit more than four time. This mode can be used in scenarios where high system performance is required.

Option	Description
	• High Detection: When the system scans to detect keywords of the rebound shell attack, logs are reported when the keywords are hit more than twice. This mode can be used in scenarios with high requirements for attack detection.

ii. Click ▸ next to **Protocol Configuration**. System supports the configurations of HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet.

In the HTTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the HTTP packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to

Option	Description

	enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
	ation, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max URI Length**: Specify a max URI length for the HTTP protocol. If the URI length exceeds the limitation, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the DNS tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Select **Enable** to analyze the DNS packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For

Option	Description

	more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration

Option	Description
: Click **Configure** to open	In the FTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the FTP packets. If abnormal contents exist, you can:

	Protocol Anomaly list: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules.
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also

	Forensic: Click the **Enable** button to enable

Option	Description

	generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

	Max Command Line Length: Specifies a max length (including carriage return) for the FTP command line. If the length exceeds the limits, you can:

Option	Description
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.
	Max Response Line Length: Specifies a max length for the FTP response line.If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the MSRPC tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Select **Enable** to analyze the MSRPC packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic func-

Option	Description

	tion, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select

Option	Description
	"permanent" to permanently block the service of the attacker. **Max Bind Length**: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Request Length**: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to

Option	Description

	enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
Max Bind Length: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet	
Forensic: Click the **Enable** button to enable	

Option	Description
capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset;	

Option	Description
Block IP; Block Service.	
Max Request Length: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button	

Option	Description
to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.	

Option	Description
• Action: Log Only; Reset; Block IP; Block Service.	

In the POP3 tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against POP3 server banners. • Banner information - Type the new information into the box that will replace the original server banner information.
Protocol Anomaly Detection	Click the **Enable** button to analyze the POP3 packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click **Disable** to disable the rules.

Option	Description

	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you

Option	Description
	want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Command Line Length**: Specifies a max length (including carriage return) for the POP3 command line. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Parameter Length**: Specifies a max length for the POP3 client command parameter. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Times**: Specifies a max failure time (within one single POP3 session) for the POP3 server. If the failure

Option	Description
	time exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the SMTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against SMTP server banners. • Banner information - Type the new information into the box that will replace the original server banner information.
Protocol Anomaly Detection	Click **Enable** to analyze the SMTP packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click Configure to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For

Option	Description

	more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
	ation, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Command Line Length**: Specifies a max length (including carriage return) for the SMTP command line. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Path Length**: Specifies a max length for the reverse-path and forward-path field in the SMTP client command. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Reply Line Length**: Specifies a max length reply length for the SMTP server. If the length exceeds the limits, you can:

Option	Description
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Text Line Length**: Specifies a max length for the E-mail text of the SMTP client. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Type Length**: Specifies a max length for the content-type of the SMTP protocol. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Filename Length**: Specifies a max length for

Option	Description
	the filename of E-mail attachment. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Time**: Specifies a max failure time (within one single SMTP session) for the SMTP server. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the SUNRPC tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Click **Enable** to analyze the SUNRPC packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile.

Option	Description

	Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.

Option	Description
	• Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

In the Telnet tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Click **Enable** to analyze the Telnet packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: • Log Only - Record a log;

Option	Description

	• Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Username/Password Max Length: Specifies a max length for the username and password used in Telnet. If the length

Option	Description
	exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

10. Click **Save** to complete the protocol configurations.

11. Click **OK** to complete the IPS rule configurations.

Notes: For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

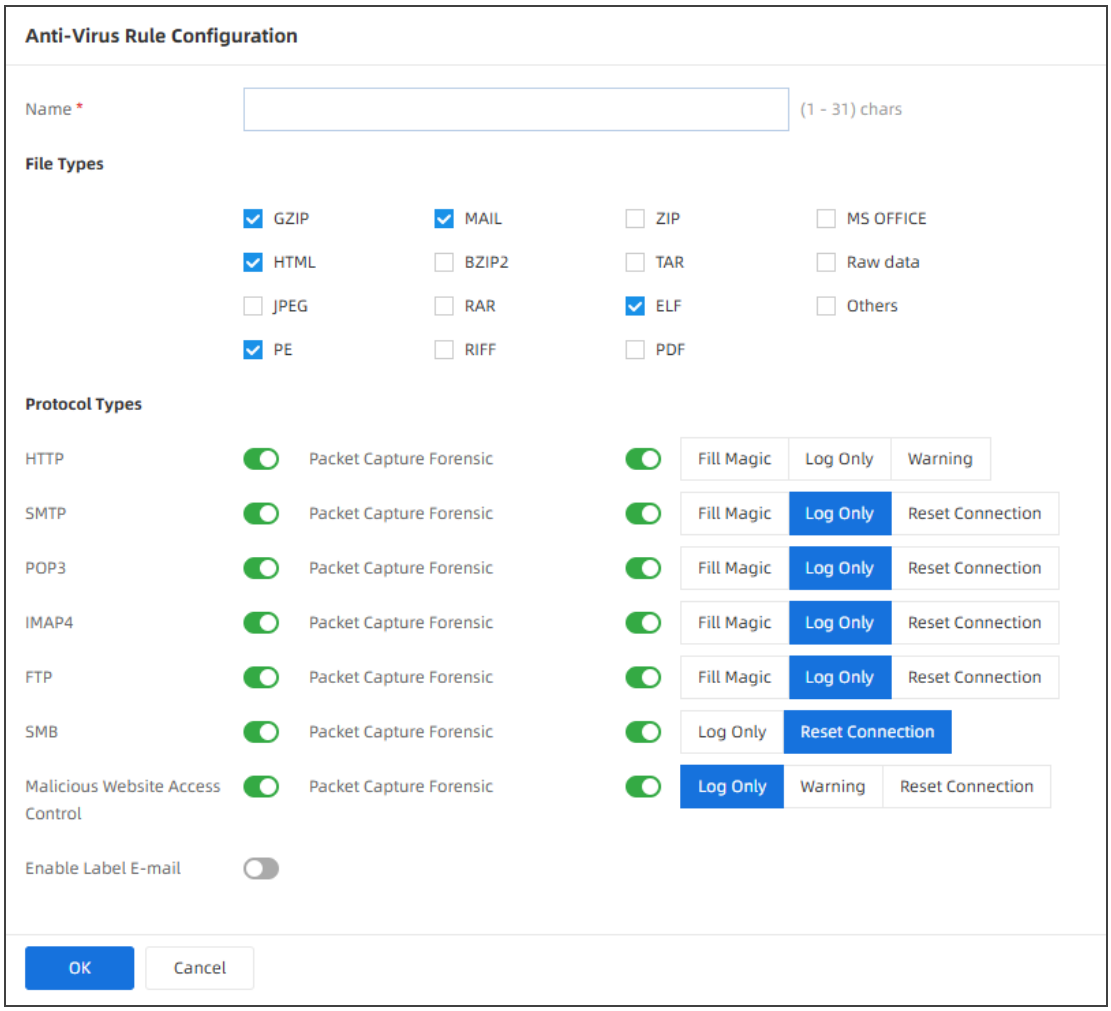
For more information, refer to the **Threat Prevention** > **IPS** > **Configuring IPS** section in *StoneOS_WebUI_User_Guide*. FR 43747

Configuring an Anti-Virus Rule

To configure an Anti-Virus rule, take the following steps:

1. Select **Object > Threat Defence Template > Anti-Virus > Profile**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
File Types	Specifies the file types you want to scan. It can be GZIP, JPEG, MAIL, RAR, HTML .etc. **Other** means scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc.

Option	Description
Protocol Types	Specifies the protocol types (HTTP, SMTP, POP3, IMAP4, FTP,SMB) you want to scan and specifies the action the system will take after the virus is found. • Fill Magic - Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section. • Log Only - Only generates log. • Warning - Pops up a warning page to prompt that a virus has been detected. This option is only effective to the messages transferred over HTTP. • Reset Connection - If virus has been detected, system will reset connections to the files.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. **Notes:** For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data,

Option	Description
	and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.
Malicious Website Access Control	Click the button behind Malicious Website Access Control to enable the function.
Action	Specifies the action the system will take after the malicious website is found. • Log Only - Only generates log. • Reset Connection - If a malicious website has been detected, system will reset connections to the files. • Warning - Pops up a warning page to prompt that a malicious website has been detected. This option is only effective to the messages transferred over HTTP.
Enable Label E-mail	If an email transferred over SMTP is scanned, you can enable label email to scan the email and its attachment(s). The scanning results will be included in the mail body, and sent with the email. If no virus has been detected, the message of "No virus found" will be labeled; otherwise information related to the virus will be displayed in the email, including the filename, result and action. Type the end message content into the box. The range is 1 to 128.

3. Click **OK**.

Notes: By default, according to virus filtering protection level, system comes with three default virus filtering rules: predef_low, predef_middle, predef_high. The default rule is not allowed to edit or delete.

For more information, refer to the **Threat Prevention** > **Anti-virus** > **Configuring Anti-virus** section in *StoneOS_WebUI_User_Guide*. FR 43747

CLI

Configuring Packet Capture Forensic Mode

The system supports the packet capture function. When a threat is detected, it captures relevant packets, making it easier for you to analyze and evaluate the evidence information later. Packet capture has two modes: basic and extended. The system uses the basic mode by default for packet capture.

- Basic mode: The system can capture packets when a threat is detected. For the HTTP protocol, the system will capture request and response packets.
- Extended mode: The system can capture packet data before and after a threat is detected. The maximum amount of captured packet data can be configured through the "Packet quantity for single connection forensics". For the HTTP protocol in botnet detection and intrusion detection functions, the system will capture request and response packets.

Configure the packet capture evidence mode. In global configuration mode, use the following commands:

attack-forensics-mode {**basic** | **extended limit** *value*}

- **basic** - Specifies using the basic mode for packet capture.
- **extended limit** *value* - Use extended mode for packet capture. When using extended mode, you need to configure the maximum number of packets captured per connection. Once the limit is

reached, the earliest captured packets will be discarded. The range is 5-50KB, with a default of 5KB.

> **Notes:** Packet capture mode only takes effect for Intrusion Prevention System and Botnet Prevention functions.

For more information, refer to the **Threat Prevention** section in *StoneOS CLI User Guide*. FR 43747

Creating an AV Profile

The AV profile specifies the file types, protocol types and the actions for viruses. To create an AV Profile, in the global configuration mode, use the following command:

av-profile*av-profile-name*

- *av-profile-name* - Specifies the AV profile name and enters the AV profile configuration mode. If the specified name exists, then the system will directly enter the AV profile configuration mode. To delete the specified AV profile, in the global configuration mode, use the command**no av-profile***av-profile-name*.

To control the scan accurately, in the AV profile configuration mode, specify the protocol types, actions and file types. Among the above options, the protocol types must be specified, while the file types can be configured as needed. If only the protocol types are configured, but the file types are not configured, the system will only scan the text files transferred over specified protocol; if the scan object is the specified file type transferred over the specified protocol type (for example, a HTML document transferred over the HTTP protocol), you need to specify the HTTP protocol type and HTML file type in the AV profile.

Enabling Malicious Website Detection

System provides the malicious website detection function to protect against attacks from malicious websites if you click maliciously URLs accidentally. With this function enabled, System will detect

Trojans, phishing and other malicious behaviors when you are trying to visit URLs, and process malicious URLs according to the actions specified by system.

The Malicious Website Detection is enabled by default. To enable the function, in the global configuration mode, use the following command:

anti-malicious-sites

To disable the function, in the global configuration mode, use the following command:

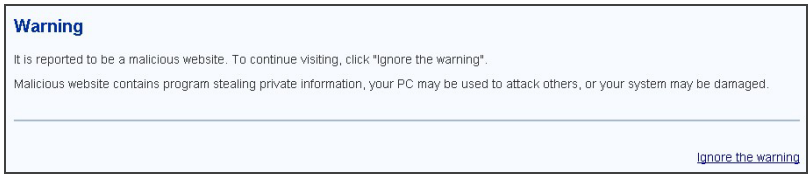
no anti-malicious-sites

Specifying Malicious Website Detection Action

To specify the action for Malicious Website Detection, in the AV profile configuration mode, use the following command:

anti-malicious-sites [**action**{ **log-only** | **reset-conn** | **warning**} | **pcap**]

- **action** {**log-only** | **reset-conn** | **warning**} – Specifies the action for the Malicious Website Detection
  - **log-only** – Only generates log.
  - **reset-conn** – If virus has been detected, system will reset connections to the files.
  - **warning** – Pops up a warning page to prompt that a virus has been detected. This option is only effective to the messages transferred over HTTP.



    To view the reason for the block, click Why blocks this website, and you will be redirected to the Google Safe Browsing page. To ignore the page and continue to visit the website, click Ignore. In the following hour, you will not be prompted anymore if you visit the website again.

- **pcap** – Enable the Capture Packet function.

To cancel the the action for Malicious Website Detection, in the AV profile configuration mode, use the following command:

no anti-malicious-sites [**action**{ **log-only** | **reset-conn** | **warning**} | **pcap**]

Notes: For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

Specifying a Protocol Type

To specify a protocol type, in the AV profile configuration mode, use the following command:

protocol-type {{**ftp** | **imap4** | **pop3** | **smtp**} [**pcap** | **action** {**fill-magic** | **log-only** | **reset-conn**}] | **http** [**pcap** |**action** {**fill-magic** | **log-only** | **reset-conn** | **warning**}]|**smb** [**pcap** | **action** {**log-only** | **reset-conn**}] }

- **ftp** – Scans the files transferred over FTP.
- **http** – Scans the files transferred over HTTP.
- **imap4** – Scans the files transferred over IMAP4.
- **pop3** – Scans the Emails transferred over POP3.
- **smtp** – Scans the Emails transferred over SMTP.

- **pcap** – Capture the packet for protocol scanning.

  Notes: For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

- **smb** – Scans the files transferred over SMB.
- **action** {**fill-magic** | **log-only** | **reset-conn** | **warning**} – Specifies the action for the viruses.
  - **fill-magic** – Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section.
  - **log-only** – Generates logs. This is the default action for FTP, IMAP4, POP3 ,SMTP and SMB.
  - **reset-conn** – Resets the connection if any virus has been detected.
  - **warning** – Pops up a warning page to prompt that a virus or malicious website download has been detected. There are two kinds of pages: the virus warning page , and malicious website warning page (the malicious website detection is enabled), as shown below. This option is only effective to the messages transferred over HTTP, and is also the default action if any virus or malicious website download has been detected.



To ignore the page and continue to visit the website, click Ignore. In the following one hour, you will not be prompted anymore if you visit the website again.



To ignore the page and continue to visit the website, click Ignore. In the following hour, you will not be prompted anymore if you visit the website again.

Repeat the above command to specify more protocol types.

To cancel the specified protocol type, in the AV profile configuration mode, use the following command:

no protocol-type {ftp | imap4 | pop3 | smtp | http| smb}

SMTP, POP3 and IMAP4 are all mail transfer protocols that are used to send Email files. To scan Emails, you must configure to scan SMTP, POP3 or IMAP4 protocol, and also configure the file types that will be scanned; besides, as the body of the message and attachments are embedded in the mail file, you also need to configure the file types for the attachment.

For more information, refer to the **Threat Prevention** > **Anti-virus** > **Configuring Anti-virus** section in *StoneOS CLI User Guide*. FR 43747

Enable/Disable the Packet Capture Function for Botnet Prevention

After enabling the packet capture function, the system captures relevant packets when it detects a threat. You can view or download the captured packets in the corresponding threat logs. By default, the packet capture function is enabled.

Enable/disable the packet capture function, in Botnet Prevention Profile configuration mode, use the following commands:

- Enable: **attack-forensic enable**
- Disable: **attack-forensic disable**

> **Notes:** For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, you will not be able to view the packet capture data on the firewall device, and the system will send the packet capture data and threat log information to CloudView Security. Operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

For more information, refer to the **Threat Prevention** > **Botnet Prevention** section in *StoneOS CLI User Guide*. FR 43747

IPS Commands

pcap

When the traffic matches the signatures configured in a filter rule or a search rule, the system will capture the packets of the traffic.

Command:

pcap enable

pcap disable

Description:

enable - Capture the abnormal packets. You can view them in the threat log.

disable -Do not capture the abnormal packets.

Default values:

disable

Mode:

Filter rule configuration mode;

search rule configuration mode.

Guidance:

For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

Example:

hostname(config)# **ips profile test**

hostname(config-ips-profile)# **pcap enable**

protocol-check

Enable the protocol legality check for the signature set and configure the strictness level for the protocol legality check.

Command:

protocol-check disable

protocol-check enable action {{ **block-service**{**permanent** | **second***timeout* | **hour***timeout* | **day** *timeout*} | **block-ip** {**permanent** | **second***timeout* | **hour***timeout* | **day***timeout*} | **log-only** | **reset**} **pcap** {**disable** | **enable**}

Description:

enable -Enable the protocol legality check.

block-ip {**permanent**|**second** *timeout* |**hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the IP address of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker IP is blocked permanently.
- **second** *timeout* | **hour** *timeout* | **day** *timeout* - Specifies the duration (by second/hour/day) for blocking the IP address of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

block-service {**permanent** | **second** *timeout* | **hour** *timeout* | **day** *timeout*} - Specifies the protection action is to block the service of the attacker, and specifies the block duration.

- **permanent** - Specifies that the attacker service is blocked permanently.
- **second***timeout* | **hour***timeout* | **day***timeout* - Specifies the duration (by second/hour/day) for blocking the service of the attacker. The value range is 60 to 3,600 seconds/ 1 to 24 hours/ 1 to 15 days.

log-only- Record a log.

reset -Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs.

pcap {disable | enable} enable- Use enable to capture the abnormal packets. You can view them in the threat log. Use **disable**to not capture the abnormal packets.

Default values:

The system disables the protocol legality check.

Mode:

protocol configuration mode.

Guidance:

For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

Example:

hostname(config)# **ips sigset http1 template http**

hostname(config-http-sigset)# **protocol-check strict**

hostname(config-http-sigset)# **protocol-check enable action log-only**

For more information, refer to the **Threat Prevention** > **IPS**> **Configuring IPS** section in *StoneOS CLI User Guide*. FR 43747

Add a New Threat Classification Database and Support Manual Updates

CLI

Threat Classification Database

Introducing the Threat Classification Database

The threat classification database is used to store threat classification data of different levels to ensure that the system can accurately identify and classify various threats.

Configuring Threat Classification Database Updates

By default, the system automatically updates the threat classification database daily. You need to change the threat classification database update configuration as required.

Currently, only updating the threat classification database via CLI is supported.

Threat classification database update configuration includes:

- Configure the Threat Classification Database Update Mode
- Configure the update transfer protocol
- Configure the update server
- Specify HTTP Proxy Server
- Specify Update Time

- Update Now
- Import the threat classification Database file
- View Threat Classification Database Information
- View the Threat Classification Database Update Configuration Information

Configuring The Threat Classification Database Update Mode

The system supports both manual and automatic update methods. To configure the threat classification database update method, in global configuration mode, use the following commands:

threat-type update mode {**auto** | **manual**}

- **auto** – Specifies automatic updates for the threat classification database. This is the system's default update method.
- **manual** – Specify manual updates for the threat classification database.

Use the command in global configuration mode in the form of no to restore the default update mode:

no threat-type update mode

Configuring the Update Transmission Protocol

The system supports updating the feature database via HTTP and HTTPS, with HTTPS as the default. To configure the transmission protocol for feature database updates to HTTP, use the following command in global configuration mode:

threat-type update protocol HTTP

Use the command in global configuration mode in the form of no to restore the default HTTPS mode:

no threat-type update protocol HTTP

Configuring the Update Server

The system provides default threat classification database update servers, namely update1.hillstonenet.com and update2.hillstonenet.com. You can also configure other update servers to download the latest threat geographic information as needed. Up to 3 can be configured. To configure update servers, use the following commands in global configuration mode:

threat-type update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter** *vrouter-name*] [**src-interface** *src-interface-name*]

- **server1 | server2 | server3** – Specify the servers to be configured. The servers support dual-stack protocols and can be configured with IPv4 and IPv6 addresses. The default value for **server1** is update1.hillstonenet.com, and the default value for **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specify the name of the update server, which can be in IP address form (*ip-address*) or domain name form (*domain-name*, for example, update1.hillstonenet.com).
- **vrouter** *vrouter-name* - Specifies the VRouter of the update server. If not specified, it defaults to **trust-vr**.
- **src-interface** *src-interface-name* – Specify the source interface name, which must be an interface under the virtual router. After specifying, the threat classification database update will access the update server through this source interface. If not specified, the management port will be used as the source interface by default.

In global configuration mode, use the command in the form of no to cancel the specified update server:

no threat-type update {**server1** | **server2** | **server3**}

Specifying the HTTP Proxy Server

When the device needs to access the internet through an HTTP proxy server, to ensure that the feature database can be updated properly, you need to specify the IP address and port number of the proxy server on the device.

Specify a proxy server for threat classification database upgrades. In global configuration mode, use the following commands:

threat-type update proxy-server {**main** | **backup**} *ip-address port-number*

- **proxy-server** {**main** | **backup**} – Use the **main** parameter to specify the primary proxy server, and use **backup** to specify the backup proxy server.
- *ip-address port-number* – Specify the IP address and port number of the proxy server.

Cancel the specified proxy server and use the **no threat-type update proxy-server** {**main** | **backup**} command.

Specifying Update Times

By default, the system uses automatic mode to update the threat classification database daily, and to avoid excessive server traffic, the update time is random each day. You need to specify the frequency and time for updating the threat classification database according to your needs. In global configuration mode, use the following command:

threat-type update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Specifies the frequency as daily updates.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Specifies the frequency as weekly updates. **mon | tue | wed | thu | fri | sat | sun** is used to specify the day of the week for updates.
- **monthly** *date* - Specifies the update frequency as monthly. *Date* is used to specify the date of the monthly update, with values ranging from 1 to 31. If a month does not contain the specified

date (for example, February does not have the 30th), then the update will not occur automatically for that month.

- *HH:MM* – Specifies the update time, for example, 09:00.

Immediately Updating

Regardless of whether the update mode is manual or automatic, you can use the following command to update the threat classification database at any time. To immediately update the threat classification database in any mode, use the following command:

exec threat-type update

> **Notes:** Update the differences between the current threat classification database and the latest released threat classification database on the update server.

Importing The Threat Classification Database File

In some cases, you may not be able to connect to the update server to update the threat classification database. To address this issue, the system provides a function to import the threat classification database file via FTP/FTPS/SFTP/TFTP server to update the device's threat classification database. To import the threat classification database file, in execution mode, use the following command:

import threat-type signature from {**ftp server** [*ip-address* **user** *user-name* **password** *password*] | **ftps server** [*ip-address* **user** *user-name* **password** *password*] | **sftp server** [*ip-address* **user** *user-name* **password** *password*] | **tftp server***ip-address*} [**vrouter***vr-name*] *file-name*

- *ip-address* – Specify the IP address of the FTP, FTPS, SFTP, or TFTP server.
- **user** *user-name* **password** *password* – Specifies the username and password for the FTP, FTPS, or SFTP server.
- **vrouter** *vr-name* – Specify the VRouter to which the FTP, FTPS, SFTP, or TFTP server

belongs.

- *file-name* – Specifies the name of the threat classification database file to be imported.

Viewing Threat Classification Database Information

You can use the corresponding show command at any time to view the threat classification database information of the device, including the threat classification database version, release date, etc. To view the threat classification database information, use the following command in any mode:

show threat-type info

The following is a sample response:

```
hostname# show threat-type info
Signature vendor: Hillstone Networks (This indicates the company to which the threat classification database belongs.)
Current version: 1.0.241224 (This shows the current version of the threat classification database.)
Release date: 2024/12/24 13:44:52 (This shows the release date of the threat classification database.)
```

Viewing The Threat Classification Database Update Configuration Information

You can use the corresponding show command at any time to view the threat classification database update information on the device, including update server information, update mode, update frequency and time, and threat classification database update status. To view the threat classification database update configuration information, use the following command in any mode:

show threat-type update

Take the following steps:

```
hostname# show threat-type update
THREAT_TYPE knowledge base signature update options:
protocol: HTTPS (This indicates that the transmission protocol for updating the threat classification database is HTTPS.)
```

server1: update1.hillstonenet.com, 443, trust-vr (Displays the threat classification database update server server1.)

server2: update2.hillstonenet.com, 443, trust-vr (Displays the threat classification database update server server2.)

server3: (Display the threat classification database update server server3.)

proxy server status: disabled (This indicates that the proxy server is not enabled.)

Main proxy server: (Displays the primary proxy server.)

backup proxy server: (Displays the backup proxy server.)

mode: auto (This indicates that the threat classification database update mode is set to automatic.)

schedule: daily 18:18 (This indicates the update frequency of the threat classification database.)

Current status: normal (This shows the update status of the threat classification database.)

last update result: success (The result of the last update of the threat classification database.)

last update time: Tue Dec 24 18:18:27 2024 (The last time the threat classification database was updated.)

For more information, refer to the **Threat Prevention** section in *StoneOS CLI User Guide*. FR 43699

Optimizing the Threat Log Display Information

WebUI

Threat Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

Threat logs can be generated under the conditions that:

- Threat logging in the Logging feature is enabled. Refer to Managing Logs.
- You have enabled one or more of the following features: "Anti Virus" on Page 1, " Intrusion Prevention System" on Page 1, "Attack-Defense" on Page 1 or "Perimeter Traffic Filtering" on Page 1 .

To view threat logs, select **Monitor > Log > Threat Log**.

In this page, you can perform the following actions:

- Filter: Click 

to configure more filter conditions. After configure the filter conditions, the system will automatically display the matched logs.

  Alternatively, move the mouse over a specific log entry. When the mouse hovers over the corresponding display item and the ⋮ icon appears, click the **Add Filter** button. The system will add the selected display item's field as a filter condition at the top of the list and perform quick filtering based on this condition.

  For devices that are of the IPv6 version, the filter conditions for source and destination addresses support both IPv4 and IPv6. When selecting **Attack Result**, view the threat log of the specified attack result, including:

  - Attempted: Indicates that an attack occurs, but the attack is unsuccessful or the result of the attack is uncertain, and it is impossible to determine whether the attacked device has

compromised.

- Successful: The attacker has successfully exploited the vulnerability or delivered a malicious sample, and it is unclear whether the malicious sample is executed.
- Confirmed Compromised: It is confirmed that the attacked device has been compromised, and there have been behaviors such as outreach and lateral spread.
- Unknown: Upgrading the attack results from the old database or the attack results preset by the unsupported detection engine.

- Save Filter: Click the drop-dow menu after the **Filter** and select "Save Filter" to save the current filter conditions, so that the next time you can directly select the save filter conditions, and view the corresponding log. If you need to delete a saved filter condition, click the drop-down arrow after the **Filter**, and in the drop-down list, click the "X" button to the right of the name of the saved filter condition you want to delete.
- Delete Filter: Hover the mouse over a filter condition and click the **X** button on the left to delete an individual filter condition; or click **Remove All** on the far right to delete all filter conditions.
- Merge Log: Select the merge type from the drop-down list, which includes Do Not Merge, Threat Name, Source IP, Destination IP.
- Configure: Click to jump to the configuration page.
- Clear: Click to clear the selected logs. (Note: This option is not supported for devices that support sending log information to the local database)
- Add to My Log: Click to add the current filtered results to MyLog list.

- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.
- Add filter: Hover over the log entry display item information. Depending on the type of display item, icons will appear. Hover over the icon, and a Add Filter button will appear. Click **Add Filter**, and the system will add the corresponding filter conditions above the list and apply quick filtering based on these conditions.
- Click a threat log name in the table and then you can view the detailed information in the Log Details tab. In the Log Details tab, you can do the following:
    - View the severity, application/protocol, source/destination port, threat start time, end time, and other threat-related information (such as plain-text SQL command, plain-text paths to URI, etc.). The system will highlight in red the critical characteristic information of detected threats.
    - Click "ViewPcap" to see the message package of the threat, or click "Download" to download the packet to local for viewing. IPv6 and IPv4 protocol type messages are both supported for users to view.
    - For threat logs related to weak password, "Password", "Packet", and "Threat Data" can only be viewed or downloaded after entering the system login password.Click **View** behind the **Password** field. The administrator can view weak password details in the **Password View** panel. Click **Copy** to copy the weak password.
    - Click "Signature ID" "Add Allowlist" "Disable Rule" to quickly link to the relevant page.
    - When the detection engine is anti-virus, click the name of the log entry whose details you want to view in the log list. You can click **Add to Allowlist** next to MD5 or URL to add this MD5 or URL to the allowlist list in **Object** > **Anti-Virus** > **Allowlist**.

- For threat logs whose detection engine is IPS, if you enable the **Capture Threat Data** function, you can view ASCII and hex information of the threat in the Log Details tab. With the help of data in the **Threat Data** section, you can analyze the whole development process of the threat. If the **Capture Threat Data** function is not enabled, the **Threat Data** option will not be displayed on the **Threat Log** page. This function can be enabled only by using the CLI. For more information, visit **Threat_Prevention** > **IPS_config** in *StoneOS CLI User Guide*.

- For threat logs whose detection engine is IPS or antivirus, you can click **Add Blocklist** behind the attacker to block the IP address of the attack source by adding it into the blocklist. For more information about how to configure IP blocklist, refer to Static IP Blocklist.

- MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base of attack behaviors. It categories known attacks as tactics and techniques, establishing a practical and clear framework. The system maps detected suspicious behaviors to the MITRE ATT&CK® model and displays the MITRE ATT&CK® tactic IDs and MITRE ATT&CK® technique IDs of the threat in threat logs, helping you identify suspicious behaviors in a better way. To ensure that the latest MITRE ATT&CK® knowledge base is used during detection, it is recommended to upgrade the MITRE ATT&CK® knowledge database. For more information about upgrading the MITRE ATT&CK®Knowledge Base, refer to Updating Signature Database.

    - Click **MITRE ATT&CK® Tactic ID** to go to the **MITRE ATT&CK® Tactic Details** panel, where you can view the name, created time, last modified time, data source, official link, and description of this tactic. MITRE ATT&CK® Tactic represents the tactical object of adversary and the reason for performing the attack.

- Click **MITRE ATT&CK® Technical ID** to go to the **MITRE ATT&CK® Technical Details** panel, where you can view this technique's name, data source, permission/system/network requirements, tactic, parent technique, sub technique, mitigation methods, official link, platform, ect. MITRE ATT&CK® Technique represents how an adversary achieves a tactical goal by performing an action.

- The system supports to upload certain elements (such as IP address) in logs generated from each module to the cloud platform. The cloud platform will query whether the element carries threat intelligence by using the third-party server. You can view details about threat intelligence of the element via CloudVista.
  - In the threat list, click the threat intelligence icon (, , or) behind the address in the "Source"/"Destination" column in the list, or hover your cursor over a object, and there is a button ( ) to its right. Click this button to open the threat intelligence center (CloudVista) to view the threat intelligence.
  - Threat intelligence status: indicates a normal intelligence that contains the allowlist; indicates a suspicious intelligence; indicates a malicious intelligence.

  Notes:
  - The threat intelligence function is controlled by license. Before you use the function, you need to install the corresponding license.
  - Before you use the function, configure Connecting to Hillstone Cloud Service Platform.

- SSD Log: Click to go to the Hard Disk Logs page, where you can view logs stored on the hard disk by time. Click the name of the log file to view its detailed information. For more information about configuring the function of storing log files on the hard disk, refer to Option Descriptions of Various Log Types. Note: Only SG-6000-X9180 supports this function.

For more information, refer to the **Monitor**> **Logging** section in *StoneOS WebUI User Guide*. FR 43691

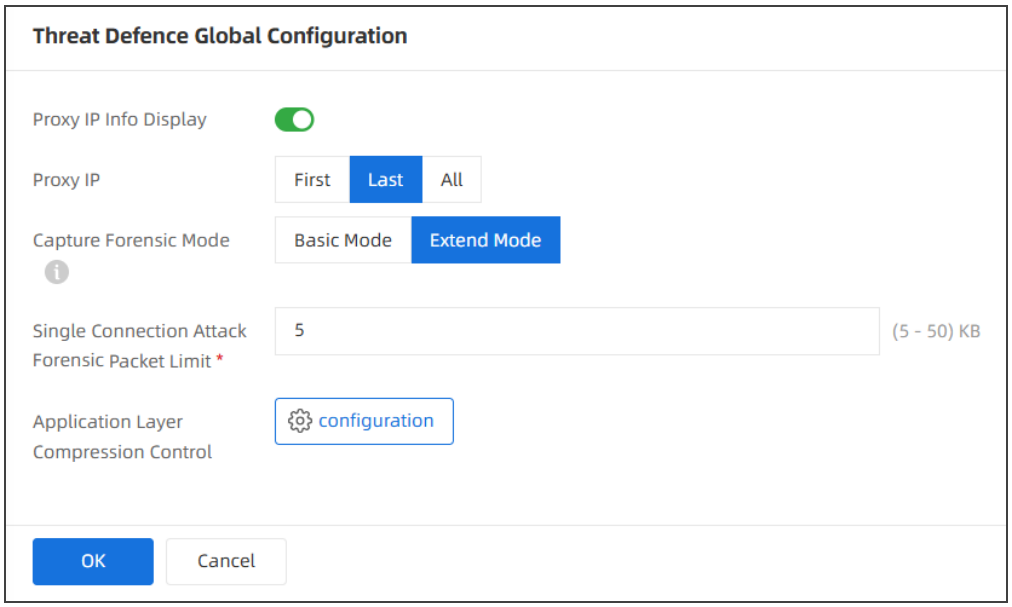
Decompression Control Function Supports Up to 20 Layers of Decompression

WebUI

Configuring The Threat Protection Global Parameters

Configure the global parameters for threat protection, Take the following steps:

1. Click **Object** > **Threat Detection Template** > **Threat Defence Global Configuration**, to open the Global Threat Prevention Configuration page.



On the Threat Defence Global Configuration page, configure the parameter information.

Option	Description
Proxy IP Info Display	Click the **Enable** button to enable the proxy IP inform-

Option	Description
	ation display function. Enabling this function allows the system to record proxy IP information in HTTP traffic when a threat event is detected in an HTTP proxy deployment environment. You can view the proxy IP addresses in the threat logs and threat events. This function is enabled by default. **Note:** The proxy IP information display function operates independently and does not affect the recording of HTTP proxy IP functionality or the X-Forwarded-For configuration in CC protection.
Proxy IP	You can choose to record the first, last, or all IP information in the proxy IP. By default, it records all proxy IP information. **Note:** After choosing to record all proxy IP information, the system will record and display a maximum of the first 5 proxy IP addresses.
Capture Forensic Mode	Specify the packet capture mode, you can choose Basic Mode or Extended Mode, default is Basic Mode. • Basic mode: The system can capture packets when a threat is detected. For the HTTP protocol, the system will capture request and response packets. • Extended mode: The system can capture packet data before and after a threat is detected. The upper limit of captured packet data can be configured

Option	Description
	through the "Number of Packets per Connection for Forensics". For the HTTP protocol in botnet detection and intrusion detection functions, the system will capture request and response packets. Note: Packet capture forensics mode only takes effect for Intrusion Prevention System and Botnet Prevention.
Single Connection Attack Forensic Packet Limit	After selecting the extended mode, you need to configure the upper limit of single connection forensic message volume. Once the limit is reached, the earliest captured packet data will be discarded. Specify the upper limit of the amount of data captured each time, with a range of 5-50KB, defaulting to 5KB.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Application Layer Compression Control</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Decompression</td><td>Click/Do not click the "Enable" button to enable/disable the decompression function.</td></tr>
<tr><td>Maximum Compression Layers</td><td>By default, the system can scan up to 5 layers of nested compressed files (up to 20 layers). You need to configure the number of compressions layers that can be scanned using this option. Select the desired number of layers from the drop-down list. The range is 1-20 layers.</td></tr>
<tr><td>Option</td><td>Specify the action to take for compressed files that exceed the maximum compression layer limit. You can choose:
Log Only - Generates only the relevant log information. This behavior is the system default.
Reset Connection - Reset the compressed file connection.</td></tr>
</table>
</td></tr>
</table>

2. Click OK.

For more information, refer to the **Threat Prevention** section in *StoneOS WebUI User Guide*. FR 45482

CLI

Configuring Decompression Control Function

After configuring the decompression control function, StoneOS can decompress the transmitted compressed files, and can handle the files that exceed the max decompression layer as well as the encrypted compressed files in accordance with the specified actions. This function supports to decompress the files in type of RAR, ZIP, TAR, GZIP, and BZIP2.

The decompression control function are effective for both the file filter function and the Anti-Virus function. For the Anti-Virus function, refer to Anti-Virus.

Enabling / Disabling Decompression Function

StoneOS can decompress the transmitted compressed files. The decompression function is enabled by default. To enable or disable the decompression function, in the global configuration mode, use the following command:

decompression {**enable** | **disable**}

- **enable** | **disable** - Enable(**enable**) or (**disable**) the decompression function.

Specifying the Maximum Decompression Layer

By default, StoneOS can check the files of up to 20 decompression layers. To configure the maximum decompression layers and the actions for the compressed files that exceed the max decompression layer, in the global configuration mode, use the following command:

decompression max-recursion*number***exceed-action** {**log-only** | **reset-conn**}

- *number* - Specifies the decompression layer. The value range is 1 to 20. The default value is 1.
- **log-only** | **reset-conn** - Specifies the action for the compressed files that exceed the maximum decompression layer. The available options include (**log-only**) and (**reset-conn**). The default action is **log-only**.

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

no decompression max-recursion

> **Notes:** For compressed files containing docx, pptx, xlsx, jar, and apk formats, when action is specified as **reset-conn**, the maximum compression layers should be added one more layer to prevent download failure.

Specifying an Action for Encrypted Compressed Files

By default, system not take any actions against the files. To specify an action for encrypted compressed files, in the global configuration mode, use the following command:

decompression encryption-file action {**log-only** | **reset-conn**}

- **log-only** | **reset-conn** – Specifies the action for the encrypted compressed files. The available options include (**log-only**) and (**reset-conn**).

Use the **no decompression encryption-file action** command to restore to the default value.

Viewing Decompression Control Configuration Information

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

show decompression configuration

For more information, refer to the **Data Security & URL Filtering** > **Data Security** > **File Filter** section in *StoneOS CLI User Guide*. FR 45482

Interface Adds Statistics for Different Byte Counts of Received and Sent Packets and Supports Reporting via SNMP

CLI

Viewing Controller Statistics

Controller is the statistical unit in the system used to count packet information at the hardware level. You can view the statistics of the Controller using the following command in any mode:

show controller [**slot** *slot-name*[**index** *index-num*]] [**port** *port-number*] [*interface_name*] **statistic**

- **slot** *slot-name* - Specify the slot number where the expansion module is located, and view the statistics of received and transmitted packets for all interfaces on this module card.
- **index** *index-num* - Specify the forwarding chip index number for the corresponding slot. View packet statistics for the forwarding chip on the specified *slot-name*.
- **port** *port-number* - Specify the interface number, which is the label of the physical interface on the expansion module, such as 0,1,2,3. View packet statistics for the specified physical interface on the expansion module.
- *interface_name* - Specify the interface name to view packet statistics for the designated physical interface on the device.

If none of the parameters are specified, **show controller statistic** indicates viewing packet statistics for all physical interfaces on the device.

For example, after using the **show controller slot 0 port 0 statistic** command, the output information of the statistics is as follows:

```
hostname# show controller slot 0 port 0 statistic
ethernet0/0, physical port 0:
InGoodOctets: 2422834                InBadOctets: 0
```

InGoodPkts: 9053	**InBadPkts:** 0
InUnicastPkts: 0	**InBroadcastPkts:** 0
InMulticastPkts: 9053	**InControlPkts:** 0
InUndersizePkts: 0	**InOversizePkts:** 0
InFragments: 0	**InJabbers:** 0
InMACRcvErrors: 0	**InCRCAlignErrors:** 0
DropEvents: 0	
OutGoodOctets: 512	**OutGoodPkts:** 8
OutUnicastPkts: 0	**OutBroadcastPkts:** 8
OutMulticastPkts: 0	**OutControlPkts:** 0
Collisions: 0	**OutDropDeferrals:** 0
SingleCollisions: 0	**MultipleCollisions:** 0
ExcessiveCollisions: 0	**LateCollisions:** 0
Pkts64Octets: 8	**Pkts65to127Octets:** 0
Pkts128to255Octets: 3020	**Pkts256to511Octets:** 6033
Pkts512to1023Octets: 0	**Pkts1024toMaxOctets:** 0

Description of each parameter in the output information is as follows:

Parameter	Description	Notes
InGoodOctets	Total count of bytes in received valid packets.	
InGoodPkts	Total number of packets of normal messages received.	For X series devices, this parameter's statistical data includes unicast packets + multicast packets + broadcast packets.
InBadOctets	Total number of bytes in received erroneous packets.	

Parameter	Description	Notes
InBadPkts	Total number of received error packets.	For X series devices, the statistical data of this parameter is the sum of the following data: UndersizePkts (total number of normal packets smaller than 64 bytes) + OversizePkts (total number of normal packets larger than 1518 bytes) + Fragments (total number of packets with frame check or alignment errors and smaller than 64 bytes) + Jabbers (total number of packets with frame check or alignment errors and larger than 1518 bytes) + MACRcvErrors (the number of occurrences of the RxErr signal); For A series, K9180, K2680, and K2380 devices, this parameter's statistics are based on hardware packet loss counts.
InUnicastPkts	Total number of unicast packets received.	
InBroadcastPkts	The total number of broadcast packets received (excluding multicast packets).	

Parameter	Description	Notes
InMulticastPkts	Total number of multicast packets received (excluding broadcast packets).	
InControlPkts	Total number of received flow control frames	
InUndersizePkts	Total number of valid packets received that are less than 64 bytes in length.	
InOversizePkts	Total number of normal packets received that are larger than 1518 bytes.	
InFragments	Total number of packets received with frame check sequence (FCS) errors or alignment errors and with a length less than 64 bytes.	
InJabbers	The total number of packets received with frame check sequence (FCS) errors or alignment errors and with a length greater than 1518 bytes.	
InMACRcvErrors	The number of times the RxErr signal is received.	
InCRCAlignErrors	Total number of packets received with frame check sequence (FCS) errors or alignment errors and	

Parameter	Description	Notes
	byte length between 64-1518.	
DropEvents	Total number of events where packets were dropped due to insufficient resources; sometimes this number is not necessarily the number of dropped packets, but the number of times this situation was detected.	For X series devices, this parameter counts the number of packet drops due to insufficient bandwidth; For A series, K9180, K2680, K2380 devices, this parameter counts the number of times the receive buffer allocation fails.
OutGoodOctets	Total number of bytes sent successfully.	
OutGoodPkts	Total number of packets sent successfully.	
OutUnicastPkts	Total number of successfully sent unicast packets.	
OutBroadcastPkts	Total number of broadcast packets sent successfully (excluding multicast packets).	
OutMulticastPkts	Total number of successfully sent multicast packets (excluding broadcast packets).	
OutControlPkts	Total number of successfully sent flow control packets.	
OutDropDeferrals	Total number of packets discarded due to excessive delay.	For A series, K9180, K2680, K2380 devices, this parameter

Parameter	Description	Notes
		counts the total number of packets that failed to send.
Cillisions	The number of MAC layer packet transmission conflicts, excluding Single, Multiple, Excessive, or Late.	For X series devices, this parameter is not supported.
SingleCollisions	Total number of packets successfully transmitted after a single collision.	This parameter is not supported for X series devices.
MultipleCollisions	Total number of packets successfully transmitted after multiple collisions.	For X series devices, this parameter is not supported.
ExcessiveCollisions	Total number of packets successfully transmitted after experiencing 16 collisions.	For X series devices, this parameter counts the number of frames dropped at the MAC layer after multiple collisions.
LateCollisions	The number of frames transmitted with an invalid FCS; this counter also increments if the original FCS of a frame is invalid and the new FCS is also invalid when the frame is modified during transmission.	For X series devices, this parameter's statistics count MAC layer late collision events.
Pkt64Octets	The total number of packets received or sent that are 64 bytes	

Parameter	Description	Notes
	in length (including error packets).	
Pkt65to127Octets	The total number of packets received or transmitted that are 65-127 bytes in length (including error packets).	
Pkt128to255Octets	The total number of packets (including error packets) received or transmitted with lengths between 128-255 bytes.	
Pkt256to511Octets	Total number of packets received or sent with lengths between 256-511 bytes (including error packets).	
Pkt512to1023Octets	The total number of packets (including error packets) received or transmitted that are between 512-1023 bytes in length.	
Pkt1024to1518Octets	The total number of packets (including error packets) received or sent with lengths between 1023-1518 bytes.	

For more information, refer to the **Monitor** > **Monitor** > **User-Defined Monitor** section in *StoneOS CLI User Guide*. FR 38376

MIB

HILLSTONE-IF-MIB

The following tables is the parsing results of HILLSTONE-IF-MIB.

Name	OID	Value
hillstoneWanIfNumber	.1.3.6.1.4.1.28557.2.6.1.1	Data type: Integer32 Description: Number of interfaces bound to WAN Zone
hillstoneLanIfNumber	.1.3.6.1.4.1.28557.2.6.1.2	Data type: Integer32 Description: Number of interfaces bound to other zones (LAN)
hillstoneIfAttriTable: Attributes of all interfaces		
hillstoneIfIndex	.1.3.6.1.4.1.28557.2.6.1.3.1.1	Data type: Integer Description: Interface index, the same as the type of IfIndex node (.1.3.6.1.2.1.2.2.1.1) in IF-MIB (public MIB)
hillstoneIfName	.1.3.6.1.4.1.28557.2.6.1.3.1.2	Data type: String Description: Interface name

Name	OID	Value
hillstoneIfAttribute	.1.3.6.1.4.1.28557.2.6.1.3.1.3	Data type: Integer Description: Type of the binding zone • 0 – Not bound • 1 - LAN Zone • 2 - WAN Zone
hillstoneIfNetAddress	.1.3.6.1.4.1.28557.2.6.1.3.1.4	Data type: IP Address Description: Interface IP address
hillstoneIfNetMask	.1.3.6.1.4.1.28557.2.6.1.3.1.5	Data type: IP Address Description: Netmask of the interface IP address
hillstoneIfManageIp	.1.3.6.1.4.1.28557.2.6.1.3.1.6	Data type: IP Address Description: Management IP of the interface (if no management IP is configured, the interface IP will be shown).
hillstoneIfSecIpAddress0	.1.3.6.1.4.1.28557.2.6.1.3.1.7	Data type: IP Address Description: Sec-

Name	OID	Value
		ondary IP address 0 of the interface
hillstoneIfSecNetMask0	.1.3.6.1.4.1.28557.2.6.1.3.1.8	Data type: IP Address Description: Net-mask of secondary IP address 0 of the interface
hillstoneIfSecIpAddress1	.1.3.6.1.4.1.28557.2.6.1.3.1.9	Data type: IP Address Description: Sec-ondary IP address 1 of the interface
hillstoneIfSecNetMask1	.1.3.6.1.4.1.28557.2.6.1.3.1.10	Data type: IP Address Description: Net-mask of secondary IP address 1 of the interface
hillstoneIfSecIpAddress2	.1.3.6.1.4.1.28557.2.6.1.3.1.11	Data type: IP Address Description: Sec-ondary IP address 2 of the interface
hillstoneIfSecNetMask2	.1.3.6.1.4.1.28557.2.6.1.3.1.12	Data type: IP Address Description: Net-mask of the sec-ondary IP address 2

Name	OID	Value
		of the interface
hillstoneIfSecIpAddress3	.1.3.6.1.4.1.28557.2.6.1.3.1.13	Data type: IP Address Description: Secondary IP address 3 of the interface
hillstoneIfSecNetMask3	.1.3.6.1.4.1.28557.2.6.1.3.1.14	Data type: IP Address Description: Netmask of secondary IP address 3 of the interface
hillstoneIfSecIpAddress4	.1.3.6.1.4.1.28557.2.6.1.3.1.15	Data type: IP Address Description: Secondary IP address 4 of the interface
hillstoneIfSecNetMask4	.1.3.6.1.4.1.28557.2.6.1.3.1.16	Data type: IP Address Description: Netmask of secondary IP address 4 of the interface
hillstoneIfSecIpAddress5	.1.3.6.1.4.1.28557.2.6.1.3.1.17	Data type: IP Address Description: Secondary IP address 5 of the interface
hillstoneIfSecNetMask5	.1.3.6.1.4.1.28557.2.6.1.3.1.18	Data type: IP

Name	OID	Value
		Address Description: Net-mask of secondary IP address 5 of the interface
HillstoneIfInRate	.1.3.6.1.4.1.28557.2.6.1.3.1.19	Data type: Counter64 Description: Real-time ingress inter-face rate. Unit: bps
hillstoneOutRate	.1.3.6.1.4.1.28557.2.6.1.3.1.20	Data type: Counter64 Description: Real-time egress inter-face rate. Unit: bps
hillstoneInPps	.1.3.6.1.4.1.28557.2.6.1.3.1.21	Data type: Counter64 Description: Real-time packets per second the interface received. Unit: pps
hillstoneOutPps	.1.3.6.1.4.1.28557.2.6.1.3.1.22	Data type: Counter64 Description: Real-time packets per second the interface sent. Unit: pps
hillstoneIfDiscards	.1.3.6.1.4.1.28557.2.6.1.3.1.23	Data type: Counter64

Name	OID	Value
		Description: Hardware packet loss data of the physical interface.
hillstoneIfInRateIPv4	.1.3.6.1.4.1.28557.2.6.1.3.1.24	Data type: Counter64 Description: IPv4 traffic rate of ingress interface
hillstoneIfInRateIPv6	.1.3.6.1.4.1.28557.2.6.1.3.1.25	Data type: Counter64 Description: IPv6 traffic rate of ingress traffic
hillstoneIfOutRateIPv4	.1.3.6.1.4.1.28557.2.6.1.3.1.26	Data type: Counter64 Description: IPv4 traffic rate of egress interface
hillstoneIfOutRateIPv6	.1.3.6.1.4.1.28557.2.6.1.3.1.27	Data type: Counter64 Description: IPv6 traffic rate of egress interface
hillstoneIfSfpModuleTemperature	.1.3.6.1.4.1.28557.2.6.1.3.1.28	Data Type: DisplayString Description: Current Temperature of the transceiver

Name	OID	Value
		module.
hillstoneIfSfpTxSupplyVoltage	.1.3.6.1.4.1.28557.2.6.1.3.1.29	Data Type: DisplayString Description: The supply voltage of the transmitting transceiver module.
hillstoneIfSfpTxBiasCurrent	.1.3.6.1.4.1.28557.2.6.1.3.1.30	Data Type: DisplayString Description: The bias current of the transmitting transceiver module.
hillstoneIfTxOpticalPower	.1.3.6.1.4.1.28557.2.6.1.3.1.31	Data Type: DisplayString Description: The optical power of the transmitting transceiver module
hillstoneIfRxOpticalPower	.1.3.6.1.4.1.28557.2.6.1.3.1.32	Data Type: DisplayString Description: The optical power of the receiving transceiver module
hillstoneInGoodOctets	.1.3.6.1.4.1.28557.2.6.1.3.1.35	Data type: Counter64 Description: The total byte count of

Name	OID	Value
		normal packets received by the interface.
hillstoneInBadOctets	.1.3.6.1.4.1.28557.2.6.1.3.1.36	Data type: Counter64 Description: The total byte count of error packets received by the interface.
hillstoneInGoodPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.37	Data type: Counter64 Description: The total number of normal packets received by the interface. Note: For X series devices, this parameter's statistical data includes unicast packets + multicast packets + broadcast packets.
hillstoneInBadPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.38	Data type: Counter64 Description: Total number of error packets received by the interface.

Name	OID	Value
		Note: For X-series devices, this parameter's statistical data is the sum of the following data: UndersizePkts (total number of valid packets smaller than 64 bytes) + OversizePkts (total number of valid packets larger than 1518 bytes) + Fragments (total number of packets with frame check or alignment errors and smaller than 64 bytes) + Jabbers (total number of packets with frame check errors followed by alignment errors and larger than 1518 bytes) + MACRcvErrors (number of occurrences of the RxErr signal); For A-series, K9180, K2680, K2380 devices, this

Name	OID	Value
		parameter's statistical data is the hardware packet drop count.
hillstoneInUnicastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.39	Data type: Counter64 Description: Total number of unicast packets received by the interface.
hillstoneInBroadcastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.40	Data type: Counter64 Description: The total number of broadcast packets received by the interface (excluding multicast packets).
hillstoneInMulticastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.41	Data type: Counter64 Description: The total number of multicast packets received by the interface (excluding broadcast packets).
hillstoneInCRCAlignErrors	.1.3.6.1.4.1.28557.2.6.1.3.1.42	Data type: Counter64 Description: The

Name	OID	Value
		total number of packets received by the interface with frame check sequence (FCS) errors or alignment errors and byte lengths between 64-1518.
hillstoneDropEvents	.1.3.6.1.4.1.28557.2.6.1.3.1.43	Data type: Counter64 Description: The total number of events where packets were discarded due to insufficient resources; sometimes this number is not necessarily the count of discarded packets, but just the number of times this situation was detected. Note: For X-series devices, this parameter counts the number of packet drops due to insufficient bandwidth; for A-series, K9180,

Name	OID	Value
		K2680, and K2380 devices, this parameter counts the number of receive buffer allocation failures.
hillstoneOutGoodOctets	.1.3.6.1.4.1.28557.2.6.1.3.1.44	Data type: Counter64 Description: Total number of bytes sent successfully by the interface.
hillstoneOutGoodPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.45	Data type: Counter64 Description: Total number of data packets successfully sent by the interface.
hillstoneOutUnicastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.46	Data type: Counter64 Description: The total number of unicast packets sent successfully by the interface.
hillstoneOutBroadcastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.47	Data type: Counter64 Description: The

Name	OID	Value
		total number of broadcast packets successfully sent by the interface (excluding multicast packets).
hillstoneOutMulticastPkts	.1.3.6.1.4.1.28557.2.6.1.3.1.48	Data type: Counter64 Description: Total number of successfully sent multicast packets on the interface (excluding broadcast packets).
hillstoneOutDrop	.1.3.6.1.4.1.28557.2.6.1.3.1.49	Data type: Counter64 Description: The total number of packets discarded due to excessive delay. Note: For A series, K9180, K2680, and K2380 devices, this parameter's statistical data represents the total number of packets that failed to send.
hillstonePkts64Octets	.1.3.6.1.4.1.28557.2.6.1.3.1.50	Data type:

Name	OID	Value
		Counter64 Description: The total number of packets, including error packets, that the interface receives or sends with a length of 64 bytes.
hillstonePkts65to127Octets	.1.3.6.1.4.1.28557.2.6.1.3.1.51	Data type: Counter64 Description: The total number of packets (including error packets) received or transmitted by the interface that are 65-127 bytes in length.
hillstonePkts128to255Octets	.1.3.6.1.4.1.28557.2.6.1.3.1.52	Data type: Counter64 Description: The total number of packets (including error packets) received or transmitted by the interface with a length between 128-255 bytes.

Name	OID	Value
hillstonePkts256to511Octets	.1.3.6.1.4.1.28557.2.6.1.3.1.53	Data type: Counter64 Description: The total number of packets (including error packets) received or transmitted by the interface with a length between 256-511 bytes.
hillstonePkts512to1023Octets	.1.3.6.1.4.1.28557.2.6.1.3.1.54	Data type: Counter64 Description: The total number of packets (including error packets) received or transmitted by the interface with lengths between 512-1023 bytes.
hillstoneInOverMax	.1.3.6.1.4.1.28557.2.6.1.3.1.55	Data type: Counter64 Description: The total number of packets, including error packets, received or transmitted by the interface that exceed

Name	OID	Value
		1024 bytes in length.

Notes: MIB information of OID .1.3.6.1.4.1.28557.2.6.1.3.1.28 to .1.3.6.1.4.1.28557.2.6.1.3.1.32 is only supported in SG-6000-A200/A200G4/A200W/A200WG4.

For more information, refer to *StoneOS SNMP MIB Reference Guide*. FR 38376

Optimizing XSS Injection Check and SQL Injection Check Functions

WebUI

Configuring an IPS Rule

System has three default IPS rules: **predef_default** , **predef_loose** and **predef_critical**.

- The **predef_default** rule is configured with IPS signatures of medium and high confidence levels, this rule can be used to detect threats and perform the default rule action.
- The **predef_loose** rule is configured with all the IPS signatures and its default action is log only.
- The **predef_critical** rule is configured with IPS signatures of the latest high-risk attacks and its default action is reset.

The system supports up to 64 user-defined IPS rules and each non-root VSYS supports up to 4 user-defined IPS rules.

To configure an IPS rule, take the following steps:

1. Select **Object > Intrusion Prevention System > Profile**.

2. Click **New** to create a new IPS rule. To edit an existing one, select the check box of this rule and then click **Edit**. To view it, click the name of this rule.



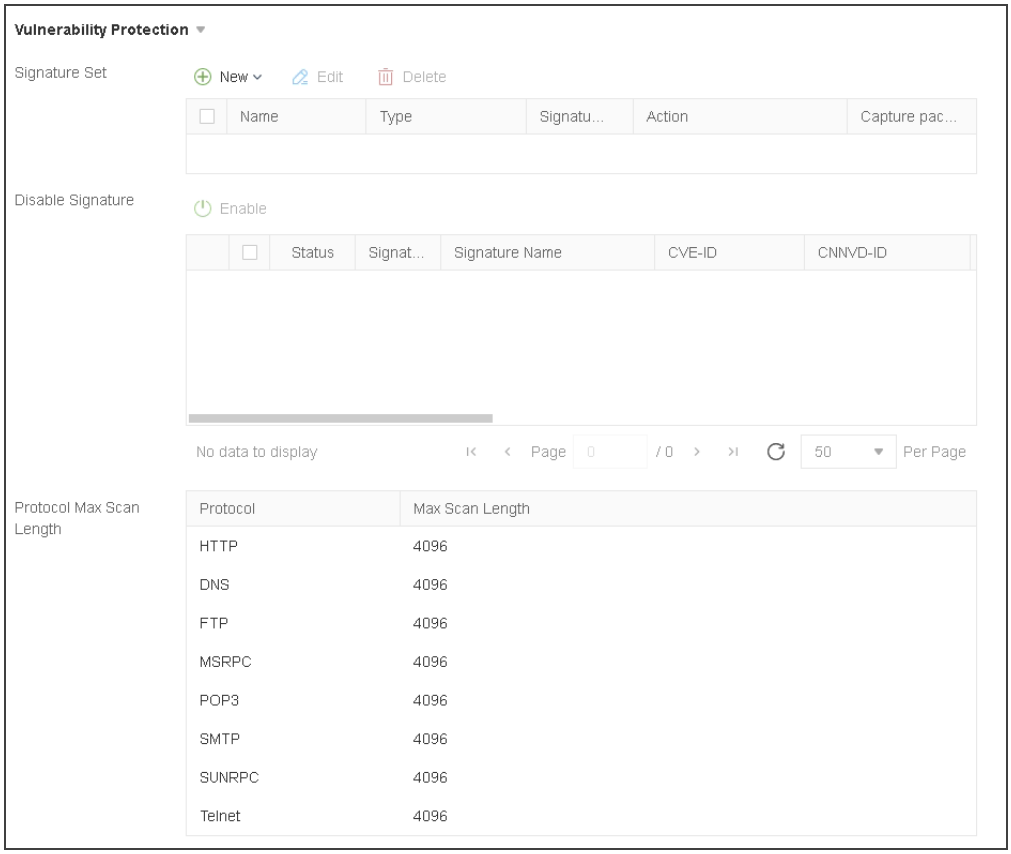
Note: A navigation bar is located on the right side of the **IPS Configuration** page. You can click any option to go to the corresponding section.

3. Configure the basic information of the profile:

Option	Description
Name	In the Name text box, enter the name of the newly-created IPS IDS profile. If you just configure the name and click **OK**, this profile will not take effect.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. **Notes:** For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to

Option	Description
	enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.
Description	Type the description information into the **Description** text box.

4. In the **Vulnerability Protection** section, click ▸ next to Vulnerability Protection to expand this section, including **Signature Set** and **Protocol Max Scan Length**.



5. In the signature configuration area, configure signature set rules and disable signatures.

    i. In the **Signature Set** area, the existing signature sets and their settings will be displayed in the table. Select the desired signature sets. You can also manage the signature sets, including **New**, **Edit**, and **Delete**. When creating a new signature set rule, you can select **Filtering Signature** or **Selection Signature** as needed to filter and retrieve the signature database to select the desired signature sets.

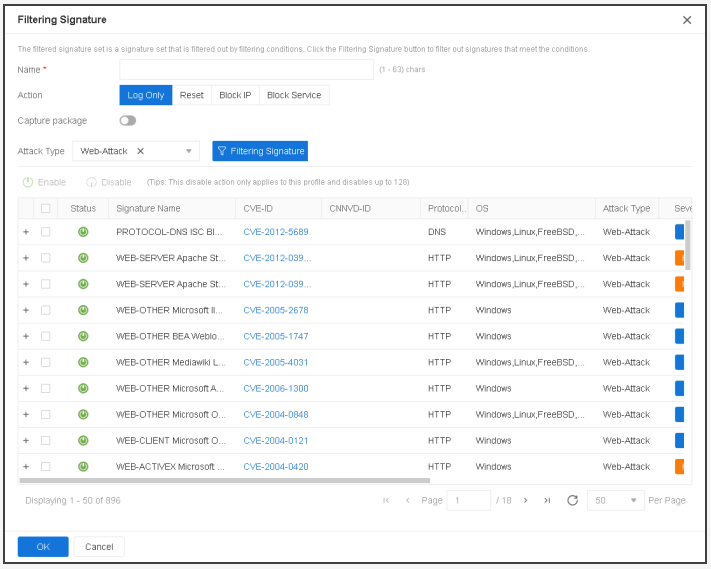
    - Filtering Signature: Filter signature sets by certain filter conditions. Click the **Filter Signature** button to search for the signatures you want. In this way, you can quickly select the signatures that have been classified by system.

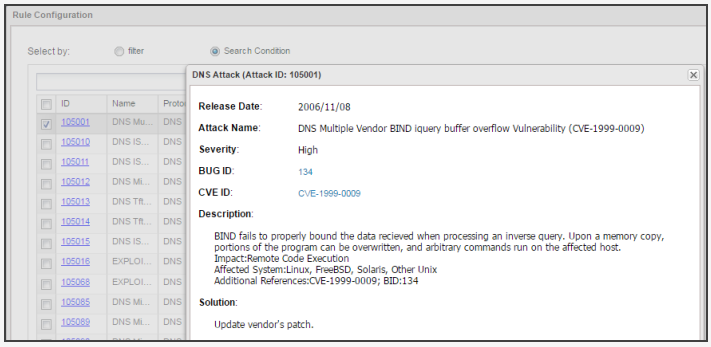
- Selection Signature: Select a particular signature set from the signature database. In this way, you can quickly select a particular signature.

ii. Click New and select Filtering Signature or Selection Signature to create a new signature set rule.

Option	Description
Name	Specify the name of signature.
Action	Specify the action performed on the abnormal traffic that matches the signature set. • Log Only: Record a log. • Reset: Reset connections (TCP) or send destination unreachable packets (UDP) and also generate logs. • Block IP: Block the IP address of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the

Option	Description
	attacker. • Default: Excute the action specifiled in the signature rule.
Packet Capture Forensic	Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
Filtering Signature	If **Filtering Signature** is selected: System categorizes the signatures according to the following aspects (aka main categories): affected OS, attack type, protocol, severity, confidence, released year, affected application, and bulletin board. A signature can be in several subcategories of one main category. For example, the signature of ID 200211 is in the Linux subcategory, the FreeBSD subcategory, and Other Linux subcategory at the same time. Note: By default, **Filtering Signature** filters signatures based on all subcategories of severity. You can select other dimensions for filtering. You can view the detailed information of the signature by clicking the signature ID, and you can select one or more signatures. Click the Disable or Enable button to disable or re-enable the signature. **Note**: The enabled/disabled state here is only for the current profile, but the global state is not affected.

Option	Description
	 When selecting main category and subcategory, note the following matters: • You can select multiple subcategories of one main category. The logic relation between them is OR. • The logic relation between each main category is AND. • For example, you have selected Windows and Linux in OS and select HIGH in Severity. The chosen signatures are those whose severity is high and meanwhile whose affected operating system is either Windows or Linux.
Selection Signature	If **Selection Signature** is selected: Type the signature information into the **Keyword** text box, and system will

Option	Description
	perform fuzzy search in the following fields: signature ID, signature name, and description.  After the matched signature is found, select the signature, and it will be added to the Selected Signatures tab, indicating the signature is included in the signature set. After the matched signature is found, select the signature, and then click the Enable or Disable button to disable or re-enable the signature. The enabled/disabled state here is only for the current profile, but the global state is not affected.
Note: You create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature , system will adopt the following rules: • Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only > Deault. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s.	

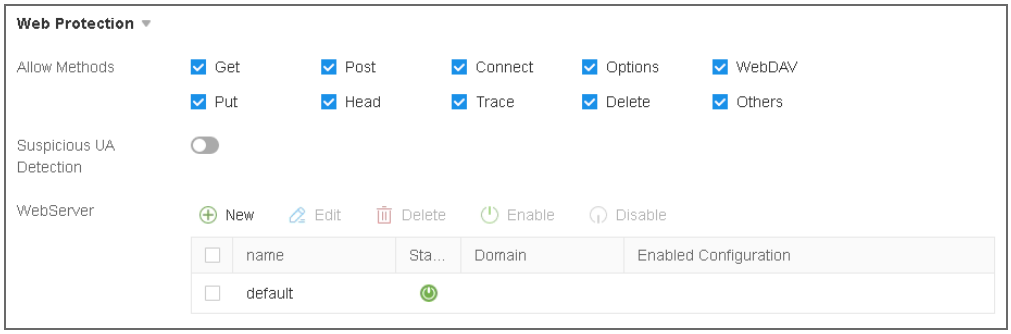
Option	Description
	• If one signature set is configured with Capture Packet, system will capture the packets. • The action of the signature set created by Selection Signature has higher priority than the action of the signature set created by Filter.

iii. Click **OK** to complete signature set configurations.

iv. In the Disable Signature section, the signatures that are Disabled in the template will be shown. Select one or more signatures, and then click the **Enable** button to re-enable the signature.

6. In the **Protocol Max Scan Length** section of **Vulnerability Protection**, click the max scan length of any protocol in the table to modify it. You can configure the max scan length of the HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet protocols. Default max scan length: 4096 bytes. Valid values: 0 to 65535 bytes, in which 0 indicates no limits.

7. In the Web Protection section, click ▸ next to Web Protection to expand this section.



Option	Description
Allow Methods	Specify the HTTP method that is allowed, including Get, Post, Connet, Options, WebDAV, Put, Head, Trace, Delete, and Others.

Option	Description
Suspicious UA Detection	Turn on the switch to enable the Suspicious UA Detection function. With this function enabled, the system detects User-Agent in HTTP Request messages. When User-Agent is detected as abnormal in HTTP messages, you can specify the action to handle User-Agent.

	Action: Specify the action to be performed when suspicious UA is detected.
	• Log Only: Record a log.
	• Block IP: Block the IP address of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service: Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the

Option	Description
	attacker.

To protect the Web server, configure Web Server in the HTTP tab.

Protecting the Web server means system can detect the following attacks: Sensitive File Scan, High Frequency Access Control, SQL injection, XSS injection, external link check, hotlinking check, iframe attack, ACL, and HTTP request flood and take actions when detecting them.

A pre-defined Web server protection rule named **default** is built in. The **default** rule supports only the following protection functions: Sensitive File Scan, SQL injection protection, XSS injection detection, iframe check, ACL, and HTTP request flood protection. By default, this protection rule is enabled and cannot be disabled or deleted. Each IPS rule can configure at most 32 Web server protection rules, excluding the **default** rule.

Configure the following settings to protect the Web server:

Option	Description
Name	Specify the name of the Web server protection rule.
Configure Domain	Specify domains protected by this rule. Click the link and the Configure Domain page will appear. Enter the domain names in the **Domain** text box. At most 5 domains can be configured. The traffic to these domains will be checked by the protection rule. The domain name of the Web server follows the longest match rule from the back to the front. The traffic that does not match any rules will match the default Web server. For example, you have configured two protection rules: **rule1 and rule2**. The domain name in rule1 is abc.com. The domain name in rule2 is email.abc.com. The traffic that visits news.abc.com will match

Option	Description
	rule1, the traffic that visits www.email.abc.com will match rule2, and the traffic that visits www.abc.com.cn will match the default protection rule.
High Frequency Access Control	Click the Enable button to enable the High Frequency Access Control feature. When this function is enabled, system will block the traffic of this IP address， whose access frequency exceeds the threshold. • Threshold: Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, system will block the flow of the IP. The value ranges from 1 to 65535 times per minute. • URL Path: Click the link and the URL Page Configuration page appears. Click **New** and enter the URL path in the **Path** text box. After the configuration, all paths that contain the name of the path are also counted. System accesses the frequency statistics for HTTP requests that access these paths. If the access frequency of the HTTP request exceeds the threshold, the source IP of the request is blocked, and the IP will not be able to access the Web server. For example: configure'/home/ab', system will perform a frequency check on the 'access/home/ab/login' and '/home/BC/login' HTTP requests. URL path does not support the path format which contains the host name or

Option	Description
	domain name, for example: you can not configure www.baidu.com/home/login.html, you should configure '/ home / login.html', and 'www.baidu.com' should be configured in the corresponding Web server domain name settings. You can configure up to 32 URL paths. The length of each path is in the range of 1-255 characters. **Note**: Non-root VSYS does not support the High Frequency Access Control.
Sensitive File Scan	Select Enable to enable the Sensitive File Scan function for Web servers. In Sensitive File Scan attacks, an attacker traverses the sites in the Web server by using a file scanning tool. This way, the attacker can obtain sensitive information of the Web server, such as the directory structure, background files, and backup files. If an attacker attempts to scan sensitive files on the Web server, the Web server returns a large number of response packets with the status code "404". In this case, the system counts the number of 404 responses returned by the Web server per minute. ① If the number is greater than 10, the system parses the URLs in all HTTP requests and matches them with the built-in sensitive file dictionary. If the number of times that the parsed URL matches the sensitive file dictionary exceeds the specified threshold, the system performs the user-specified protection actions. The specified actions can be Log Only, Reset, Block IP, or Block Service. ②If

Option	Description

	the number is equal to or greater than 100, the system determines the behavior as a sensitive file scanning attack and performs the specified protection action.
	• Threshold: Specifies the threshold for the system to defend against sensitive file scanning attacks. If the number of times that URL paths match sensitive file dictionaries per minute exceeds the threshold, the system performs the user-specified protection actions. Default value: 10. Valid values: 10 to 100. Unit: times/min.
	• Action: Specifies the protection action for the system to defend against sensitive file scanning attacks: Log Only, Block IP, or Block Service.
	  • Log Only: record a log.
	  • Reset: Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
	  • Block IP: Block the IP address of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the attacker's IP address of the attacker.

Option	Description
	• Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
SQL Injection Protection	Click the Enable button to enable SQL injection check. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Check point: Specifies the check point for the SQL injection check. It can be Cookie, Cookie2, Post, Referer, URI or Additional_Headers. • Sensitivity: The sensitivity level determines the strictness of SQL injection checks. Different levels affect the detection rate of injection attacks and false positives. The system's

Option	Description
	default sensitivity level is "Medium". Specifically as follows: • When the sensitivity is set to "High", the system has a higher detection rate for injection attacks, but it may also increase the false positive rate; • When the sensitivity is set to "Low", the system's injection attack detection rate will decrease, but the false positive rate will also be relatively lower; • When the sensitivity is set to "Medium", the system's injection attack detection rate and false positive rate reach a relatively balanced state. It can effectively detect injection attacks while avoiding too many false positives, meeting the requirements of most usage scenarios. Therefore, you need to set the sensitivity to "Medium".
XSS Injection Protection	Click the Enable button box to enable XSS injection check for the HTTP protocol. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and

Option	Description

	also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration.
	• Check point: Specifies the check point for the XSS injection check. It can be Cookie, Cookie2, Post, Referer, URI or Additional_Headers.
	• Sensitivity: The sensitivity level determines the strictness of XSS injection checks. Different levels affect the detection rate of injection attacks and false positives. The system's default sensitivity level is "Medium". Specifically as follows:
	  • When the sensitivity is set to "High", the system has a higher detection rate for injection attacks, but it may also increase the false positive rate;
	  • When the sensitivity is set to "Low", the system's injection attack detection rate will decrease, but the false positive rate will also be relatively lower;
	  • When the sensitivity is set to "Medium", the system's injection attack detection rate and false positive rate reach a relatively balanced state. It can effectively detect injection attacks while avoiding too many false positives, meeting the requirements of most usage

Option	Description
	scenarios. Therefore, you need to set the sensitivity to "Medium".
External Link Check	Click the Enable button to enable external link check for the Web server. This function controls the resource reference from the external sites. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • External link exception: Click this link, and the External Link Exception Configuration page will appear. All the URLs configured on this page can be linked by the Web sever. At most 32 URLs can be specified for one Web server. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
Hotlinking Check	Click the Enable button to enable Hotlinking Check. System checks the headers of the HTTP packets and obtains the source site of the HTTP request. If the source site is in the Hotlinking Exception list, system will release it; otherwise, log or reset the connection. Thus controlling the Web site from other sites and to prevent chain of CSRF (Cross Site Request Forgery cross-site

Option	Description
	request spoofing) attacks occur. • Hotlinking Exception: Click the 'Hotlinking Exception ' to open the <Hotlinking Exception Configuration> page, where the configured URL can refer to the other Web site. Each Web server can be configured with up to 32 URLs. • Action: Specify the action for the HTTP request for the chaining behavior, either "Log only" or "Reset". “
Iframe check	Click the Enable button to enable iframe checking. System will identify if there are hidden iframe HTML pages by this function, then log it or reset its link. After iframe checking is enabled, system checks the iframe in the HTML page based on the specified iframe height and width, and when any height and width is less than or equal to the qualified value, system will identify as a hidden iframe attack, record, or reset connection that occurred. • Height: Specifies the height value for the iframe, range from 0 to 4096. • Width: Specifies the width value of the iframe, range from 0 to 4096. • Action: Specify the action for the HTTP request that hides iframe behavior, which is 'Only logged' or 'Reset'. Log Only - Record a log.

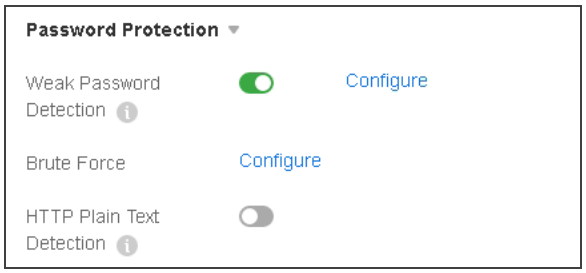
Option	Description
	Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
ACL	Click the Enable button to enable access control for the Web server. The access control function checks the upload paths of the websites to prevent the malicious code uploading from attackers. • ACL: Click this link, the ACL Configuration page appears. Specify websites and the properties on this page. "Static" means the URI can be accessed statically only as the static resource (images and text), otherwise, the access will handle as the action specified (log only/reset); "Block" means the resource of the website is not allowed to access. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
HTTP Request Flood Protection	Select the Enable check box to enable the HTTP request flood protection. Both IPv4 and IPv6 address are supported. • Request threshold: Specifies the request threshold. For the protected domain name, when the number of HTTP connecting request per second reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack, and will enable the HTTP request flood protection. • When the number of HTTP connecting request per second

Option	Description
	by the object reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack by this object, and will enable the HTTP request flood protection. • x-forwarded-for: Select None, system will not use the value in x-forwarded-for as the statistic object. Select First, system will use the first value of the x-forwarded-for field as the statistic object. Select Last, system will use the last value of the x-forwarded-for field as the statistic object. Select All, system will use all values in x-forwarded-for as the statistic object. • x-real-ip: Select whether to use the value in the x-real-ip field as the statistic field. When the HTTP request flood attack is discovered, you can make the system take the following actions: • Authentication: Specifies the authentication method. System judges the legality of the HTTP request on the source IP through the authentication. If a source IP fails on the authentication, the current request from the source IP will be blocked. The available authentication methods are: • No Authentication: The system does not authenticate the source IP of the HTTP request. • Auto (JS Cookie): The Web browser will finish the

Option	Description
	authentication process automatically. • Auto (Redirect): The Web browser will finish the authentication process automatically. • Manual (Access Configuration): The initiator of the HTTP request must confirm by clicking OK on the returned page to finish the authentication process. • Manual (CAPTCHA): The initiator of the HTTP request must be confirmed by entering the authentication code on the returned page to finish the authentication process. • Crawler-friendly: When the authentication method is selected as **Auto (JS Cookie)**, **Auto (Redirect)**, **Manual (Access Configuration)** or **Manual (CAPTCHA)**, you can enable the Crawler-friendly function. If this button is clicked, system will not authenticate to the crawler. • Request limit: Specifies the request limit for the HTTP request flood protection. After configuring the request limit, system will limit the request rate of each source IP. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enable button.

Option	Description
	• Proxy limit: Specifies the proxy limit for the HTTP request flood protection. After configuring the proxy limit, system will check whether each source belongs to the each source IP proxy server. If belongs to, according to configuration to limit the request rate. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enbale button. • Allow List: Specifies the allow list for the HTTP request flood protection. The source IP added to the allow list will not check the HTTP request flood protection. **Note**: Non-root VSYS does not support the HTTP Request Flood Protection.

8. In the Password Protection section, click ▸ next to **Password Protection** to expand this section, including Weak Password Detection, Brute Force, HTTP Plain Text Detection, and HTTP Password Protect Configuration.



   i. Turn on the **Weak Password Detection** switch to enable this function. Then, the system checks the strength of the plaintext password which is set under the

FTP/Telnet/POP3/IMAP/SMTP/HTTP protocols in this profile. The password is detected as weak if it meets the conditions configured in the Weak Password Detection section. In this case, the system issues an alarm log to prevent potential security risks caused by a weak password. Click Configure to configure the detection parameters of the weak password.

Note: When SSL proxy is configured in the policy, you can detect weak password for encrypted protocols such as HTTP.

Configure the detection parameters of the weak password.

Option	Description
Password Length	Specify the length criterion of the password. If a password is shorter than the length criterion, it will be detected as a weak password. The default length criterion is 6 characters. You can specify the password length criterion from 6 characters to 50 characters.
Password Character Type	Specify how many character types should be covered in the password. There are four types of characters: digits, uppercase letters, lowercase letters, and symbols. If the character types covered in a password are less than the specified number, the password will be detected as a weak password. By default, the system will detect the password containing less than 2 character types as a weak password and you can specify up to 4 character types for the detection of the password character type.
Other situations:	In the following situations, the password will be detected as a weak password: User Name Equals Password, Continuous Character Detection, FTP Anonymous Login Detection.

Option	Description
	• **User Name Equals Password**: The password that equals the user name will be detected as a weak password after the detection function is enabled. • **Continuous Character Detection**: After this detection is enabled, a password that has less than 10 characters, among which at least 8 characters are the same or in consecutive sequence, will be detected as a weak password, such as 1aaaaaaaa, 1abcdefgh, a87654321. • **FTP Anonymous Login Detection**: When you log in anonymously through FTP, the system identifies your password as a weak password.
Specify Weak Password	You can specify the weak passwords. If a password matches the specified weak password, the system will consider the password as a weak one. You can specify up to 100 weak passwords.

ii. Click **Configure** next to **Brute Force** to go to the **Brute Force** panel. You can configure to block the brute force attacks under the FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP/HTTP protocol.

Note: The blocklist of brute-force attack IP does not take effect after the system is restarted.

To configure the protocol, click the Enable button behind the protocol. To enable/disable all protocols, click Enable All or Disable All.

Option	Description
FTP/MSRPC/ POP3/SMTP/ SUNRPC/Telnet/ IMAP/SSH/ LDAP/SMB/ VNC/RDP	**Action for Brute-force**: If the login attempts per 5 minutes fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Click the **Enable** button to enable brute-force. • Login Threshold per 5 Mins: Specifies a permitted authentication/login failure count per 5 minutes. • Action: Block the IP address of the attacker • Block Time: Specifies the block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. • Time Unit: If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address or the service of the attacker.

iii. Turn on the **HTTP Plain Text Detection** switch to enable this function. Then, the system checks the password field in the HTTP packet. If the password is not encrypted, an alarm log is generated.

Note: When the login is successful, the system performs plaintext detection only against the password in the HTTP packet but not the HTTPs packet because the HTTPS protocol is not transmitted in plaintext by default.

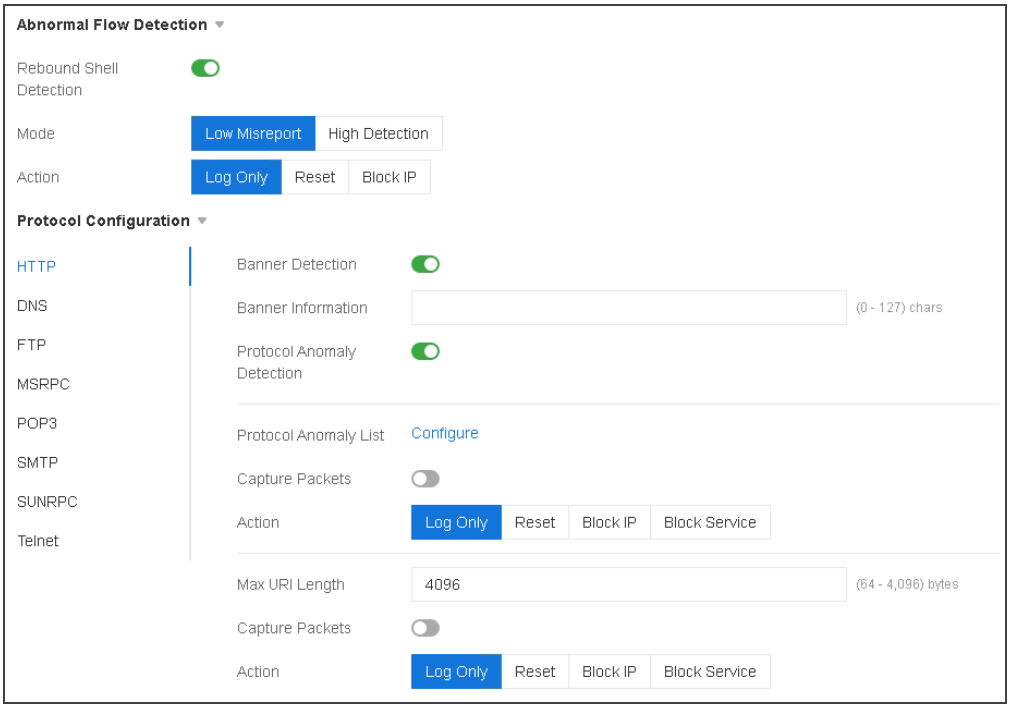
iv. In the **HTTP Password Protect Configuration** section, you can configure the username field , password field, success-login response code, success-login field, fail-login response code, and fail-login field in the HTTP login packet. The system can determine whether the login password is weak and whether there is brute-force attack by parsing the username, password, and login results contained in the HTTP login packet. The system is configured with a list of default username field, password field, and login result fields. However, the content of the HTTP protocol depends on the negotiation between the client and the server, therefore, to avoid false negatives, you can customize fields that tell information about the username, password, successful login, and failed login in the actual HTTP packet. This way, the system detects weak password and brute-force attacks and perform corresponding actions according to the configured rules.

Configure the following options in the HTTP Password Protect Configuration.

Option	Description
Username Field(s)	Specifies the username field in the HTTP login packet. The username field is case insensitive. Multiple fields can be separated with a semicolon. For example, username;user;usrname;j_username.
Password Field(s)	Specifies the password field in the HTTP login packet. The password field is case insensitive. Multiple fields can be separated with a semicolon. For example, password;passwd;pass;pwd;j_password.
Success-login Response	Specifies the success-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semi-

Option	Description
Code(s)	colon. For example, 200;302;201.
Success-login Field(s)	Specifies the success-login field in the HTTP login packet. The success-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, login-success;login-success.
Fail-login Response Code(s)	Specifies the fail-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semicolon. For example, 200;302;201;303.
Fail-login Field(s)	Specifies the fail-login field in the HTTP login packet. The fail-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, loginerror;login-error;loginerr.

9. In the **Abnormal Flow Detection** section, click ▸ next to **Abnormal Flow Detection** to expand this section, including **Rebound Shell Detection and Protocol Configuration**.



i. Turn on the switch next to Rebound Shell Detection and configure this function.

Option	Description
Action	Specifies the defend action against the rebound shell attacks. • Log Only - The system only generate logs when it detects the rebound shell attacks. • Reset - When a rebound shell attack is detected, the system resets connection (TCP) or sends destination unreachable packets (UDP), and then generates logs. • Block IP - Block the IP address of the rebound shell attacker and configure the block time. • Block Time: The default value is 60 seconds. The value range is from 60 to 3600 seconds. If longer block duration is needed, you can select bigger time unit, such as Hour or Day. You can also block the attacker IP permanently.
Mode	Specifies the detect and defend mode for the rebound shell attacks. • Low Misreport: When the system scans to detect keywords of the rebound shell attack, logs are reported only when the keywords are hit more than four time. This mode can be used in scenarios where high system performance is required.

Option	Description
	• High Detection: When the system scans to detect keywords of the rebound shell attack, logs are reported when the keywords are hit more than twice. This mode can be used in scenarios with high requirements for attack detection.

ii. Click ▸ next to **Protocol Configuration**. System supports the configurations of HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet.

In the HTTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the HTTP packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to

Option	Description

	enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
	ation, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max URI Length**: Specify a max URI length for the HTTP protocol. If the URI length exceeds the limitation, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the DNS tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Select **Enable** to analyze the DNS packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For

Option	Description

	more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration

Option	Description
: Click **Configure** to open	In the FTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the FTP packets. If abnormal contents exist, you can:

	Protocol Anomaly list: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules.
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also

Forensic: Click the **Enable** button to enable	

Option	Description

	generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

	Max Command Line Length: Specifies a max length (including carriage return) for the FTP command line. If the length exceeds the limits, you can:

Option	Description
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.
	Max Response Line Length: Specifies a max length for the FTP response line.If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the MSRPC tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Select **Enable** to analyze the MSRPC packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to

Option	Description

	enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
	ation, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Bind Length**: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Request Length**: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.

Option	Description

	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you

Option	Description
Max Bind Length: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet Forensic: Click the **Enable** button to enable	

Option	Description
capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset;	

Option	Description
Block IP; Block Service.	
Max Request Length: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button	

Option	Description
to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.	

Option	Description
• Action: Log Only; Reset; Block IP; Block Service.	

In the POP3 tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against POP3 server banners. • Banner information - Type the new information into the box that will replace the original server banner information.
Protocol Anomaly Detection	Click the **Enable** button to analyze the POP3 packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click **Disable** to disable the rules.

Option	Description

	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you

Option	Description
	want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Command Line Length**: Specifies a max length (including carriage return) for the POP3 command line. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Parameter Length**: Specifies a max length for the POP3 client command parameter. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Times**: Specifies a max failure time (within one single POP3 session) for the POP3 server. If the failure

Option	Description
	time exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the SMTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against SMTP server banners. • Banner information - Type the new information into the box that will replace the original server banner information.
Protocol Anomaly Detection	Click **Enable** to analyze the SMTP packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click Configure to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For

Option	Description

	more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking dur-

Option	Description
	ation, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Command Line Length**: Specifies a max length (including carriage return) for the SMTP command line. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Path Length**: Specifies a max length for the reverse-path and forward-path field in the SMTP client command. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Reply Line Length**: Specifies a max length reply length for the SMTP server. If the length exceeds the limits, you can:

Option	Description
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Text Line Length**: Specifies a max length for the E-mail text of the SMTP client. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Type Length**: Specifies a max length for the content-type of the SMTP protocol. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Filename Length**: Specifies a max length for

Option	Description
	the filename of E-mail attachment. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Time**: Specifies a max failure time (within one single SMTP session) for the SMTP server. If the length exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

In the SUNRPC tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Click **Enable** to analyze the SUNRPC packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile.

Option	Description

	Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.
	• Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.

Option	Description
	• Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

In the Telnet tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Click **Enable** to analyze the Telnet packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: • Log Only - Record a log;

Option	Description

	• Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Username/Password Max Length: Specifies a max length for the username and password used in Telnet. If the length

Option	Description
	exceeds the limits, you can: • Packet Capture Forensic: Click the **Enable** button to enable the packet capture forensic function. For more information about packet capture forensic function, see Packet Capture Forensic. • Action: Log Only; Reset; Block IP; Block Service.

10. Click **Save** to complete the protocol configurations.
11. Click **OK** to complete the IPS rule configurations.

Notes: For devices without Disk and A1600/A1800/A2200 devices with Disk, you need to enable the packet capture function by enabling the **Join the User Experience Program** and enabling the threat log reporting to CloudView. Only then will the packet capture function take effect. In this case, the firewall device will not be able to view the packet capture data, and the system will send the packet capture data and threat log information to CloudView Security operations personnel can analyze and evaluate the threat log information based on the packet capture evidence.

For more information, refer to the **Threat Prevention** > **IPS**> **Configuring IPS** section in *StoneOS WebUI User Guide*. FR 39423

CLI

Configuring the Sensitivity Level for SQL Injection Checks

After the system enables the SQL injection check function, you can configure the sensitivity level of the SQL injection check. The sensitivity determines the strictness of the SQL injection check. Different levels affect the detection rate of injection attacks and the false positive rate. The system's

default sensitivity level is "Medium". Specifically as follows:

- When the sensitivity is set to "High", the system has a higher detection rate for injection attacks, but it may also increase the false positive rate;
- When the sensitivity is set to "Low", the system's injection attack detection rate will decrease, but the false positive rate will also be relatively lower;
- When the sensitivity is set to "Medium", the system's injection attack detection rate and false positive rate reach a relatively balanced state. It can effectively detect injection attacks while avoiding too many false positives, meeting the needs of most usage scenarios. Therefore, you need to set the sensitivity to "Medium".

Configure the sensitivity level for SQL injection checks. In Web server configuration mode, use the following commands:

sql-injection-check enable sensitive {**high** | **low** | **medium**}

- **high** - Set the sensitivity level for SQL injection checks to "high". When the sensitivity is set to "high", the system detects more injection attacks, but it may also increase the false positive rate.
- **low** - Specifies the sensitivity level for SQL injection checks as "low". When the sensitivity is set to "low", the system's detection rate for injection attacks decreases, but the false positive rate also decreases.
- **medium** - Set the sensitivity level for SQL injection checks to "medium". When the sensitivity is set to "medium", the system achieves a relatively balanced state in detecting injection attacks and minimizing false positives. It can effectively detect injection attacks while avoiding excessive false alarms, meeting the needs of most usage scenarios. Therefore, you are recommended to set the sensitivity to "medium". This level is also the system's default sensitivity setting.

Enable/Disable the SQL Injection Checkpoint

SQL injection checkpoints are enabled by default. You need to disable or re-enable specified SQL injection checkpoints as needed.

Disable the SQL injection checkpoint in Web server configuration mode by using the following command:

sql-injection {**cookie** | **post** | **referer** | **uri**| **additional-headers**} **disable**

- {**cookie** | **post** | **referer** | **uri**| **additional-headers**} **disable** - disable the specified SQL injection checkpoints, which can be HTTP Cookie, HTTP Post, HTTP Referer, HTTP URI or other HTTP checkpoints.

Use the command in the following form to enable the checkpoint: **no sql-injection** {**cookie** | **post** | **referer** | **uri** | **additional-headers**} **disable**

Configuring the Sensitivity Level for XSS Injection Checks

After the system enables the XSS injection check function, it supports configuring the sensitivity level of the XSS injection check. The sensitivity determines the strictness of the XSS injection check. Different levels affect the detection rate of injection attacks and the false positive rate. The system's default sensitivity level is "Medium". Specifically as follows:

Different sensitivity levels correspond to different detection rates for injection attacks and false positive rates:

- When the sensitivity is set to "High", the system has a higher detection rate for injection attacks, but it may also increase the false positive rate;
- When the sensitivity is set to "Low", the system's injection attack detection rate will decrease, but the false positive rate will also be relatively lower;
- When the sensitivity is set to "Medium", the system's injection attack detection rate and false positive rate reach a relatively balanced state. It can effectively detect injection attacks while

avoiding too many false positives, meeting the needs of most usage scenarios. Therefore, you need to set the sensitivity to "Medium".

Configure the sensitivity level for XSS injection checks. In Web server configuration mode, use the following commands:

xss-check enable sensitive {**high** | **low** | **medium**}

- **high** - Set the sensitivity level for XSS injection checks to "high".At this level, the system detects more injection attacks, but it may also increase the false positive rate.
- **low** - Specify the XSS injection check sensitivity level as "low". At this level, the system's detection rate for injection attacks will decrease, but the false positive rate will also be relatively lower.
- **medium** - Set the XSS injection check sensitivity level to "medium". At this level, the system achieves a relatively balanced state for detecting injection attacks and minimizing false positives. It can effectively detect injection attacks while avoiding excessive false alarms, meeting the needs of most use cases. Therefore, you are recommended to set the sensitivity level to "medium". This level is also the system's default sensitivity setting.

Enable/Disable the XSS Injection Checkpoint

XSS injection checkpoints are enabled by default. You need to disable or re-enable specified XSS injection checkpoints as needed.

Disable the XSS injection checkpoint in Web server configuration mode by using the following command:

xss-injection {**cookie** | **post** | **referer** | **uri**| **additional-headers**} **disable**

- {**cookie** | **post** | **referer** | **uri**| **additional-headers**} **disable** - disable the specified XSS injection checkpoints, which can be HTTP Cookie, HTTP Post, HTTP Referer, HTTP URI or other HTTP checkpoints.

Use the command in the following form to enable the checkpoint: **no sql-injection** {**cookie** | **post** | **referer** | **uri** | **additional-headers**} **disable**

Enable/Disable SQL Injection and XSS Injection Check Rules

In the field of network security, SQL injection and XSS injection attacks are extremely harmful and can lead to unauthorized access, alteration of database information, and theft of user session information. To ensure that the device can accurately and efficiently respond to these attacks, the system includes a series of default-enabled SQL injection and XSS injection detection rules. These rules can be combined with other configuration functions for SQL injection and XSS injection checks to further optimize detection effectiveness, improve the detection rate of injection attacks, and reduce false positives and false negatives.

> **Notes:** SQL injection and XSS injection detection rules must be used with IPS signature database version 3.0.232 or higher to ensure the rules take effect. Therefore, you need to upgrade the IPS signature database to version 3.0.232 or higher before use; otherwise, the rules that are enabled by default will also not take effect.

enable the SQL injection and XSS injection check rules, Take the following steps:

1. **Upgrade to the latest IPS signature database:** For more information about how to configure this, see "Threat Protection > Intrusion Prevention > Configure Intrusion Prevention > Signature Database Update" section.
2. **Enable the SQL Injection and XSS Injection Check Rules:** In global configuration mode, use the **ips msre-rule enable** command.

To disable the SQL injection and XSS injection check rules, in global configuration mode, use the **ips msre-rule disable** command.

For more information, refer to the **Threat Prevention** > **IPS** section in *StoneOS CLI User Guide*.
FR 39423

Optimizing the Feature Library Upgrade WebUI Page

WebUI

Updating Signature Database

The signature databases that can be installed include Encrypted traffic detection database,Share Access signature database,Application signature database, URL signature database, Antivirus signature database, antivirus intelligence file engine database, Sandbox Allowlist Database, IPS signature database, IP reputation database, SSL proxy domain allowlist signature database, Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database. Except Encrypted traffic detection database,SSL proxy domain allowlist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, you can only view other signature databases when the system is installed with the corresponding licenses. The system support the following two methods to upgrade signature databases: remote update via HTTP and HTTPS; local update via downloading update package through the default signature database update server.Except the SSL proxy domain allowlist signature database or ISP Information Database, you can only view signature databases installed with licenses.

- Upgrading the signature database will consume system resources. You need to try to avoid peak business hours for the upgrade.
- Upgrade operations for each signature database are the same. It is recommended that you choose an appropriate upgrade method based on your network environment and Take the following steps:
- Starting from R11P3 and subsequent P versions, R11F3 and subsequent F versions, and R12 and subsequent R versions, the original "Trusted Root Certificate Upgrade" function has been merged into the configuration page of the "Signature Database Upgrade" function, and the Trusted Root Certificate upgrade operation is the same as the Signature Database upgrade operation.

Online Upgrading the Signature Database

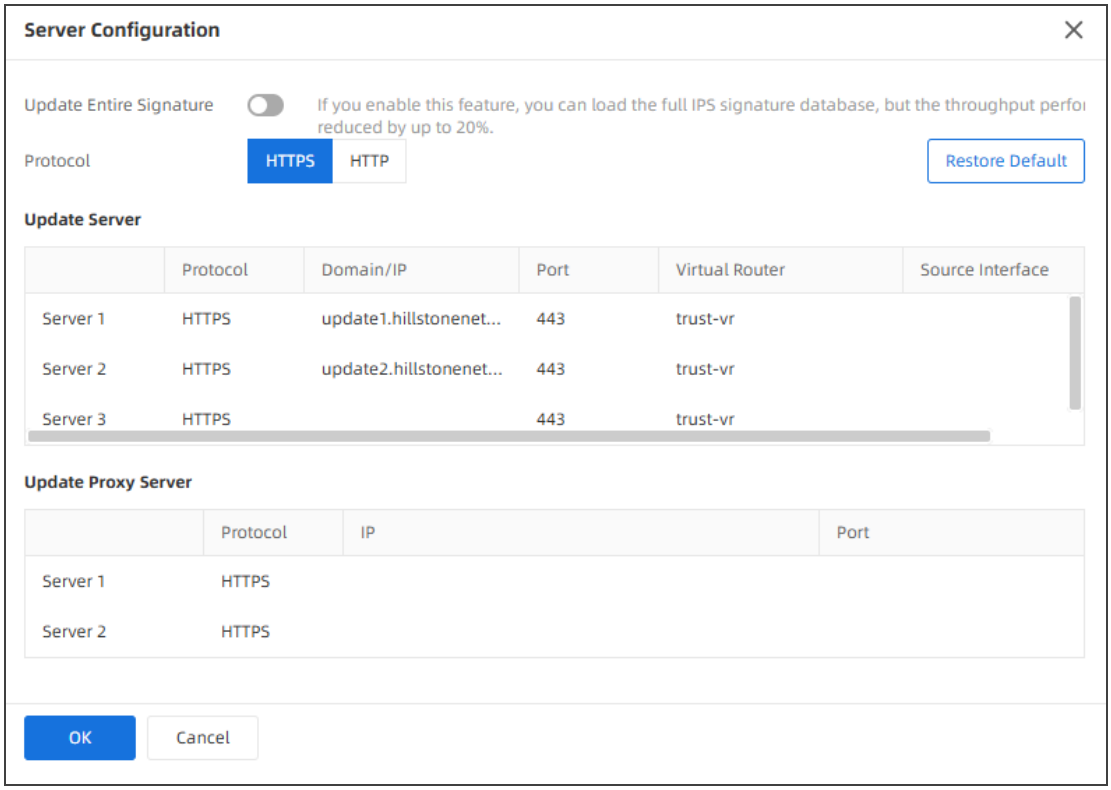
Before You Begin

- Please confirm whether the license corresponding to the signature database is still valid. Expired licenses cannot upgrade the signature database.

When the device is connected to the internet and can access the upgrade server normally, you need to use the online upgrade method to obtain the latest feature database files and perform the upgrade. Online upgrades can be achieved through automatic online upgrades and manual online upgrades.

Online upgrade the signature database, Take the following steps:

1. Click **System** > **Upgrade Management** > **Signature Database Upgrade** to enter the signature database upgrade page.
2. Configure the upgrade server. In the signature database upgrade list, click the  button in the "Operation" column to open the <Server Configuration> page. Perform the following configurations:



Option	Description
Upgrade Entire Signature	When upgrading the intrusion prevention signature database, you can choose whether to upgrade the device's current intrusion prevention signature database to the full intrusion prevention signature database. This option is disabled by default. Click to upgrade the full intrusion prevention signature database. This operation may reduce the device's throughput performance by up to 20%. It is recommended to configure this based on the actual load of the device.

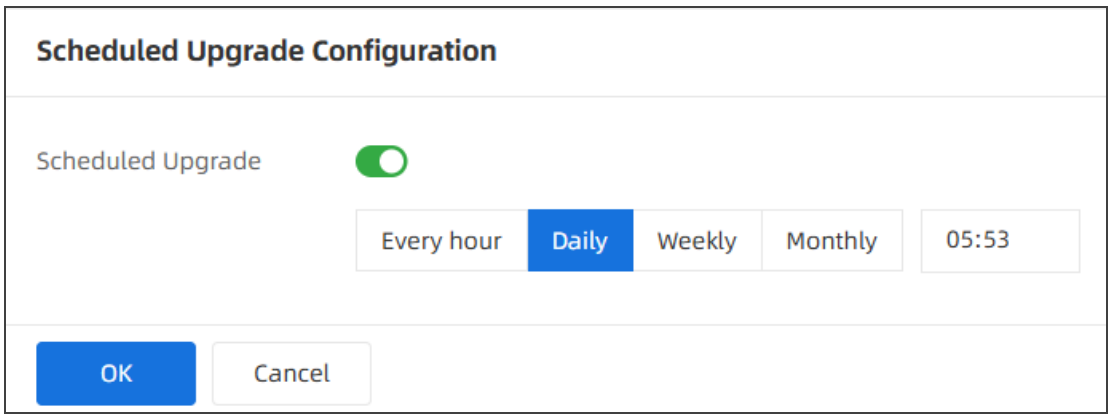
Option	Description
	Click  to cancel the upgrade of the full intrusion prevention signature database. This operation will reduce the number of current IPS signatures in the system, which may affect the details of generated threat events. **Notes:** The upgrade entire signature function is available only for : • A series some devices: SG-6000-A200/A200G4 /A200W/A200WG4/A1000/A1100 • B series some devices: SG-6000-B600/B600G4 /B600W/B600WG4/B2000
Protocol	Select the upgrade method for the signature database, including HTTP and HTTPS. Click the "Restore Default" button to restore the default HTTPS transmission method.
Upgrade Server	The device provides two default signature database upgrade servers, which are https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can also customize the upgrade server as needed: in the "Upgrade Server" module, specify the IP address or

Option	Description
	domain name of the required server, and select the virtual router and source interface from the drop-down list. The source interface must be an interface under the virtual router, and it will be used to access the update server when updating the trusted root certificate library. All upgrade servers support dual-stack protocols and can be configured with IPv4 and IPv6 addresses.
Upgrade Proxy Server	When the device needs to access the internet through an HTTP proxy server, to ensure that the signature database can be updated properly, you need to specify the IP address and port number of the proxy server on the device. In the "Upgrade Proxy Server" section, enter the IP addresses and ports of the primary and backup proxy servers. The upgrade servers support dual-stack protocols and can be configured with IPv4 and IPv6 addresses.

3. Click **OK** to complete the server upgrade configuration.
4. In the signature database upgrade list, click the button in the "Operation" column to perform the online upgrade operation.
5. (Optional) Supports batch upgrade of signature database. Check the checkboxes of the signature database to be upgraded in the list, then click **One-click Upgrade** at the top of the list to perform a batch upgrade of the signature database.
6. (Optional) Supports automatic upgrade of signature database. Click **Disabled** in the "Scheduled Upgrade" column to enable the automatic upgrade function and configure the automatic upgrade cycle. After enabling, the signature database will automatically upgrade online

according to the fixed upgrade cycle.

Notes: Only the Intrusion Prevention System signature database, IP Reputation signature database, and Botnet Prevention signature database support automatic upgrades on an hourly basis.



Local Upgrading the Signature Database

Before You Begin

- Please confirm whether the license corresponding to the signature database is still valid. Expired licenses cannot upgrade the signature database.

When the device cannot connect to the internet, you can use the local upgrade method and manually offline upgrade the system's signature database version using the locally saved signature database upgrade package.

Local upgrade of the signature database, Take the following steps:

1. Download the upgrade package to your local machine. Visit https://update1.hillstonenet.com or https://update2.hillstonenet.com, and download the upgrade package corresponding to the signature database you want to upgrade to your local machine.
2. Click **System** > **Upgrade Management** > **Signature Database Upgrade** to enter the signature database upgrade page.

3. In the signature database upgrade list, click the button in the "Operation" column to open the< Local Upgrade Configuration> page.

4. In the "Location" field, click **Browse**and select the local signature database file, then click **Upload** and the system starts uploading the signature database information.

Notes:

- Before StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Botnet C&C Detection Package" link of the default update server. From StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Encrypt Botnet C&C Detection Package" link of the default update server.
- If a large number of devices (with the same version and model) need local update, contact Hillstone's support team to acquire bulk update solutions.

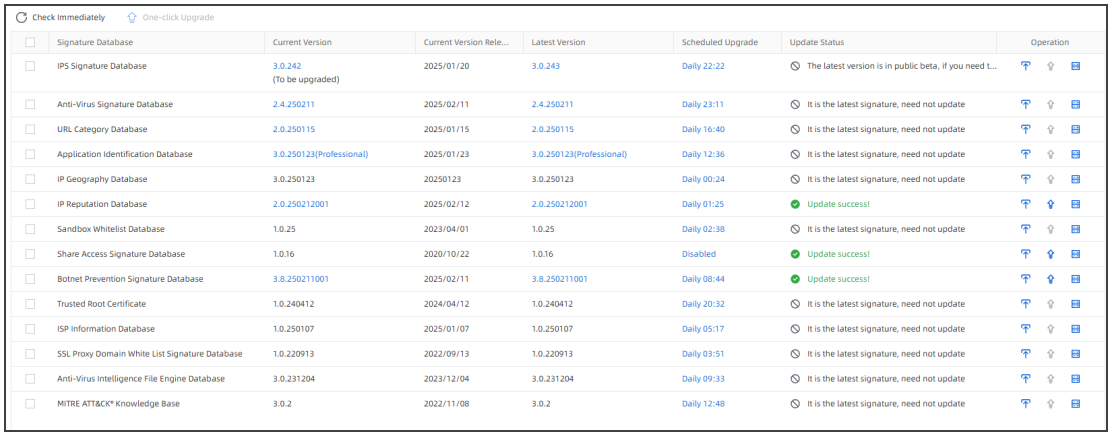
Feature Library Upgrade Status Explanation

Detailed explanations of different upgrade statuses of the signature database are as follows:

- Update Running: This indicates that the signature database is being upgraded.
- Update success: This indicates that the signature database upgrade was successful.
- It is the latest signature, need not update: This indicates that the signature database has been upgraded to the latest version, and no additional upgrade is required. At this time, the button in the "Operation" column of the feature library upgrade list is grayed out.
- Not update yet from system up: This indicates that the signature database has not been upgraded since the system started. You can upgrade the signature database online or locally based on your needs.

- Upgrade failed: Download signature failed; please confirm the servers are reachable: This indicates that the device cannot access the update server. You need to check if the network is working properly and if there are any errors in the update server configuration.
- The latest version is in public beta, if you need to upgrade urgently, please try offline import: This indicates that the latest version is temporarily unavailable through online upgrades. If you need to upgrade, use the local upgrade method. For more information, see Local Upgrade Signature Database.

Viewing the Signature Database Upgrade List



You can perform the following operations in the feature library upgrade list:

- Check the upgrade status: Click **Check Immediately** to check the latest upgrade status of the signature database.
- Bulk upgrade: Check the checkboxes of the feature libraries to be upgraded, click **One-click Upgrade**, to bulk upgrade multiple signature database.
- Check the current version or latest version release notes of thesignature database: Click the link in the "Current Version" or "Latest Version" column to view the release notes for the current or latest version of the signature database.

- Automatic upgrade of signature database: Click the link in the "Scheduled Upgrade" column to modify the automatic upgrade schedule, or enable/disable the automatic upgrade function.
- Check the upgrade status: For more information about the signature database upgrade status, see Signature Database Upgrade Status Description.
- Local upgrade of the signature database: Click the  button in the "Operation" column to locally upgrade the signature database. For more information, see Local Upgrade of the Signature Database.
- Online upgrade of the feature library: Click the  button in the "Operation" column to upgrade the feature library online. For more information, see Online Upgrade of the Signature Database.
- Server configuration: Click the button in the "Operation" column of the specified feature library  to open the <Server Configuration> page, configure or modify the information related to the upgrade server and the upgrade proxy server. For more information about how to do this, see Online Upgrade Signature Database.

For more information, refer to the **System Management** section in *StoneOS CLI User Guide*. FR 37251, FR 41237, FR 41235

New Usage Restrictions Added for Optical Interface Configuration Commands

CLI

Configuring the Negotiation Mode of Fiber-optic Interface

Notes:

- This function cannot be configured on the HA interface of the device.
- For X8180 and K9180, before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

Fiber-optic interfaces have the following two negotiation modes:

- Auto-negotiation mode: This is the default negotiation mode. In this mode, an interface operates in auto-duplex mode at 1000Mb/s. After auto negotiation is completed, interfaces at both ends operate in full-duplex mode at 1000Mb/s.
- Forced mode: In this mode, an interface operates in full-duplex mode at 1000Mb/s.

To ensure that interfaces at both ends can complete link negotiation, you need to make the negotiation mode configuration of interfaces at both ends consistent. Negotiation mode configuration involves the following scenarios:

- Interfaces at both ends are in auto-negotiation or forced mode: No configuration is required.
- The peer interface is in forced mode and the local interface is in auto-negotiation mode: In interface configuration mode, use the **sfp-to-copper force** command to set the negotiation mode of the local fiber-optic interface to forced. The negotiation will not succeed until the negotiation mode of interfaces at both ends are consistent.

- The peer interface is in auto-negotiation mode and the local interface is in forced mode: In interface configuration mode, use the **no sfp-to-copper force** command to set the negotiation mode of the local fiber-optic interface to auto-negotiation. The negotiation will not succeed until the negotiation mode of interfaces at both ends are consistent.

Enabling/Disabling the Transceiver Module

Notes:

- This function cannot be configured on the HA interface of the device.
- For X8180 and K9180, before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

After you insert the transceiver module into the device, the module is enabled by default. To avoid that certain devices can complete link negotiation due to the transceiver module even if no network cable is used to connect both ends or a network cable is used to connect both ends but the rates at both ends are inconsistent, you are allowed to manually disable this module.

In interface configuration mode, use the **sfp-to-copper shutdown** command to disable the transceiver module.

To enable the transceiver module again, in interface configuration mode, use the **no sfp-to-copper shutdown** command.

Manually Configuring the Fiber-optic Interface to Negotiate with Peer Port

Device Supported: : Supported model

- X series: X8180。

Notes:

- This function cannot be configured on the HA interface of the device.
- Before you use the function, use the **show module** command to confirm that the SIOM module is present and in the online state.

After you insert a transceiver module into the device, the fiber-optic interface of the device works in auto-negotiation mode by default. In this case, the device can only interoperate with the 1 GE port at the peer end. To ensure that the fiber-optic interface can negotiate with the peer 100M/10M port, you need to manually configure the fiber-optic interface.

To configure the negotiation mode of the fiber-optic interface to negotiate with the peer port, take the following steps:

1. In interface configuration mode, use the **channel-speed 1000** command to switch to the 1G working mode.
2. Use the **sfp-to-copper tri_speed** command to configure the fiber-optic interface to negotiate with the peer port.

In interface configuration mode, use the **no sfp-to-copper tri_speed** command to restore to the default configuration.

For more information, refer to the **System Management** section in *StoneOS CLI User Guide*.
FR42571, FR42509

Supporting for detecting IPv6 type packets

WebUI

Packet Path Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

Based on the packet process flow, the packet path detection function detects the packets and shows the detection processes and results to the users with charts an descriptions. This function can detect the following packet sources: emulation packet, online packet, and imported packet (system provides the Packet Capture Tool for you that can help you capture the packets).

The detectable packets from different packet sources have different detection measures. System supports the following measures:

- Emulation packet detection: Emulate a packet and detect the process flow in the system of this packet.
- Online packet detection: Perform a real-time detection of the process flow of the packets in system.
- Imported packet detection: Import the existing packets and detect the process flow in system of the packets.

Configuring Packet Path Detection

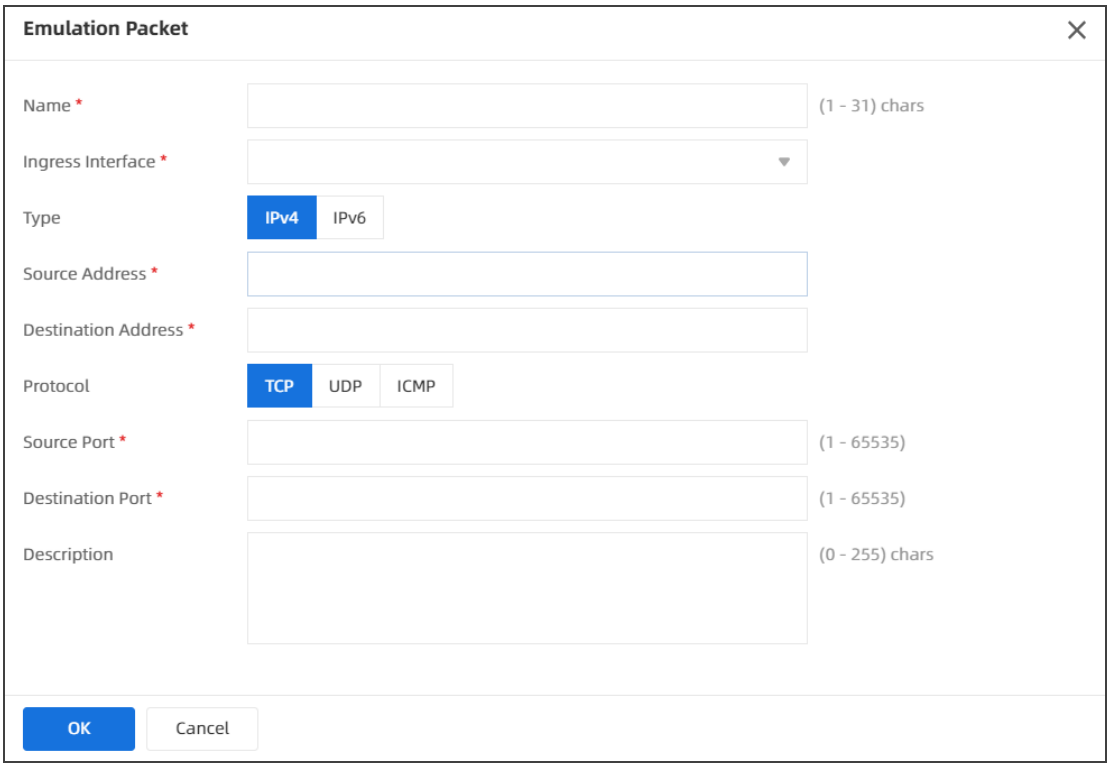
You can configure the packet path detection configurations and view the detection results in the report.

Emulation Detection

To perform the emulation detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.
2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Emulation Packet** tab.



Option	Description
Name	Specifies the name of the emulation packet.
Ingress Interface	Select the ingress interface of the emulation packet from the drop-down list.
Type	Specifies the IP address type for the detection source, which can be IPv4 or IPv6. This option is configurable only when IPv6 is supported. After selection, the system supports detection of IPv6 packets.
Source Address	Specifies the source IP address and the destination IP address based on the selected IP address type.
Destination Address	
Protocol	Select the protocol type for the detection source from the drop-

Option	Description
	down list based on the selected IP address type. • When the "Type" is specified as IPv4, you can select TCP, UDP, or ICMP protocols. • When the "Type" is specified as IPv6, you can select TCP, UDP, or ICMPv6 protocols. If you select TCP or UDP protocols, you need to enter the source port number and destination port number in the "Source Port" and "Destination Port" text boxes respectively; if you select ICMP/ICMPv6 protocols, you need to enter the ICMP/ICMPv6 type and code in the "Type" and "Code" text boxes respectively.
Description	Specifies the description for this emulation packet.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. Click **Start** to start the detection. The system displays the detection flow in the flow chart and describes the detection process. The flow chart contains all modules the packets passes in the system. After the detection for a particular module is completed, the status indicator above the module indicates the detection results.

   - Green indicator() - Indicates the detection for this module has been passed. System will proceed with the detection. Hover your mouse over this step to view its introduction.

- Yellow indicator() - Indicates the detection for this module has been passed, but there are potential security risks. System will proceed with the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report.

- Red indicator() - Indicates the detection for this module fails to pass. System has stopped the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report. If the failure is caused by the policy rule configurations, you can click the link in the Policy Rule step to jump to the policy rule configuration page.

6. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the detailed detection report. The meanings of status indicators are as follows:

   - Green indicator() - Indicates the detected source has passed all detection.

   - Yellow indicator() - Indicates the detected source has passed all detection, but there are potential security risks in one or more steps. You can click the **View Details** link to view the potential risks and advice.

   - Red indicator() - Indicates not all detection is passed by the detected source. You can click the **View Details** link to view the failure reasons and advice.

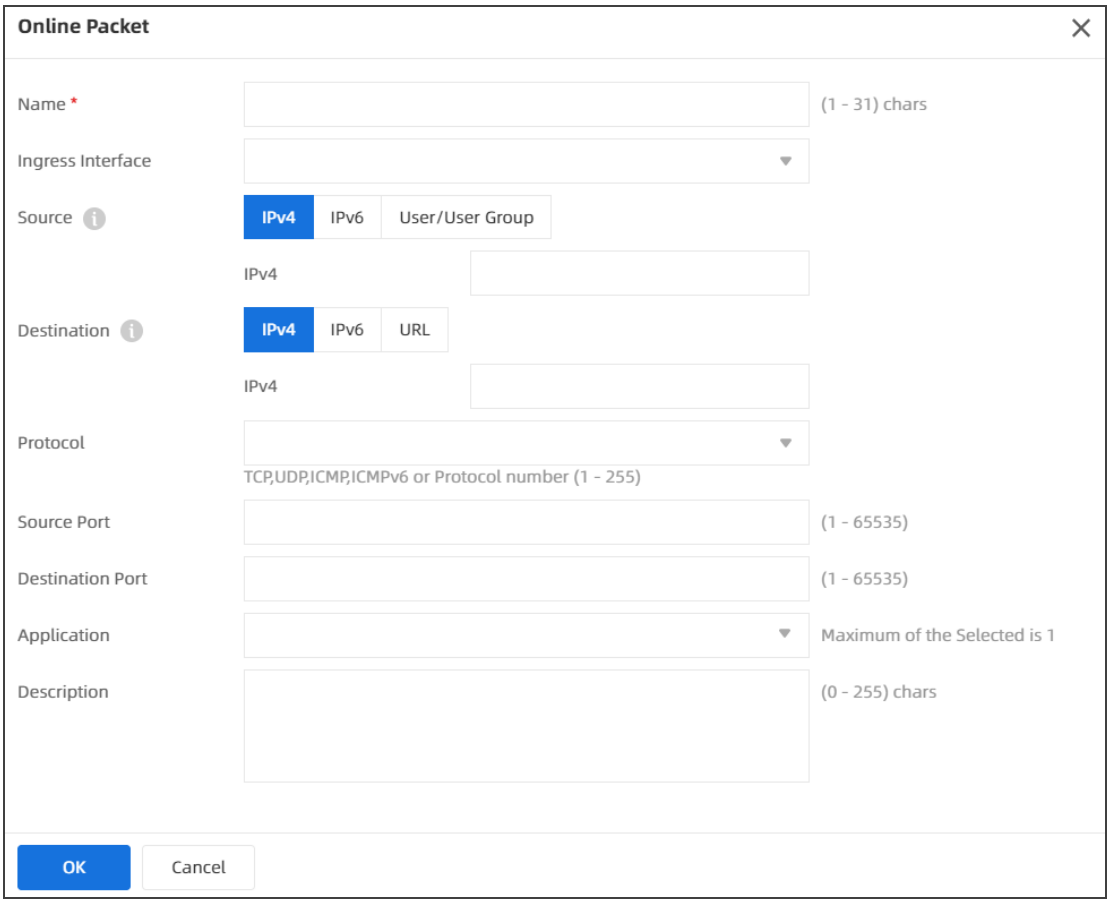
Online Detection

To perform the online detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.

2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Online Packet** tab.



Option	Description
Name	Specifies the name of the online packet.
Ingress Interface	Select the ingress interface of the online packet from the drop-down list.
Source	Specifies the source IP address or the user/user group of the online packet.

Option	Description
	• IPv4: Select the IPv4 radio button and enter the IPv4 address in the text box. • IPv6: Select the IPv6 radio button and enter the IPv6 address in the text box. • User/User Group: Select the User/User Group radio button and select the user/user group from the drop-down list. **Notes:** The source IP address type and destination IP address type of the detection source need to be consistent.
Destination	Specifies the destination IP address of the online packet. • IPv4: Select the IPv4 radio button and enter the IPv4 address in the text box. • IPv6: Select the IPv6 radio button and enter the IPv6 address in the text box. • URL: Select the radio button and enter the URL in the text box.
Protocol	Specifies the protocol type or the protocol number of the packet. When specifying the ICMP or ICMPv6 protocol, if the source/destination IP address of the detection source is IPv4, it is recommended to specify the ICMP protocol; if it is IPv6, specify the ICMPv6 protocol.

Option	Description
Source Port	Specifies the source port of the online packet.
Destination Port	Specifies the destination port of the online packet.
Application	Specifies the application type of the online packet.
Description	Enter the description of the online packet in the text box.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. If needed, specify the detecting duration in the Detecting Duration section; Or select **Capture Packets** check box to enable the capture packets function.

6. Click **Start** to start the detection. The system displays the detection process. If errors occurr during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to view the details. During each detection process, the system can pop up at most six thumbnails.

7. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the detailed detection report. About the meanings of status indicators, view step 3 in Emulation Detection.

Notes:

- If one of the following situations happens during the detection, the system will stop the detection.

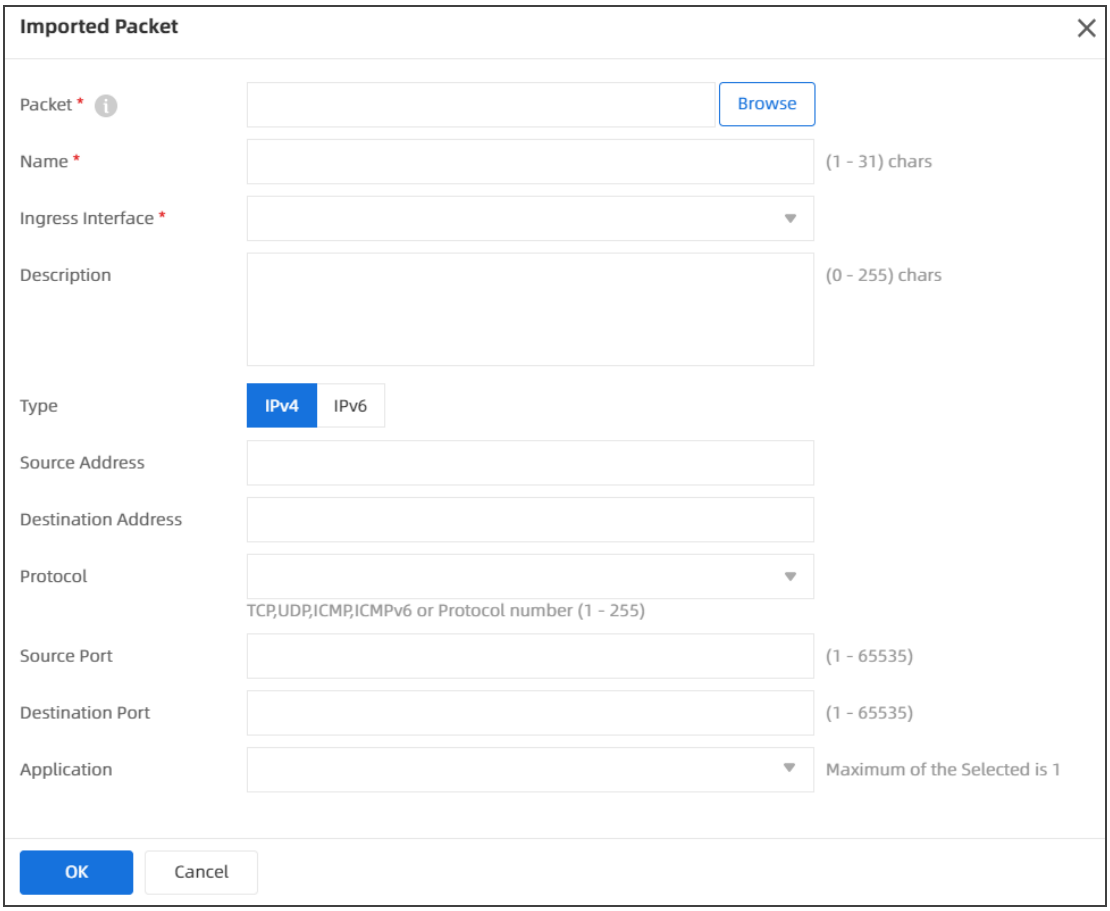
- Click the **Stop** button.
- Reach the upper limit of the detecting duration. If you do not set the detecting duration, the detecting duration keeps the default value (30 minutes).
- The total number of errors of the same type reaches 10. For example, the flow is blocked by the same policy.
- The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
- After selecting the **Capture Packets** option, the size of the captured packet file reaches 10M during the detection.

Imported Detection

To perform the imported detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.
2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Imported Packet** tab.



Option	Description
Packet	Click the **Browse** button and select the packet file to import it. The maximum size of the imported packet file can be 20M. The format of packet can be .pcap or .pcapng.
Name	Specifies the name of the imported packet.
Ingress Inter-face	Select the ingress interface of the imported packet from the drop-down list.
Description	Enter the description of the online packet in the text box.
Type	Specifies the IP address type for the detection source, which can

Option	Description
	be IPv4 or IPv6. This option is configurable only when IPv6 is supported. After selection, the system supports detection of IPv6 packets.
Source Address	Specifies the source IP address and the destination IP address of the imported packet based on the selected IP address type.
Destination Address	
Protocol	Specifies the protocol type or the protocol number of the imported packet. When specifying the ICMP or ICMPv6 protocol, if the source/destination IP address of the detection source is IPv4, you need to specify the ICMP protocol; if it is IPv6, specify the ICMPv6 protocol.
Source Port	Specifies the source port of the imported packet.
Destination Port	Specifies the destination port of the imported packet.
Application	Specifies the application type of the imported packet.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. Click **Start** to start the detection. The system displays the detection process in the Detection Process tab. If errors occurr during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to view the details. During each detection process, the system can pop up at most six thumbnails.

6. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicators and detection result summary. You can click the **View Details** link to view the detailed detection report. For the meanings of the status indicators, view step 3 in Emulation Detection.

Notes: If one of following situations happens during the detection, the system will stop the detection.

- Click the **Stop** button.
- The total number of errors of the same type reaches 10. For example the flow is blocked by the same policy.
- The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
- The imported packets have been all detected.

Detected Sources

Click **Choose Detected Source** to display all existing detection sources in the system, including the emulation packet, online packet, and imported packet, on the **Choose Source** page. You can then perform the following actions:

- Click **Details** in the Result column to view the detection report of the detected source. On the report page, you can click **Download Packet** to export the detection packet to a local PC.
- Click **Export** in the Export Packet column to export the detected packet to the local PC. Click **Export** in the Export Packet column to display the **Export** page. Select a specified slot to export the detection packets to the local PC.

- Click **Edit** in the Option column to edit the configurations of the detected source.
- Click **Delete** in the Option column to delete the detected source.

For more information, refer to the **Diagnosis Center** > **Packet Path Detection** section in *StoneOS WebUI User Guide*. FR 45842

CLI

Emulation Packet

troubleshooting packet-trace emulation-template

Configure emulation detection.

Command:

troubleshooting packet-trace emulation-template*name***type** {**tcp** | **udp**} {**src-ip***ip-address* | **src-ipv6***ipv6-address*} **src-port***port-num* {**dst-ip***ip-address* | **dst-ipv6***ipv6-address*} **dst-port***port-num***ingress-interface***interface-name* [**description***description*]

troubleshooting packet-trace emulation-template*name***type** {**icmp src-ip***ip-address***dst-ip***ip-address* | **icmpv6 src-ipv6***ipv6-address***dst-ipv6***ipv6-address*} **type***type-value***code***code-value***ingress-interface***interface-name* [**description***description*]

no troubleshooting packet-trace emulation-template*name*

Description:

emulation-template *name* -Specifies the name of the emulation packet.

type {**tcp** | **udp**} /**type** {**icmp** | **icmpv6**} - Specifies the protocol type of the emulation packet.

src-ip*ip-address* - Specifies the source IPv4 address of the emulation packet.

src-ipv6*ipv6-address* - Specifies the source IPv6 address of the emulation packet.

dst-ip*ip-address* - Specifies the destination IPv4 address of the emulation packet.

dst-ipv6*ipv6-address* - Specifies the destination IPv6 address of the emulation packet.

src-port *port-num* - Specifies the source port of the emulation packet, only when the protocol type is specified as TCP/UDP.

dst-port*port-num* -Specifies the destination port of the emulation packet, only when the protocol type is specified as TCP/UDP.

type*type-value* **code***code-value* -Specifies the ICMP/ICMPv6 type value and code value only when the protocol type is specified as ICMP/ICMPv6.

ingress-interface*interface-name* -Specifies the ingress interface of the emulation packet.

description*description* -Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 20 emulation packets.

The source IP address type and destination IP address type of the detection source need to be consistent.

Example:

hostname(config)# **troubleshooting packet-trace emulation-template temp1 type udp src-ip 10.0.0.1 src-port 10 dst-ip 192.168.0.1 dst-port 100 ingress-interface ethernet0/0**

Online Packet

troubleshooting packet-trace filter

Configure online detection.

Command:

troubleshooting packet-trace filter*name***type live-traffic** {[[**src-ip***ip-address*] | [**src-ipv6***ipv6-address*] | [**user***aaa-server user-name*] | [**user-group***aaa-server user-name*]] [**src-port***port-num*] [[**dst-ip***ip-address*] | [**dst-ipv6***ipv6-address*] | [**url***url*]] [**dst-port***port-num*]

[**proto** {**tcp** | **udp** | **icmp** | **icmpv6** | *proto-num*}] [**application***app-name*] [**ingress-interface***interface-name*]} [**description***description*]

no troubleshooting packet-trace filter*name*

Description:

filter *name* - Specifies the name of the online packet.

[**src-ip***ip-address*] | [**src-ipv6***ipv6-address*] - Specifies the source IPv4 or IPv6 address of the online packet.

user*aaa-server user-name* - Specifies the user of the online packet.

user-group*aaa-server user-name* - Specifies user group of the online packet.

src-port *port-num* - Specifies the source port of the online packet.

[**dst-ip***ip-address*] | [**dst-ipv6***ipv6-address*]- Specifies the destination IPv4 or IPv6 address of the online packet.

url*url* - Specifies the URL of the online packet.

dst-port*port-num* - Specifies the destination port of the online packet.

proto {**tcp** | **udp** | **icmp** | **icmpv6** | *proto-num*} - Specifies the protocol type or the protocol number of the packet. When specifying the ICMP or ICMPv6 protocol, if the source/destination IP address of the detection source is IPv4, you need to specify the ICMP protocol; if it is IPv6, specify the ICMPv6 protocol.

application*app-name* - Specifies the application type of the online packet.

ingress-interface*interface-name* - Specifies the ingress interface of the online packet.

description*description* - Specifies the description.

Default values:

None

Mode:

Global configuration mode

Guidance:

The system allows you to create at most 5 packets capture entries.

The source IP address type and destination IP address type of the detection source need to be consistent.

Example:

hostname(config)# **troubleshooting packet-trace filter test type live-traffic dst-ip 10.1.1.1 application http ingress-interface ethernet0/0**

Imported Packet

import troubleshooting packet-trace

Import a file for packet path detection.

Command:

import troubleshooting packet-trace replay-file from {{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] | **tftp server***ip-address*} [**vrouter***vr-name*] *file-name*

Description:

{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password*] - Import the specified file from FTP/FTPS/SFTP server.

- *ip-address* - Specifies the FTP IP address.
- **user***user-name***password***password* – Specifies the username and password for the FTP/FTPS/SFTP user. If not specified, system will use anonymous to login.

tftp server*ip-address* -Import the specified file from TFTP server.

vrouter*vr-name* -Specifies the VR name.

file-name -Specifies the file name you imported.

Default values:

vrouter*vr-name* - trust-vr。

Mode:

Executive mode

Guidance:

None

Example:

hostname# **import troubleshooting packet-trace replay-file from ftp server 10.1.1.1 user user1 password password1 test.pcap**

For more information, refer to **Monitor** > **Diagnostic Tool** section in *StoneOS CLI User Guide*.

FR 45842

Supporting Bookmark Menu Function and Enhancing WebUI Usability

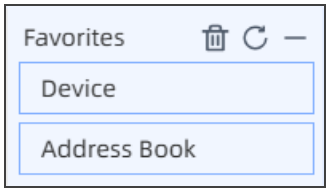
WebUI

Collecting Menu

To improve operational efficiency, the system provides a favorite menu function. You can collect frequently accessed important functions. Later, you do not need to navigate through complex firewall feature levels repeatedly; you can quickly locate and directly access the corresponding function pages via the favorite menu bar, effectively improving operation efficiency and making maintenance work smoother and more efficient.

Collecting Menu Operation Steps

1. Find the menu you want to bookmark in the left menu bar.
2. Click the  button next to the menu to add it to the favorites menu.
3. After bookmarking the menu, a movable bookmark bar will appear at the bottom right corner of the page to display the menus you have bookmarked.



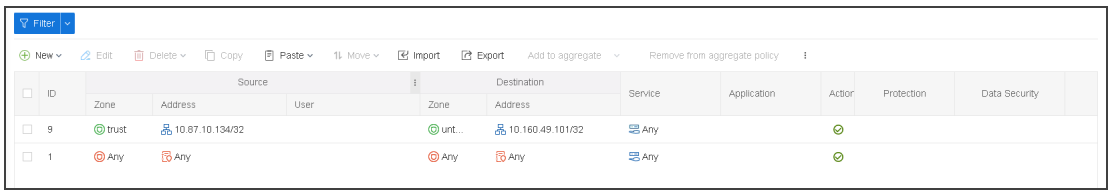
In the bookmark bar, you can take the following steps:

- Quick jump page: Click the saved menu name to quickly navigate to the corresponding page.
- Cancel favorite: Click the × button after the specified menu to unfavorite the menu.
- Remove the menu favorites bar: Click the button in the top right corner to remove the menu favorites bar. This action will also unmark all menus as favorites.
- Refresh the menu favorites bar: Click the button in the top right corner to refresh the menu favorites bar.
- Folding menu favorites bar: Click the button in the top right corner to fold the menu favorites bar into an icon. Click this icon to unfold the menu favorites bar again.

For more information, refer to **System** section in *StoneOS WebUI User Guide*.FR 39996, FR 41279, FR 41281, FR 41297

Viewing the Policy/ Policy Group/ Mini Policy

View the security policy rules in the policy rule list.



- Each column displays the corresponding configurations.
- Click icon under the Session Detail column in the Policy list to open then the **Session Detail** page. You can view the current session status of the selected policy.

    - You can also click Filter button to add filtering conditions and search out the filtered sessions.
    - The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. You can select Long Session to view the status of persistent sessions. For more information, see Session Timeout.
    - Select one or more sessions and click **Clear** to clear them. You can select at most all sessions on the current page and clear them.
- To provide you with a clearer view of the schedule and status of policies, the system displays the schedule in a separate column. The display includes an icon and the schedule name. The icons indicate different schedule statuses:  indicates active,  indicates inactive, and  indicates expired. Each policy can display up to 8 schedules. If there are more than 8 schedules, a "More" option will appear. You can click **More** to view all schedules for this policy.
- Supports editing configuration items individually: For individual configuration items, you can directly click the  button to edit without opening the entire policy rule's edit page.
- Hover over the configurations in different columns to directly display configuration details, and **Edit**, **Add Filter**, and **Jump List** buttons will appear. The displayed content varies depending on the configuration type.
    - Viewing the detailed configurations: You can view the detailed configurations directly.
    - Editing object: Click **Edit**, which allows you to directly edit the current object on the policy rule list page without needing to go to the corresponding object configuration page for editing.
    - Jump list display: Click **Jump List**, which redirects you to the list page corresponding to the current configuration item.

- Adding configuration items as filtering conditions： Click **Add Filter**, the filter condition of the configuration you are hovering over with your mouse appears on the top of the list, and then you can filter the policy according to the filter condition. For more information about how to filter policy rules, see Searching Security Policy Rules/ Policy Groups.

Adjusting Security Policy Rule Position

You can adjust the position of policy rules in two ways.

- **Method 1: Use the "Move" button in the policy rule list to adjust:**
  1. Select **Policy > Security Policy > Policy**.
  2. Select the check box of the security policy whose position will be adjusted.
  3. Click **Move**.
  4. In the drop-down list, type the rule ID or name , and click **Top**, **Bottom**, **Before ID** , **After ID** , **Before Name** ,or **After Name**. Then the rule will be moved to the top, to the bottom, before or after the specified ID or name.
- **Method 2: Directly Drag and Drop Policy Rules in the List**:
  1. Click **Policy > Security Policy > Policy**.
  2. In the security policy list, hover over the row of the security policy rule whose priority you need to adjust.
  3. When  appears, hold down the mouse and drag it to the target position in the list.

For more information, refer to **Policy** > **Security Policy** section in *StoneOS WebUI User Guide*.FR 39996, FR 41279, FR 41281, FR 41297

Adjusting Priority

Each SNAT rule has a unique ID. When the traffic flows into the device, the device will search the SNAT rules in order and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching.

You can adjust the position of SNAT rules in two ways.

- **Method 1: Use the "Move" button in the SNAT rule list to adjust:**

    1. Select **Policy > NAT > SNAT**.
    2. Select the rule you want to adjust its priority and click **Priority**.
    3. In the Priority page, move the selected rule to:
        - Top: The rule is moved to the top of all of the rules in the SNAT rule list.
        - Bottom: The rule is moved to the bottom of all of the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all of the SNAT rules.
        - Before ID: Specifies an ID number. The rule will be moved before the ID you specified.
        - After ID: Specifies an ID number. The rule will be moved after the ID you specified.
    4. Click **OK** to save the settings.

- **Method 2: Directly Drag and Drop SNAT Rules in the List**:

    1. Click **Policy > NAT > SNAT**.
    2. In the SNAT list, hover over the row of the SNAT rule whose priority you need to

adjust.

3. When  appears, hold down the mouse and drag it to the target position in the list.

For more information, refer to **Policy** > **NAT** > **Configuring SNAT** section in *StoneOS WebUI User Guide*.FR 39996, FR 41279, FR 41281, FR 41297

Adjusting Priority

Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules in order, and then implement NAT of the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching.

You can adjust the position of DNAT rules in two ways.

- **Method 1: Use the "Move" button in the DNAT rule list to adjust:**

    1. Select **Policy > NAT > DNAT**.
    2. Select the rule you want to adjust its priority and click **Priority**.
    3. In the Priority page, move the selected rule to:
        - Top: The rule is moved to the top of all of the rules in the DNAT rule list.
        - Bottom: The rule is moved to the bottom of all of the rules in the DNAT rule list. By default, system will put the newly-created DNAT rule at the bottom of all of the DNAT rules.
        - Before ID: Specifies an ID number. The rule will be moved before the ID you specified.
        - After ID: Specifies an ID number. The rule will be moved after the ID you specified.

4. Click **OK** to save the settings.

- **Method 2: Directly Drag and Drop DNAT Rules in the List**:

  1. Click **Policy > NAT > DNAT**.
  2. In the SNAT list, hover over the row of the DNAT rule whose priority you need to adjust.
  3. When  appears, hold down the mouse and drag it to the target position in the list.

For more information, refer to **Policy** > **NAT** > **Configuring DNAT** section in *StoneOS WebUI User Guide*.FR 39996, FR 41279, FR 41281, FR 41297

Supporting Configuration of Firewall Log Types Sent to HSM

WebUI

Connecting to HSM

Before you start

- Read Connecting to HSM.

To configure HSM or CloudPano parameters in the firewall, take the following steps:

1. Select **System > Extended Services > Connecting to Security Management**. Click **Edit** button.

2. Click **Enable** button of HSM Agent field to enable this feature.



3. Input HSM server's IP address in the Sever IP/Domain text box. The address cannot be 0.0.0.0 or 255.255.255.255, or mutlicast address.

4. Enter the port number of HSM server.

5. Select the VR in the Virtual Router drop-down list.

6. In the "Log Server" section, it supports specifying the log types to be sent to HSM.

7. Specify the source interface name for connecting to the HSM server in the drop-down list.

8. Click **OK**.

Specifying the Log Types Sent to HSM

You can perform basic firewall operation and maintenance management on the HSM, such as deploying security policies, monitoring the system's real-time status and traffic information, viewing log information, device properties, etc.

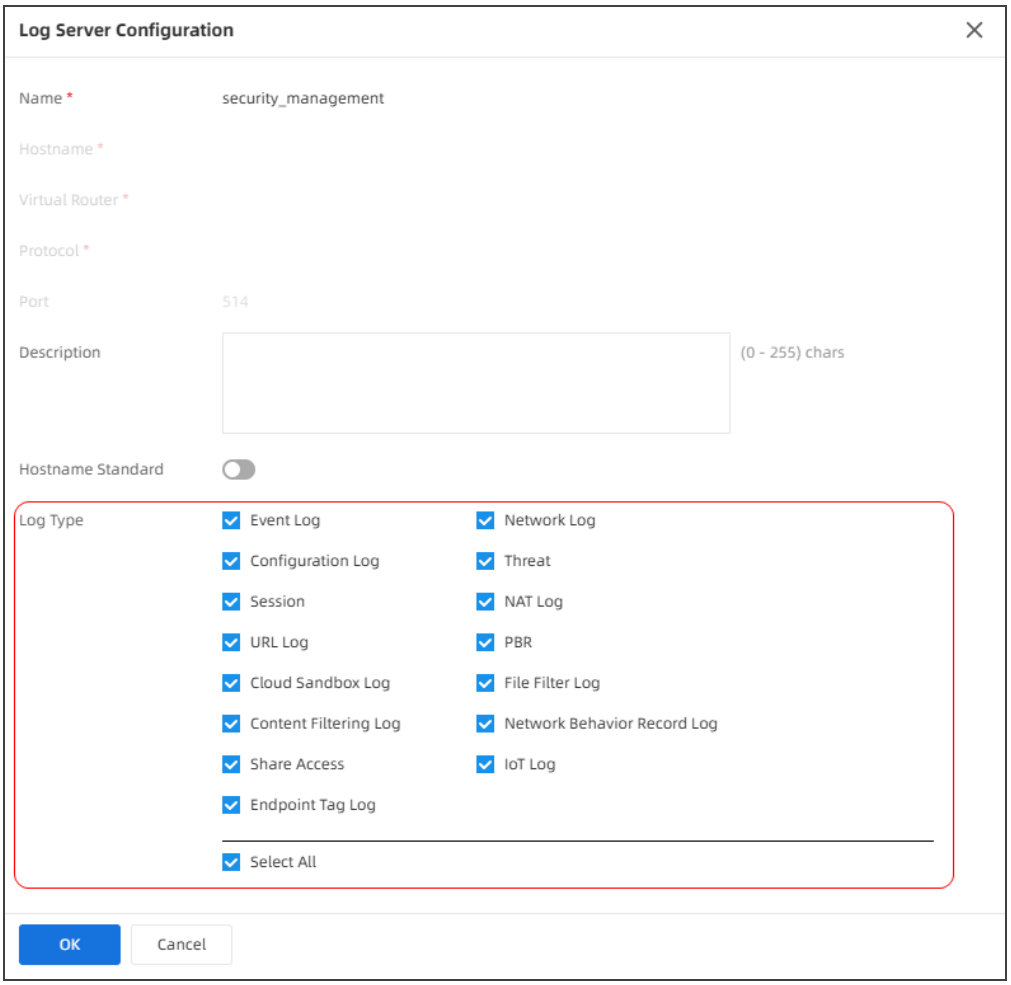
When the firewall successfully connects to the HSM, the HSM will act as a log server, receiving and storing logs generated by the firewall. The HSM supports receiving Chinese logs and binary format logs from the firewall, and by default, it stores logs for the most recent 180 days. Since the firewall is configured by default to send all types of logs to the HSM, this can lead to issues with the HSM being unable to handle large volumes of log data. To avoid this problem, the system has created a predefined empty configuration log server "security_management" for the HSM, which allows you

to specify the types of logs sent to the HSM. In this way, you can flexibly choose the log types that need to be sent to the HSM based on your actual needs, enhancing configuration flexibility and effectively improving the system's ability to handle different scenarios.

Specify the log types to be sent to the HSM. Take the following steps:

1. Select **System > Extended Services**, go to the extended services page, and in the "Connection Central Management" area, click the  button at the lower left corner to enter the connection central management configuration page.
2. Click **Edit security_management** after the "Log Server" to open the <Log Server Configuration> page. In the "Log Type" section, check the log types that need to be sent to HSM. For more information about the log server configuration items, see the "Create a New Log

Server" section.



3. Click **OK**.

For more information, refer to **System** > **Extended Services** > **Connecting to HSM** section in *StoneOS WebUI User Guide*.FR 40735

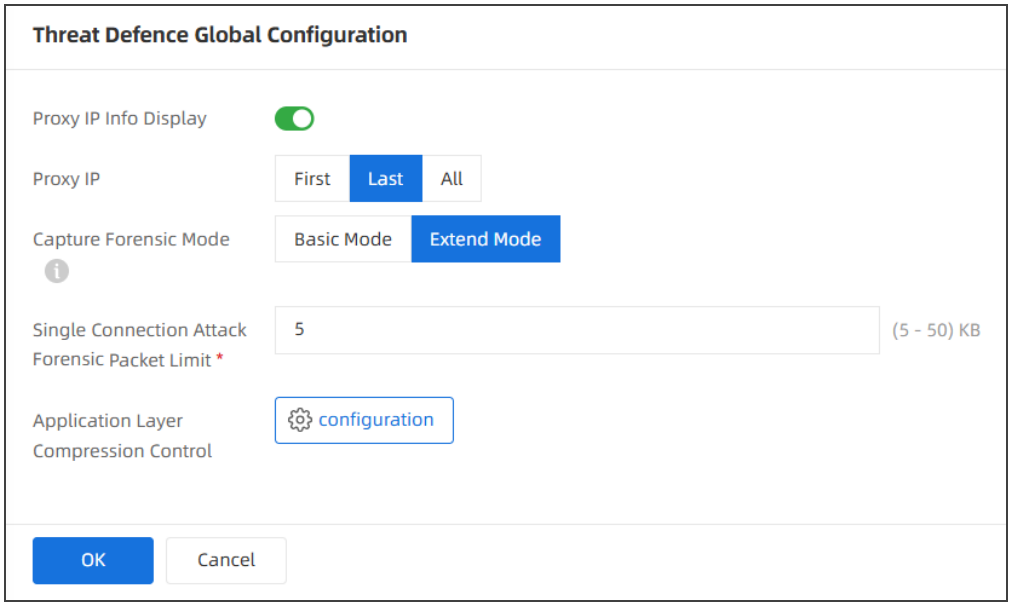
Threat Prevention Supports to record Proxy IP Information

WebUI

Configuring The Threat Protection Global Parameters

Configure the global parameters for threat protection, Take the following steps:

1. Click **Object** > **Threat Detection Template** > **Threat Defence Global Configuration**, to open the Global Threat Prevention Configuration page.



On the Threat Defence Global Configuration page, configure the parameter information.

Option	Description
Proxy IP Info Display	Click the **Enable** button to enable the proxy IP information display function. Enabling this function allows the system to record proxy IP information in HTTP traffic when a threat event is detected in an HTTP proxy deployment environment. You can view the proxy IP addresses in the threat logs and threat events. This function is enabled by default. **Note:** The proxy IP information display function operates independently and does not affect the recording of HTTP proxy IP functionality or the X-Forwarded-For configuration in CC protection.

Option	Description
Proxy IP	You can choose to record the first, last, or all IP information in the proxy IP. By default, it records all proxy IP information. **Note:** After choosing to record all proxy IP information, the system will record and display a maximum of the first 5 proxy IP addresses.
Capture Forensic Mode	Specify the packet capture mode, you can choose Basic Mode or Extended Mode, default is Basic Mode. • Basic mode: The system can capture packets when a threat is detected. For the HTTP protocol, the system will capture request and response packets. • Extended mode: The system can capture packet data before and after a threat is detected. The upper limit of captured packet data can be configured through the "Number of Packets per Connection for Forensics". For the HTTP protocol in botnet detection and intrusion detection functions, the system will capture request and response packets. Note: Packet capture forensics mode only takes effect for Intrusion Prevention System and Botnet Prevention.
Single Connection Attack Forensic	After selecting the extended mode, you need to configure the upper limit of single connection forensic message volume. Once the limit is reached, the earliest captured packet data will be discarded.

Option	Description
Packet Limit	Specify the upper limit of the amount of data captured each time, with a range of 5-50KB, defaulting to 5KB.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Application Layer Compression Control</td><td>
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Decompression</td><td>Click/Do not click the "Enable" button to enable/disable the decompression function.</td></tr>
<tr><td>Maximum Compression Layers</td><td>By default, the system can scan up to 5 layers of nested compressed files (up to 20 layers). You need to configure the number of compressions layers that can be scanned using this option. Select the desired number of layers from the drop-down list. The range is 1-20 layers.</td></tr>
<tr><td>Option</td><td>Specify the action to take for compressed files that exceed the maximum compression layer limit. You can choose:
Log Only - Generates only the relevant log information. This behavior is the system default.
Reset Connection - Reset the compressed file connection.</td></tr>
</table>
</td></tr>
</table>

2. Click OK.

For more information, refer to **Threat Prevention** section in *StoneOS WebUI User Guide*.FR 43687

CLI

Enable/Disable the Proxy IP Information Display Function

After enabling this function, in the HTTP proxy deployment environment, when the system detects a threat event, it can record the proxy IP information in the corresponding HTTP traffic. You can view the proxy IP address in the threat logs and threat events. This function is enabled by default.

Enable/disable the proxy IP information display function. In global configuration mode, use the following commands:

- Enable: **proxy-ip enable**
- Disable: **proxy-ip disable**

> **Notes:** The proxy IP information display function operates independently and does not affect the HTTP proxy IP logging function or the X-Forwarded-For configuration in CC protection.

Configuring The Proxy IP Extraction Location

You can choose to extract the first, last, or all IP information from the proxy IP details. By default, all proxy IP information is recorded.

Configure the extraction location of the proxy IP. Under global configuration, use the following command:

extract proxy-ip position {**first** | **last** | **all**}

- **first** - Extract the first proxy IP information from the proxy IP information.
- **last** - Extract the last proxy IP information from the proxy IP information.
- **all** - Extract all proxy IP information from the proxy IP information.

> **Notes:** After selecting to extract all proxy IP information, the system will record and display a maximum of the first 5 proxy IP information entries.

For more information, refer to **Threat Prevention** section in *StoneOS CLI User Guide*.FR 43687

SIOM Module Supports Power On and Off Through Command Line

CLI

Powering On or Off the SIOM Module

> **Device Supported: : Platform Supports:**
>
> - All models of X series devices
> - K series some devices: SG-6000-K20803/K9180

Power Down the SIOM Module

The device requires at least one SIOM module to operate normally. When the SIOM module has redundancy and the service is idle, you can power down the specified SIOM module using the following two methods to save energy.

- Manually remove the SIOM module: The SIOM module supports hot swapping. You can remove the SIOM module without affecting services, and the removed SIOM module will automatically power off.
- Using the command: Compared to manually removing the SIOM module, this method eliminates the complexity of manual operations and enables remote maintenance of the data center. Take the following steps:

    1. Use the **show module** command to check the status of the SIOM modules inserted into the device. SIOM modules that are allowed to be powered down must be in Booting, Loading, or Online states.
    2. In any mode, use the **power off slot** *slot-id* command to perform the power-down operation for the SIOM module. After powering down, the status of the SIOM module will be displayed as PowerDown.

Powering On the SIOM Module

If you need to re-enable the powered-down SIOM module, you can power it back on through the following two methods. After powering on, the SIOM module enters the boot process. Under normal circumstances, after some time, the status will be displayed as Online.

- Reinsert the SIOM module: Remove the powered-down SIOM module from the device slot, and then reinsert it. The SIOM module will power on automatically.
- Use the command: In any mode, use the **power on slot** *slot-id* command to power up the SIOM module that is in PowerDown state.

For more information, refer to **System Management** section in *StoneOS CLI User Guide*.FR 44842

Correcting Log Command-Line Parameters

CLI

Enabling/Disabling the Log Function

By default, the traffic logs are disabled (enabling the above logs will affect system performance). To enable or disable a system log, in the global configuration mode, use the following command:

- Enable: **logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **url-filter** | **iot-monitor**} | **debug** | **threat** | email | **data-security** [**dlp** | **cf** | **nbr**]} **on**
- Disable: **no logging** {**event** | **configuration** | **operation** | **network** | **traffic** {**session** | **nat** | **url-filter** | **iot-monitor**} | **debug** | **threat** | email | **data-security** [**dlp** | **cf** | **nbr**]} **on**

For more information, refer to **Monitor** > **Logs** > **Configuring System Logs** section in *StoneOS CLI User Guide*.Bug 485536

Supporting to Specify the Version Field of the Binary Log Packet Header

CLI

Configuring the Version Number Field of the Binary Log Packet Header

When sending logs in binary format, multiple logs will be merged into a single packet for transmission, and each packet will have a standard packet header. The packet header includes four fields: checksum, version number, number of logs included, and device basic information. Among these, the device basic information field contains the hostname of the device, which is used to identify the device sending the logs; the version number field can be either 2 or 3, which determines whether the maximum length of the extracted hostname during log parsing is 32 bytes or 64 bytes.

By default, the version number of the binary log packet header is 2. In this case, the maximum length of the hostname is 32 bytes. If the hostname of the device exceeds this length limit, it may

result in incomplete display of the hostname when parsing binary logs. To avoid this issue, the system allows you to configure the version number of the binary log packet header to adjust the length limit of the hostname. You can configure the version number to 2 or 3 as needed to accommodate hostnames of different lengths.

- When the version number is configured to 2, the maximum length of the hostname remains 32 bytes.
- When the version number is configured to 3, the maximum length of the hostname extends to 64 bytes.

To configure the version number field of the binary log packet header, use the following command in global configuration mode:

logging syslog binary-format version *version-number*

- *version-number* - Specifies the version number of the binary log packet header as 2 or 3. When the version number is set to 2, the maximum length of the hostname remains 32 bytes; when the version number is set to 3, the maximum length of the hostname extends to 64 bytes. By default, the version number is 2.

For more information, refer to the **Monitor** > **Log** > **Configuring System Logs** topic in *StoneOS CLI User Guide*. Bug 461361

Adding Model Restrictions to the Traffic Quota Function

WebUI/CLI

Traffic Quota

System supports the traffic quota function, which can limit and control the allowable flow quota of users/user groups per day or per month. When the user traffic reaches the daily or monthly quota defined by the traffic quota profile, the system will block the user traffic.

Device Supported: : Platform supports :

- A Series Some Devices: Other devices except for A7600/A6800.
- K Series Some Devices: Other devices except for K20803/K7680/K7280/K6680.

For more information, refer to the **Traffic Management** topic in *StoneOS CLI User Guide*. Bug 464248

Optimizing the Prompt Information After Successfully Importing Configuration Files Using the CLI Method

CLI

Importing Configuration Information

Configuration files can be imported into the system from the FTP server, TFTP server, SFTP server, FTPS server or USB flash disk inserted to the device USB port.

Notes: After importing the configuration information file, you need to restart for the changes to take effect.

To import configurations from an FTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from ftp server** *ip-address* **user** *user-name* **password** *password* [**vrouter** *vrouter-name*] *file-name*

- **all-vsys** – Imports configuration information of all VSYS.
- **config-filetype zip** [**zip-password** *zip-password*] - Specifies the imported file type as being ZIP. If the file is encrypted, enter the compression password.
- *ip-address* - Specifies the IP address of FTP server.

- **user***user-name***password***password* - Specifies the username and password of the FTP server.
- *vrouter-name* - Exports configuration information for the specified VRouter.
- *file-name* - Specifies a name for the configuration file.

To import configurations from a TFTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from tftp server** *ip-address* [**vrouter** *vrouter-name*] *file-name*

To import configurations from a SFTP server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from sftp server** *ip-address* [**vrouter** *vrouter-name*] [**user***user-name***password***password*] [*file-name*]

To import configurations from a FTPS server, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from sftp server** *ip-address* [**vrouter** *vrouter-name*] [**user** *user-name* **password** *password*] [*file-name*]

To import configurations from a USB flash disk, in the execution mode, use the following command:

import configuration [**all-vsys** | **config-filetype zip** [**zip-password** *zip-password*]] **from** {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

For more information, refer to the **System Management** topic in *StoneOS CLI User Guide*. Bug 481308

Configuration Restrictions When Adding a Policy Rule with a Duplicate Name

CLI

Creating a Policy Rule

To create a policy rule, in the global configuration mode or policy configuration mode, use the following command:

rule [**id***id*] [**name***name*] [**top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id*}] [**role** {**UNKNOWN** | *role-name*} | **user***aaa-server-nameuser-name* | **user-group***aaa-server-nameuser-group-name*] [**from** {**host***host-name* | **range***min-ipmax-ip* | *src-addr* }] [**to** {**host***host-name* | **range***min-ipmax-ip* | *dst-addr* }] [**from-zone***zone-name***to-zone***zone-name*] [**service***service-name*] [**application***app-name*] [**permit** | **deny** | **tunnel***tunnel-name* | **fromtunnel***tunnel-name* | **webauth** | **portal-server***server-name*]

- **id***id* - Specifies the ID of the policy rule. If not specified, the system will automatically assign an ID to the policy rule. The ID must be unique in the entire system.
- **name***name* – Specifies the name of the policy rule. The policy rule name cannot duplicate an existing policy rule name in the system.
- **top** | **before** {**name***rule-name*| *id*} | **after** {**name***rule-name*| *id* - Specifies the location of the policy rule. By default, the newly-created policy rule is located at the end of all the rules.
    - **top** Specifies the location of the policy rule to the top of all rules.
    - **before** {**name***rule-name*| *id*} – Specifies the location of the policy rule before the rule of specified ID or name.
    - **after** {**name***rule-name*| *id* – Specifies the location of the policy rule after the rule of specified ID or name.

- **role** {**UNKNOWN** | *role-name*} | **user***aaa-server-nameuser-name* | **user-group***aaa-server-nameuser-group-name* - Specifies the role/user/user group for the policy rule.
    - **role** {**UNKNOWN** | *role-name*} – Specifies the role name. **UNKNOWN** is the role reserved by the system, i.e., the role that is neither authenticated nor statically bound.
    - **user***aaa-server-nameuser-name* – Specifies the user. *aaa-server-name* is the AAA server the user belongs to, and *user-name* is the name of the user.
    - **user-group***aaa-server-nameuser-group-name* – Specifies the user group. *aaa-server-name* is the AAA server the user group belongs to, and *user-group-name* is the name of the user group.
- **from** {**host***host-name* | **range***min-ipmax-ip* | *src-addr* } – Specifies the source address of the policy rule.
    - **host***host-name* - The source address entry for the host defined in the address book.
    - **range***min-ipmax-ip* – The source address entry for the IP addresses defined in the address book.
    - *src-addr* – The address entry defined in the address book.
- **to** {**host***host-name* | **range***min-ipmax-ip* | *dst-addr* } – Specifies the destination address of the policy rule.
    - **host***host-name* – The destination address entry for the host defined in the address book.
    - **range***min-ipmax-ip* – The destination entry for the IP addresses defined in the address book.
    - *dst-addr* - The address entry defined in the address book.
- **from-zone***zone-name* – Specifies the source zone of the policy rule.

- **to-zone***zone-name* - Specifies the destination zone of the policy rule.
- **service***service-name* - Specifies the service name of the policy rule. *service-name* is the service defined in the service book.
- **application***app-name* − Specifies the application name for the policy rule. *app-name* is the application name you defined in the application book.
- **permit** | **deny** | **tunnel***tunnel-name* | **fromtunnel***tunnel-name*| **webauth** } - Specifies the action of the policy rule, including:
  - **permit** - Permits the traffic to pass through.
  - **deny** - Denies the traffic.
  - **tunnel** - For the traffic from local to a peer, this option allows the traffic to pass through the VPN tunnel.
  - **fromtunnel** - For the traffic from a peer to local, if this action is selected, StoneOS will first determine if the traffic originates from a tunnel. Only such traffic will be permitted.
  - **webauth** - Performs Web authentication on the matched traffic.

After switching to the multi-zone mode, repeat the above commands to add more source/destination zones. Each policy supports up to 16 source/destination zones. If Any zone is configured, you cannot configure other zones at the same time.

For example, to create a policy rule that permits ICMP service from any address to any address, use the following commands:

```
hostname(config)# policy-global
hostname(config-policy)# rule from any to any service icmp permit
Rule id 5 is created.
```

To delete the policy rule, in the global configuration mode or policy configuration mode, use the following command:

no rule {**id***id* | **name***name*}

- **id***id* – Deletes the policy rule of the specified ID.
- **name***name* - Deletes the policy rule of the specified name.

Tips: For information about how to configure parameters of a policy rule, see "Editing a Policy Rule".

For more information, refer to the **Policy** > **Security Policy** topic in *StoneOS CLI User Guide*. Bug 473496

The WebUI of the log server has added CUCC format.

WebUI

Creating a Syslog Server

To create a Syslog server, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**.
2. Click **Syslog Server Configuration** tab.
3. Click **New**.

Option	Description
Name	Specifies the name of the Syslog server, which needs to be 1 to 127 characters in length.
Hostname	Specifies the IP address or host name of the Syslog server.
Log Format	Specifies the log format of Syslog Server log server, including Default, SGCC S5000, SGCC S6000 and CUCC. Select the format according to the Syslog server type.

Option	Description
	• Default - Syslog Server log Server can only receive the Hillstone log format. • S5000 - Syslog Server log Server can only receive SGCC-S5000 log format, such as the log Server's of State Grid Corporation of China. • S6000 - Syslog Server log Server can only receive SGCC-6000 log format, such as the monitoring Server's of State Grid Corporation of China. • CUCC - Syslog server can only receive logs in a special format (China Unicom log format) for NAT444.
Binding	Specifies the source IP address to receive logs. • Virtual Router: Select **Virtual Router** and then select a virtual router form the drop-down list. If a virtual router is selected, the device will determine the source IP address by searching the reachable routes in the virtual router. • Source Interface: Select **Source Interface** and then select a source interface from the drop-down list. The device will use the IP address of the interface as the source IP to send logs to the syslog server. If management IP address is configured on the interface, the management IP address will be preferred.
Protocol	Specifies the protocol type of the syslog server. The Secure-TCP uses the TLS encryption protocol. If "Secure-TCP" is selected, you

Option	Description
	can select **Do not validate the server certificate** option, and system can transfer logs normally and do not need any certifications.
Port	Specifies the port number of the syslog server.
Hostname Standard	By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, i.e. **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**. With this option checked, the logs sent to the Syslog Server displays the hostname and does not display the device SN, the format is: **<Device Number*8+log severity> date/timehostname log ID HillstoneNetworks#log type@module: descriptions**.
Description	Enter a description for the syslog server as needed, which can be up to 255 characters in length.
Log Type	Specifies the log types the syslog server will receive.

4. Click **OK** to save the settings.

Notes: You can add at most 15 Syslog servers.

For more information, refer to the **Monitor** > **Logging** > **Log configuration** topic in *StoneOS CLI User Guide*. Bug 459454

Global Allowlist Additional Scope Explanation

WebUI

Configuring IP Allowlist

The system supports Global Allowlist and Perimeter Traffic Filtering Allowlist. The Global Allowlist applies to the whole firewall. For the IP addresses on the Global Allowlist, the system bypasses them without performing security checks. The Perimeter Traffic Filtering Allowlist applies to the perimeter traffic filtering function. For the IP addresses on the Perimeter Traffic Filtering Allowlist, the system does not perform perimeter traffic filtering detection. Therefore, it does not block these IPs.

Notes:

- NAT and Traffic Quota functions are not affected by the Global Allowlist.
- The scope of the global allowlist includes: Perimeter Traffic Filtering, IPS, Attack Defense, AV, Data Security, Botnet Prevention, URL filtering, content filtering, sandbox protection, spam, policy control, shared access, session limitations, endpoint protection, iQos, traffic quotas, Web authentication, DNS proxy, policy access control.
- After the NAT function is configured, the system performs perimeter traffic filtering detection before and after the NAT translation. if the IP addresses before and after NAT translation are not all added to the Global Allowlist, the traffic may be blocked by the blocklist.
- Some Attack-Defense types of X-Series devices are not affected by the Global Allowlist. These types are: Teardrop、IP Option、IP Fragment、WinNuke、Ping-of-Death、Huge ICMP Packet、UDP Flood，DNS Flood

To configure IP Allowlist, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP AllowList**.

2. Click **New**.

   Configure the corresponding options.

Option	Description
IP Type	Select the address type, including IPv4 and IPv6.
IP/Netmask	Type the IP address and netmask for the user-defined allow list.
Global Allowl-ist	After this function is enabled, the allowlist takes effect globally.
Perimeter Traffic Fil-tering Allowlist	Specify that the allowlist applys to All Zones, specified Zones or specified Virtual Routers. When "All Zones" is selected, the allowl-ist takes effect in all security zones or Virtual Routers (that is, in the perimeter traffic filtering module). When selecting "Zone" or "Virtual Router", you must select a security zone or Virtual Router from the drop-down list. Once specified, the allowlist takes effect in the specified security zone or Virtual Router.

3. Click **OK** to save the settings.

For more information, refer to the **Threat Prevention** topic in *StoneOS WebUI User Guide*. Bug 480218

Expanding the Scope of Platforms Supported by the Log Stor-age Period Function

WebUI

Configuring Logs

To configure parameters of various log types, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click the **Enable** button of the log type that you want, and click the  button to enter the corresponding log settings.
3. Click **OK**.

Option Descriptions of Various Log Types

This section describes the options when you set the properties of each log types.

Event Log

Option	Description
Enable	Click the button to enable the event logging function.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Console	Select the check box to send a syslog to the Console. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Terminal	Select the check box to send a syslog to the terminal. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to send a syslog to the cache. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Option	Description
	• Max Buffer Size - The maximum size of the cached logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send a syslog to the local database. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. Note: AEX-series firewalls installed with hard disks support this function.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export event logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add new server. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Email Address	Select the check box to send event logs to the email. • View Email Address: Click to see all existing email addresses or

Option	Description
	add a new address. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
SMS	Select the check box to send event logs to the SMS. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Network Log

Option	Description
Enable	Click the button to enable the network logging function.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Cache	Select the check box to export network logs to the cache. • Max Buffer Size - The maximum size of the cached network logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive

Option	Description
	(USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Local DB	Select the check box to send network logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.

Configuration Log

Option	Description
Enable	Click the button to enable the configuration logging function.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Cache	Select the check box to export configuration logs to the cache. • Max Buffer Size - The maximum size of the cached configuration logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send configuration logs to a file. • Max File Size - Specifies the maximum size of the configuration

Option	Description
	log file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the network log file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add new server.
Log Speed Limit	Select the check box to define the maximum efficiency of generating logs. • Maximum Speed - Specified the speed (messages per second).
Local DB	Select the check box to send configuration logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.

Session Log

Option	Description
Enable	Click the button to enable the session logging function. • Record User Name: Select to show the user's name in the session log messages. • Record Host Name: Select to show the host's name in the session log messages.
Log Storage	Specify the storage duration for logs; logs exceeding this duration

Option	Description
Time	will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Cache	Select the check box to export session logs to cache. • Max Buffer Size - The maximum size of the cached session logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Local DB	Select the check box to send session logs to the local database. Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to export session logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

PBR Log

Option	Description
Enable	Click the button to enable a PBR logging function. • Record User Name: Select to show the user's name in the PBR log messages.

Option	Description
	• Record Host Name: Select to show the host's name in the PBR log messages.
Cache	Select the check box to export PBR logs to the cache. • Max Buffer Size - The maximum size of the cached PBR logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export PBR logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of plain text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

NAT Log

Option	Description
Enable	Click the button to enable the NAT logging function. • Record Host Name: Select to show the host's name in the NAT log messages.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support con-

Option	Description
	figuring the Log Storage Time.
Cache	Select the check box to export NAT logs to cache. • Max Buffer Size - The maximum size of the cached NAT logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send NAT logs to the local database. Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to export NAT logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.
IPFIX Server	Select the checkbox to export NAT444 logs (only user allocation port logs and user release port logs) to the IPFIX server. • View IPFIX Server - Click to view all existing IPFIX servers in the system.

IoT Log

Option	Description
Enable	Click the button to enable the IoT logging function. • Record Host Name: Select to show the host's name in the IoT log messages.

Option	Description
Cache	Select the check box to export IoT logs to cache. • Max Buffer Size - The maximum size of the cached IoT logs.
Syslog Server	Select the check box to export IoT logs to the Syslog server. • View Syslog Server - Click to see all existing Syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

URL Log

Option	Description
Enable	Click the button to enable the URL logging function. • Record Host Name: Select to show the host's name in the URL log messages.
Cache	Select the check box to export URL logs to the cache. • Max Buffer Size - The maximum size of the cached URL logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export URL logs to a Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in

Option	Description
	the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

File Filter Log

Option	Description
Enable	Click the button to enable the File Filter logging function.
Cache	Select the check box to export File Filter logs to cache. • Max Buffer Size - The maximum size of the cached File Filter logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export File Filter logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

Content Filtering Log

Option	Description
Enable	Click the button to enable the Content Filter logging function.
Cache	Select the check box to export Content Filter logs to cache. • Max Buffer Size - The maximum size of the cached Content Fil-

Option	Description
	ter logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export Content Filter logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

Network Behavior Record Log

Option	Description
Enable	Click the button to enable the Network Behavior Record logging function.
Cache	Select the check box to export Network Behavior Record logs to cache. • Max Buffer Size - The maximum size of the cached Network Behavior Record logs. The default value may vary from different hardware platforms.
Syslog Server	Select the check box to export Network Behavior Record logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Option	Description
	• Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

CloudSandBox Log

Option	Description
Enable	Click the button to enable the CloudSandBox logging function.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Cache	Select the check box to export CloudSandBox logs to the cache. • Max Buffer Size - The maximum size of the cached CloudSandBox logs.
Local DB	Select the check box to send cloud sandbox logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.
File	Select to export CloudSandBox logs as a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive

Option	Description
	(USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export CloudSandBox logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Threat Log

Option	Description
Enable	Click the button to enable the threat logging function. • Record User Name: Select to show the user's name in the threat log messages.
Record User Information	Click the button to enable the Record User Information function for Threat Log. With this function enabled, threat logs will record information about the authenticated user, including AAA server, username, and hostname.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Cache	Select the check box to export threat logs to the cache. • Max buffer size - The maximum size of the cached threat logs.

Option	Description
	The default value may vary from different hardware platforms. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Local DB	Select the check box to export threat logs to local database. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. Note: AEX-series firewalls installed with hard disks support this function.
File	Select to export threat logs as a file to USB. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Exported log file maximum size. • Save logs to USB - Select a USB device and enter a name as the log file name. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Terminal	Select to send logs to terminals.
Syslog Server	Select the check box to export threat logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - the distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve

Option	Description
	the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.
Email address	Select the check box to export logs to the specified email address. • Viewing Email Address: Click to see or add email address.
Database	Select the checkbox to save logs in the local device. Only several platforms support this parameters. • Disk Space - Enter a number as the percentage of a storage the logs will take. For example, if you enter 30, the threat logs will take at most 30% of the total disk size. • Disk Space Limit - If **Auto Overwrite** is selected, the logs which exceed the disk space will overwrite the old logs automatically. If **Stop Storing** is selected, system will stop storing new logs when the logs exceed the disk space.

Share Access Log

Option	Description
Enable	Click the button to enable the Share Access logging function.
Console	Select to export Share Access logs to the console.
Cache	Select the check box to export Share Access logs to the cache. • Max buffer size - The maximum size of the cached Share Access logs.
Syslog Server	Select the check box to export Share Access logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Endpoint Tag Log

Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Log Storage Time	Specify the storage duration for logs; logs exceeding this duration will be automatically deleted. The storage duration ranges from 6 to 12 months. The default storage duration is 6 months. **Notes:** SG-6000-A1600/A1800/A2200 do not support configuring the Log Storage Time.
Console	Select to export Share Access logs to the console.
Cache	Select the check box to send endpoint tag logs to the memory buffer. • Max Buffer Size - Specify the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Local DB	Select the check box to send endpoint tag logs to the local database. Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "View Log Server" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Syslog Server.

For more information, refer to the **Monitor** > **Logging** > **Log Configuration** topic in *StoneOS WebUI User Guide*. Bug 482604

Unauthorized External Link Detection

In application scenarios such as video dedicated networks, e-government, and medical IoT, internal endpoints may face the risk of being hacked or illegally transmitting data to the Internet due to configurations like dual network cards or connections to other WIFI/hotspots. When these endpoints access the Internet, their traffic usually bypasses the firewall, preventing it from detecting such risky behaviors. To address the issues in the above application scenarios, the system provides an Unauthorized External Link Detection function. This function can detect the behavior of endpoint devices accessing the Internet without authorization and bypassing the firewall, or gateway devices accessing the Internet without authorization, achieving the effect of effectively discovering and blocking unauthorized external connections, providing a solid guarantee for network security.

This section contains the following content:

- "Gateway Unauthorized Check (WebUI)" on Page 421
- "Endpoint Unauthorized Check " on Page 425

Gateway Unauthorized Check (WebUI)

Before You Begin

- Read the "Unauthorized External Link Detection " on Page 421 introduction.
- Read the Track Object introduction.

The Gateway Unauthorized Check function is mainly used to identify whether the firewall can illegally access the Internet without authorization, helping you timely block illegal external connections from the internal network and ensure network security. This function specifies a track object, which makes the firewall automatically send network requests to specific track member (such as IPs or hosts) based on the period set in the track object, and detects whether the firewall is connected to the public network by checking if the protocol packets successfully reach the track member. It also records event logs of unauthorized external connection behaviors.

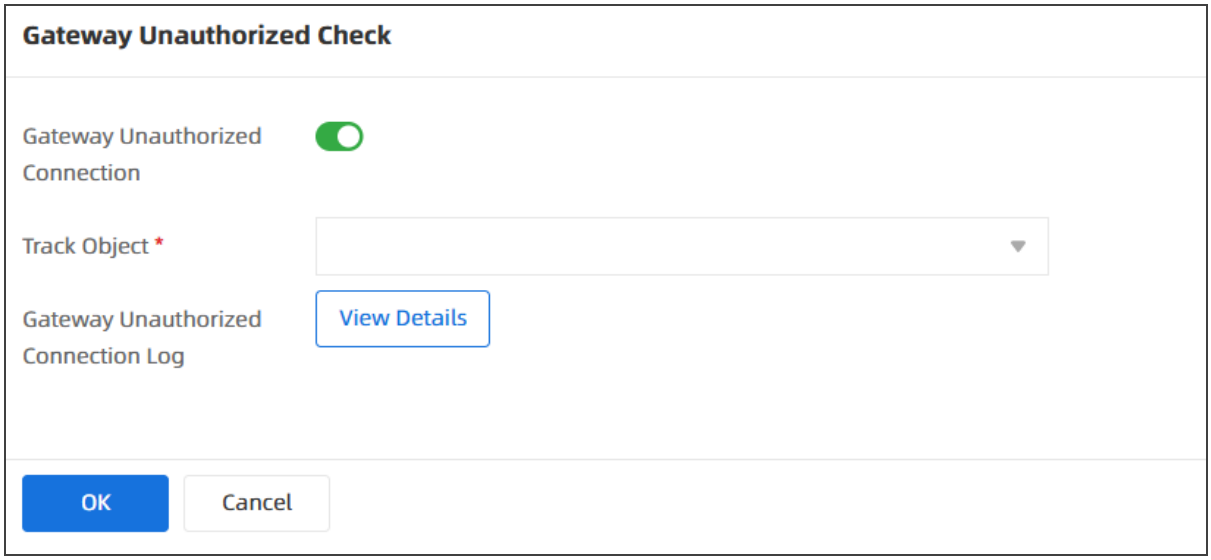
Prerequisites

Please configure the Track Object in advance, so that you can quickly select it when configuring the Gateway Unauthorized Check.

Configuring Gateway Unauthorized Check

Configure the gateway unauthorized external link detection, please Take the following steps:

1. Select **Object** > **Unauthorized External Link Detection** > **Gateway Unauthorized Check**.
2. Click the **Enable** button to enable the Gateway Unauthorized Check function. This function is disabled by default.



3. Select the specified track object in the drop-down list. If no track object has been created, you can click the ⊕ button in the drop-down list to Create a Track Object.

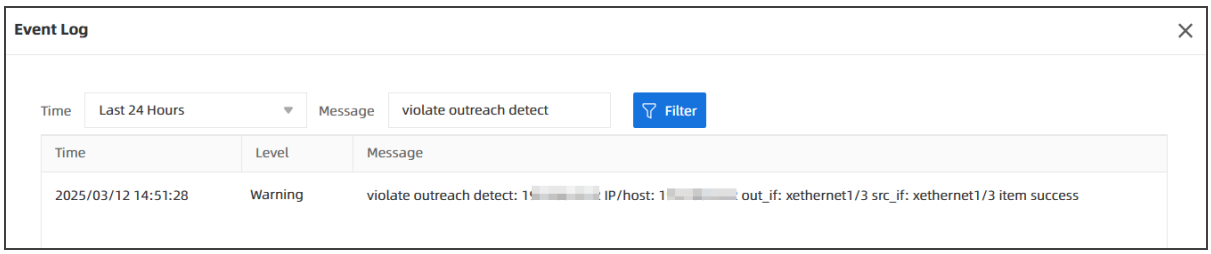
> **Tips:** Only track object of the types "HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP" protocols are supported. It is

recommended that one track member be one track object to ensure the accuracy and effectiveness of Gateway Unauthorized Check.

4. Click OK.

Viewing Gateway Unauthorized External link Logs

After completing the configuration of Unauthorized External Link Detection for the gateway, the firewall will send network requests to the specified track member (such as IPs or hosts) according to the period set in track object, and detects whether there is any unauthorized external connection behavior (i.e., whether it connects to the public network) by checking if the protocol packets successfully reach the track member. If the track member is reachable, the status of the track object will change from failure to success, and the system will determine that the gateway has an unauthorized external connection behavior and record the corresponding event logs. You can go to the **Object** > **Unauthorized External Link Detection** > **Gateway Unauthorized Check** page, click **View Details**, view the event logs of the unauthorized external connection behavior of the gateway, and adjust the corresponding protection strategy based on the log details to enhance the security of the system.



Gateway Unauthorized Check （CLI）

Before You Begin

- Read the "Unauthorized External Link Detection " on Page 421 introduction.
- Read the Configuration of track object introduction.

The Gateway Unauthorized Check function is mainly used to identify whether the firewall can illegally access the Internet without authorization, helping you timely block illegal external connections from the internal network and ensure network security. This function specifies a track object, which makes the firewall automatically send network requests to specific track member (such as IPs or hosts) based on the period set in the track object, and detects whether the firewall is connected to the public network by checking if the protocol packets successfully reach the track member. It also records event logs of unauthorized external connection behaviors.

Prerequisites

Please prepare in advance to configure track object , so that you can quickly select it when configuring the Gateway Unauthorized Check.

Entering the Unauthorized External Link Detection Configuration Mode

To enter the Unauthorized External Link Detection configuration mode, in the global configuration mode, use the following command:

violate-outreach-detect

Enabling/Disabling Gateway Unauthorized Check

By default, this function is disabled. Enable the Gateway Unauthorized Check function, and in the Unauthorized External Link Detection configuration mode, use the following commands:

gateway-detect enable track *track-name*

- *track-name* - Specifies the track object. Only supports specifying track objects of type "HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP" protocol.

Tips: It is recommended that one track member be one track object to ensure the accuracy and effectiveness of Gateway Unauthorized Check.

In the Unauthorized External Link Detection configuration mode, use the following commands to disable the Gateway Unauthorized Check function:

gateway-detect disable

Endpoint Unauthorized Check

Endpoint Unauthorized Check function is mainly used to monitor and identify unauthorized access to the Internet by internal endpoint devices (such as IoT devices) through multiple network cards or WiFi, etc. This function is crucial for key application scenarios such as video dedicated networks, e-government, and medical IoT. It not only helps prevent data leakage and resist hacker attacks but also provides important auditing and tracing tools for network security management.

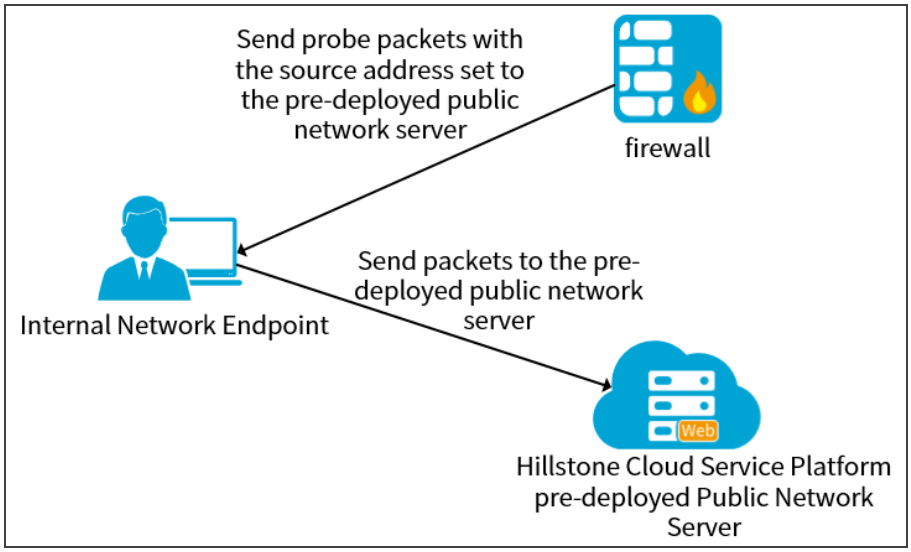
This function is implemented by deploying public network servers and an Unauthorized External Platform on the Hillstone Cloud Service Platform, working in conjunction with the firewall to effectively detect illegal external connection behaviors of internal network endpoint devices. The public network server is responsible for receiving probe data sent by the firewall-triggered endpoint, while the Unauthorized External Platform is used for registering firewall devices, activating the Endpoint Unauthorized Check function, and recording detailed information about the internal network endpoint's unauthorized external connection behavior. In most cases, when internal network endpoint devices attempt to access the Internet, these traffic flows bypass the firewall, making it impossible for the firewall to directly perform detection. By pre-deploying public network servers, the firewall can trigger internal network endpoint devices to access these servers. Once the pre-deployed public network server receives a request from an internal network endpoint device, it indicates that the endpoint has engaged in unauthorized external connection behavior, and the Unauthorized External Platform will record the detailed information of this behavior for you to investigate and handle.

Endpoint Unauthorized Check function is divided into two methods: active detection and passive detection.

- **Active Detection Mode**: The firewall will proactively send probe packets to endpoint devices with the source address of the pre-deployed public network server according to the set period. If the pre-deployed public network server receives the probe packet, it indicates that the endpoint has unauthorized external connection behavior, and the Unauthorized External Platform

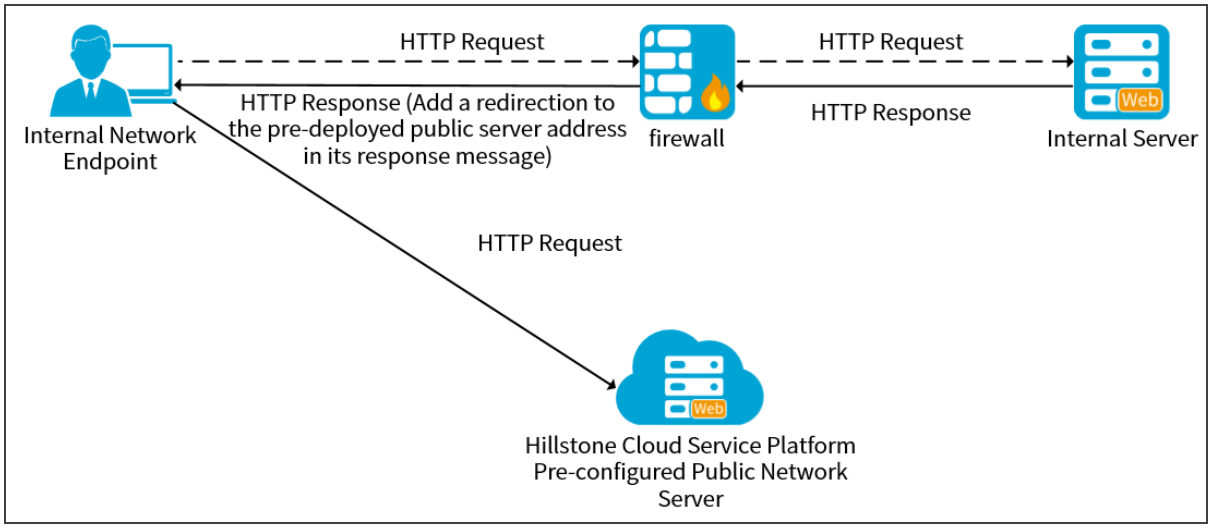
will record detailed information of this behavior.

The detection period for this mode is set to 30 minutes by default and can be configured according to your needs.



- **Passive Detection Mode**: When the firewall processes access requests from endpoint devices to internal network servers, it adds the address of a pre-deployed public network server to the response packet. After the endpoint device receives this response packet, it will redirect the access to the pre-deployed public network server. If the pre-deployed public network server receives an access request, it indicates that the endpoint has unauthorized external connection behavior, and at the same time, the Unauthorized External Platform will record detailed information about this behavior.

  In passive detection mode, an endpoint with the same IP address is only detected once within the detection period, and the default detection period is 1 hour. If you need to modify the detection period for this mode, it can only be done by executing CLI commands. For more information, use the **endpoint-detect mode passive enable period** *time-value* command to readjust the specified period.



Notes: Enabling the passive detection mode for Endpoint Unauthorized Check may impact system performance when the number of endpoints is enormous. Therefore, it is recommended to enable this function with caution.

Configuring Endpoint Unauthorized Check (WebUI)

Before You Begin

- Read the "Unauthorized External Link Detection " on Page 421 introduction.
- Read the "Endpoint Unauthorized Check " on Page 425 introduction.

Using Endpoint Unauthorized Check, you can Take the following steps:

1. Activating the Endpoint Unauthorized Check function.
2. Configure Endpoint Unauthorized Check on the firewall.
3. From Unauthorized External Platform, export Endpoint Unauthorized Check records.

4. Importing Endpoint Unauthorized Check records, to import the Endpoint Unauthorized Check records previously exported from the Unauthorized External Platform into the firewall.

5. On the firewall, view the Endpoint Unauthorized Check details.

Activating The Endpoint Unauthorized Check Function

Before configuring the Endpoint Unauthorized Check function, you need to activate the Endpoint Unauthorized Check function first. You can activate this function by registering the firewall device to the Unauthorized External Platform, so that the Unauthorized External Platform can effectively monitor and record endpoint unauthorized external connection events in the network where the firewall device is located.

To activate the Endpoint Unauthorized Check function, you need to Take the following steps:

1. Log in to the firewall WebUI, select **Object** > **Unauthorized External Link Detection** > **Endpoint Unauthorized Check**, and enter the Endpoint Unauthorized Check page.

2. In the **Device Identifier** text box, click button to copy the device ID.

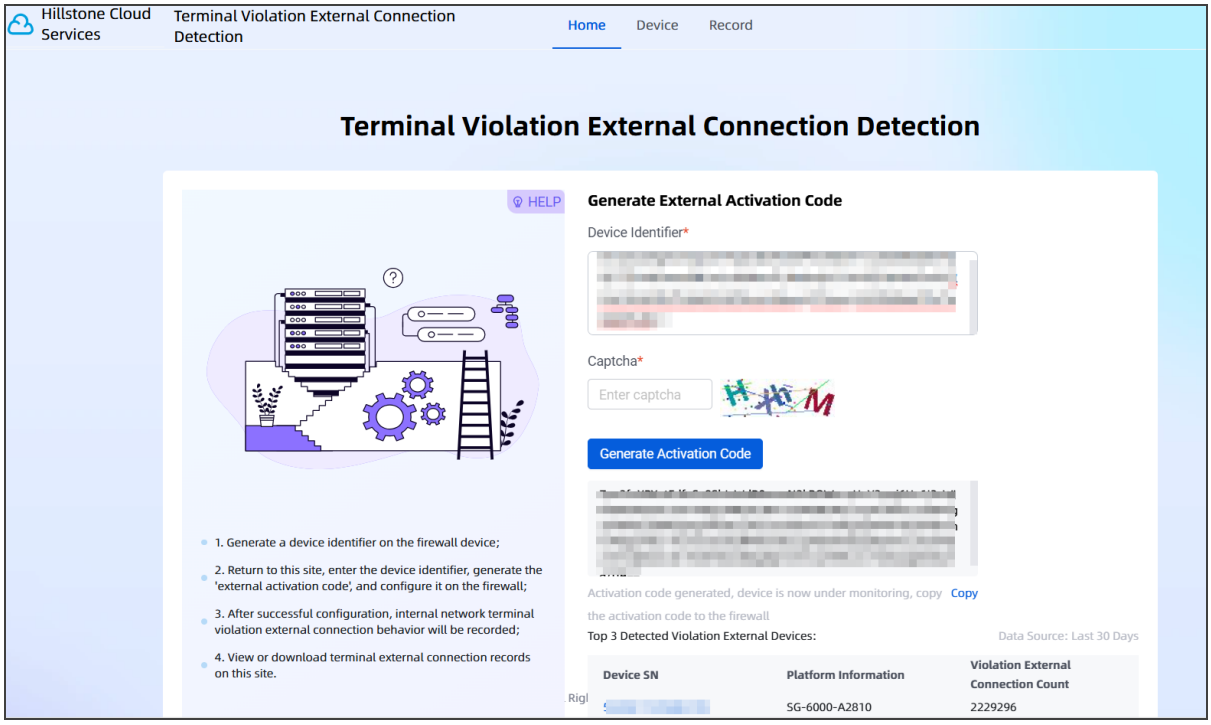
3. Click the Access Unauthorized External Platform button, and in the new window that opens, use your Hillstone Cloud Service Platform account to log in to the Unauthorized External Platform.

   Or click the button after **Access Unauthorized External Platform** to copy the access address of the Unauthorized External Platform, and then enter the address in the browser to log in.

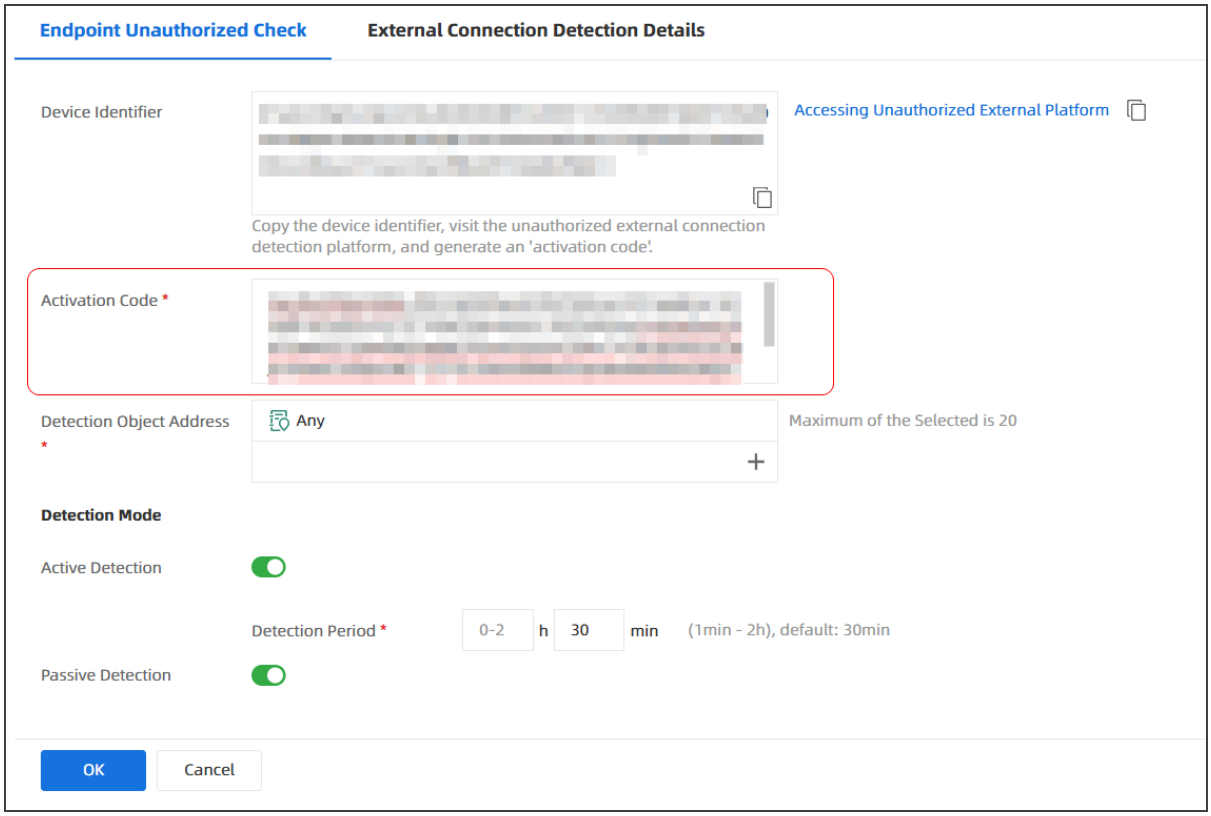
   Unauthorized External Platform Access Address: https://vod.hillstonenet.com.cn

4. Paste the device ID copied from the firewall into the **Device Identifier** text box of Unauthorized External Platform, and then enter the Captcha.

5. Click **Generate Activation Code** , to obtain the external connection activation code.



6. Go back to the firewall's **Endpoint Unauthorized Check** page, and in the **Activation Code** text box, copy the external connection activation code obtained on the Unauthorized External Platform into this text box.



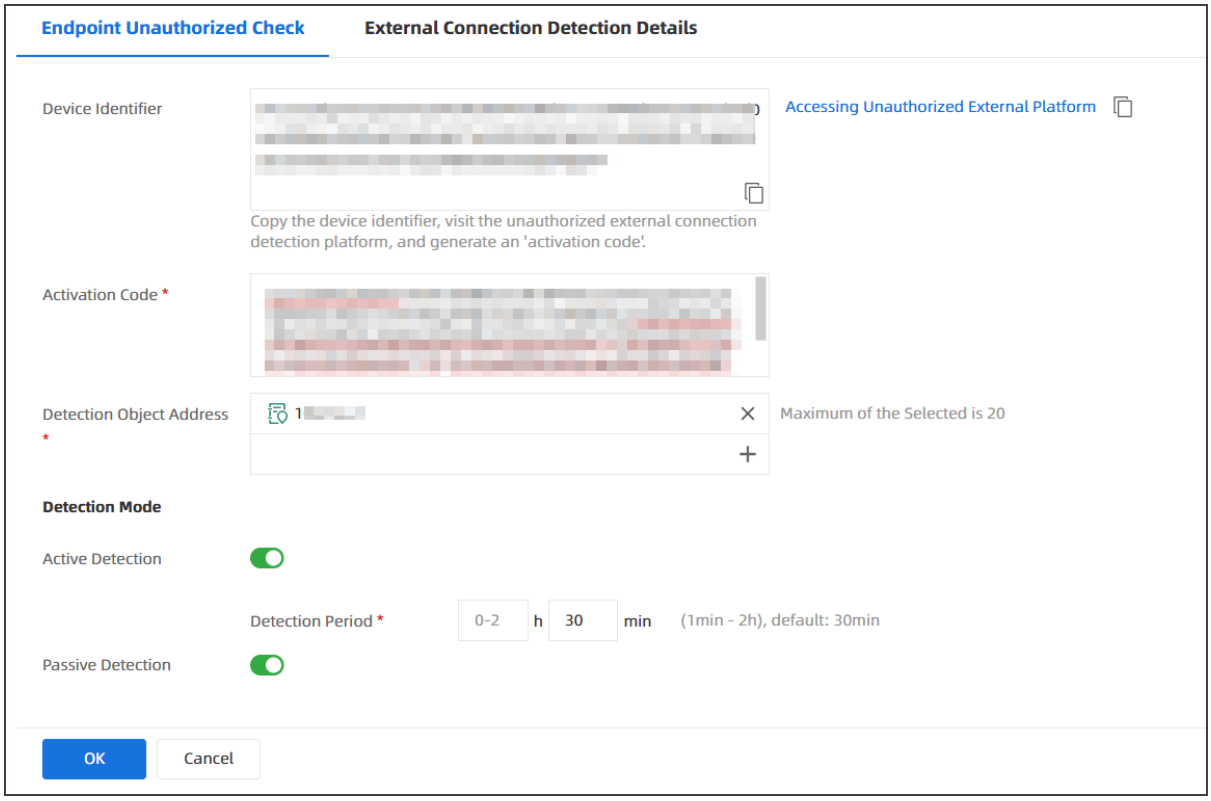
7. Click OK to complete the registration. You can view the information of this firewall on the Unauthorized External Platform.

Configuring Endpoint Unauthorized Check

After successfully activating the Endpoint Unauthorized Check function, you need to configure the objects and detection mode for Endpoint Unauthorized Check.

To configure Endpoint Unauthorized Check, please Take the following steps:

1. Select **Object > Unauthorized External Link Detection > Endpoint Unauthorized Check**.
2. Configure the Endpoint Unauthorized Check related information.



Option	Description
Device Identifier	Displays the identification code of the firewall device. When registering the firewall to the Unauthorized External Platform, you need to use this identification code to obtain the external connection activation code.
Activation Code	Enters the external activation code, which is generated by the Unauthorized External Platform through the device identification code and includes the device SN, preset public network server IP and port, request URL, and Unauthorized External Platform address. When registering the firewall to the Unauthorized External Platform, this activation code is required for authentication.

Option	Description
Detection Object Address	Specifies the detection address of objects to be monitored for unauthorized external connection behavior, i.e., the address of internal endpoint devices. Click the + button next to this option to configure the following address entries: • Address Book: When selecting the address book type, you can directly click the existing address book to add the selected address to the left list; or click the ⊕ button to create a new address book and use it afterward. • Address members: When selecting the address member type, you can enter the IP address range or IP address/subnet mask in the corresponding text box, then click **Add** to add the entered IP address range or IP address/subnet mask to the list on the left. The system supports up to 20 detection object address entries. If not specified, the system will be configured by default as Any. To restore the default configuration, you need to click the **Enable** button after Any.
Detection Mode: The Endpoint Unauthorized Check function includes two methods: active detection and passive detection. You need to choose to enable either mode based on your requirements. The system supports enabling multiple detection modes simultaneously to improve the effectiveness and accuracy of system detection.	

Option	Description
Active Detection	Click the **Enable** button to enable the active detection mode and specify the detection cycle. After enabling, The firewall will proactively send probe packets to endpoint devices with the source address of the pre-deployed public network server according to the set period. If the pre-deployed public network server receives the probe packet, it indicates that the endpoint has unauthorized external connection behavior, and the Unauthorized External Platform will record detailed information of this behavior. this function is disabled by default. • Detection period: Specifies the period for the firewall to send probe packets to the endpoint. The value range is from 1 minute to 2 hours. The system default is 30 minutes.
Passive Detection	Click the **Enable** button to enable the passive detection mode. After enabling, When the firewall processes access requests from endpoint devices to internal network servers, it adds the address of a pre-deployed public network server to the response packet. After the endpoint device receives this response packet, it will redirect the access to the pre-deployed public network server. If the pre-deployed public network server receives an access request, it indicates that the endpoint has unauthorized external connection behavior, and at the same time, the Unau-

Option	Description
	thorized External Platform will record detailed information about this behavior. this function is disabled by default. In passive detection mode, the same IP address endpoint is detected only once within the detection period, and the detection period is set to 1 hour by default. If you need to modify the detection period for this mode, it can only be done via CLI commands. For more information, use the **endpoint-detect mode passive enable period** *time-value* command to readjust the specified period. **Notes:** Enabling the passive detection mode for Endpoint Unauthorized Check may impact system performance when the number of endpoints is enormous. Therefore, it is recommended to enable this function with caution.

3. Click OK.

Exporting Endpoint Unauthorized Check Records

After completing the Endpoint Unauthorized Check configuration, you need to go to the Unauthorized External Platform and export the detailed information of the endpoint violations recorded by the platform to your local device. The exported file format is CSV and supports exporting up to 100,000 records.

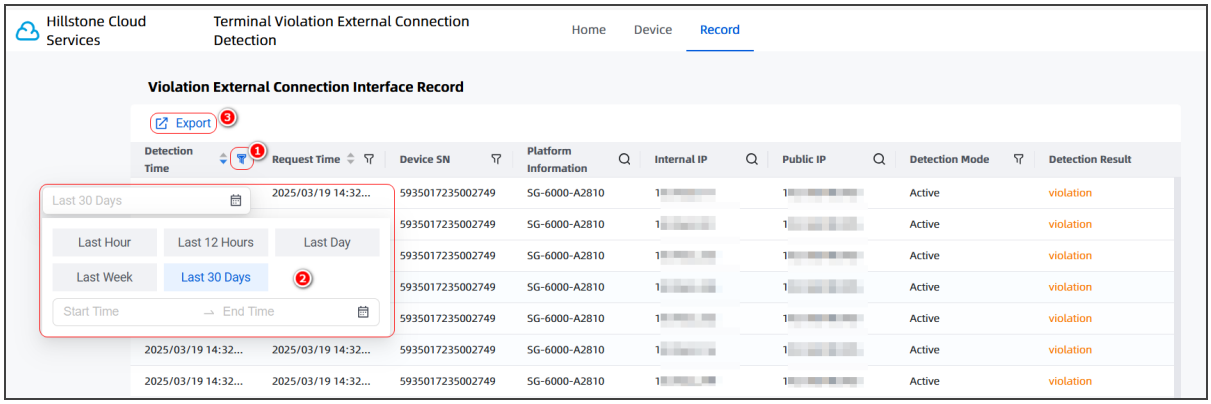
To export Endpoint Unauthorized Check records, please Take the following steps:

1. Log in to the Unauthorized External Platform using your Hillstone Cloud Service Platform account.

   Unauthorized External Platform Access Address: https://vod.hillstonenet.com.cn

2. On the **Record** page, click the **Export** button to export Endpoint Unauthorized Check records from the last 30 days.

   If you need to export Endpoint Unauthorized Check records with specified conditions (such as detection time, device SN, internal network IP, detection mode, etc.), you can click the filter ( ) or search ( ) icon next to the corresponding condition, enter the filter condition, select the records that meet the condition, and then click "Export".



In Unauthorized External Platform, you can also perform the following operations:

- **Viewing all device information registered to the Unauthorized External Platform**: Switch to the **Device** page to view all device information registered to the Unauthorized External Platform, including device SN, platform information, and the number of times violations were detected.
- **Deleting Registered Devices**: Switch to the **Device** page, click the **Delete** button in the operation column of the specified device entry, and delete the registered devices.

Importing Endpoint Unauthorized Check Records Into The Firewall

You need to import the Endpoint Unauthorized Check record file exported in advance from the violation management platform into the firewall for easy viewing and analysis of the reasons for violations, thereby further adjusting the protection strategy and ensuring the security of the system. The system only supports importing CSV format files, and the file size must not exceed 20MB.

To import Endpoint Unauthorized Check records, please Take the following steps:

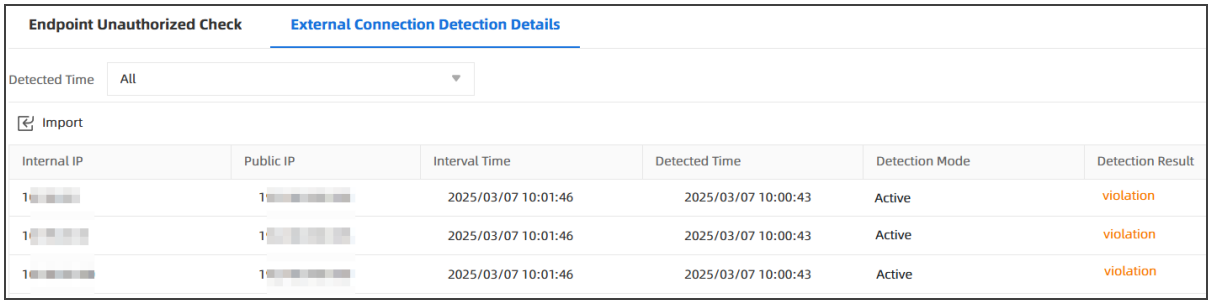
1. Log in to the firewall WebUI, and select **Object** > **Unauthorized External Link Detection** > **Endpoint Unauthorized Check**.
2. Switch to the **External Connection Detection Details** page, click the **Import** button, and open the Import page.



3. Click **Browse** and select the file of the Endpoint Unauthorized Check records obtained in advance from the Unauthorized External Platform.
4. Click OK to complete the import.

Viewing Endpoint Unauthorized Check Details

After importing the Endpoint Unauthorized Check details into the firewall, you can go to the **Object** > **Unauthorized External Link Detection** > **Endpoint Unauthorized Check** > **External Connection Detection Details** page to view the Endpoint Unauthorized Check details and analyze the reasons for the violations, thereby further adjusting the protection strategy to ensure the security of the system.



Configuring Endpoint Unauthorized Check (CLI)

Before You Begin

- Read the "Unauthorized External Link Detection " on Page 421 introduction.
- Read the "Endpoint Unauthorized Check " on Page 425 introduction.

You can configure the Endpoint Unauthorized Check function through two methods: the command-line interface (CLI) and the Web interface (WebUI). To detect endpoint unauthorized of external connection behavior, you need to activate the Endpoint Unauthorized Check function and configure parameters such as detection objects and detection modes on the firewall device.

Using Endpoint Unauthorized Check, you can Take the following steps:

1. Entering the Unauthorized External Link Detection configuration mode
2. Activating the Endpoint Unauthorized Check function
3. Configuring the Unauthorized External Link Detection Object
4. Configuring the detection mode

Entering the Unauthorized External Link Detection Configuration Mode

To enter the Unauthorized External Link Detection configuration mode, in the global configuration mode, use the following command:

violate-outreach-detect

Activating the Endpoint Unauthorized Check function

Before configuring the Endpoint Unauthorized Check function, you need to activate the Endpoint Unauthorized Check function first. You can activate this function by registering the firewall device to the Unauthorized External Platform, so that the Unauthorized External Platform can effectively monitor and record endpoint unauthorized external connection events in the network where the firewall device is located.

To take the following steps to activate the Endpoint Unauthorized Check function:

1. Obtaining the device identifion code on the firewall.
2. Geting the external connection activation code from Unauthorized External Platform
3. Configuring the activation code on the firewall

Obtaining the Device Identifion Code On the Firewall

In any mode, by executing the **show violate-outreach-detect** command, obtain the device identification code in the **Check Code** field of the displayed results. For more information, see "Viewing The Unauthorized External Link Detection Configuration (CLI)" on Page 442.

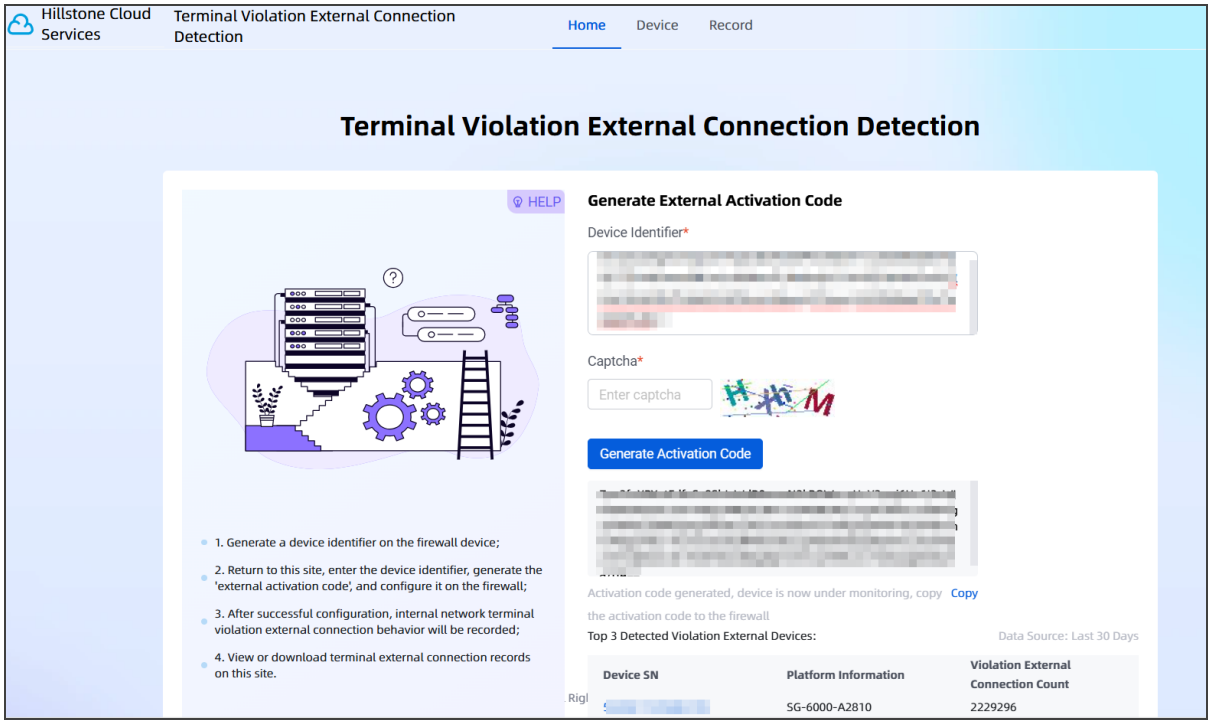
Geting the External Connection Activation Code From Unauthorized External Platform

To get an external activation code from the Unauthorized External Platform, Take the following steps:

1. Enter the access address of Unauthorized External Platform in the browser, and log in to the Unauthorized External Platform using your Hillstone Cloud Service Platform account.

   Unauthorized External Platform Access Address: https://vod.hillstonenet.com.cn

2. Paste the device ID copied from the firewall into the **Device Identifier** text box of Unauthorized External Platform, and then enter the Captcha.



3. \Click **Generate Activation Code** , to obtain the external connection activation code.

Configuring Activation Code

In the Unauthorized External Link Detection configuration mode, use the following commands to configure the activation code:

endpoint-detect activecode *active-code*

- *active-code* - Enter the external connection activation code, which is generated by the Unauthorized External Platform through the device identification code and includes the device SN, preset public network server IP and port, request URL, and Unauthorized External Platform address. When registering the firewall with the Unauthorized External Platform, this activation code is required for authentication. For more information about how to obtain the activation code, see Getting the External Connection Activation Code From Unauthorized External Platform.

In the Unauthorized External Link Detection configuration mode, use the following commands to delete the activation code configuration:

no endpoint-detect activecode *active-code*

Configuring Unauthorized External Link Detection Objects

In the Unauthorized External Link Detection configuration mode, use the following commands to configure the Unauthorized External Link Detection object:

endpoint-detect {**ip** *ip-address/netmask* | **ip-range** *min-ip-address max-ip-address* | **address** *address-book*}

- **ip** *ip-address/netmask* | **ip-range** *min-ip-address max-ip-address* | **address** *address-book* - Specifies the target object addresses for detecting unauthorized external connection behavior, i.e., the addresses of internal endpoint devices. These can be an IP address/netmask, IP address range, or address book.
    - **ip** *ip-address/netmask* - This represents the IP address/netmask.
    - **ip-range** *min-ip-address max-ip-address* - Indicates an IP address range.
    - **address** *address-book* - This represents the address book.

In the Unauthorized External Link Detection configuration mode, use the following commands to delete the specified detection object configuration:

no endpoint-detect {**ip** *ip-address/netmask* | **ip-range** *min-ip-address max-ip-address* | **address** *address-book*}

Configuring The Detection Mode

The Endpoint Unauthorized Check function is divided into two methods: active detection and passive detection. You need to choose to enable either mode based on your requirements. The system supports enabling multiple detection modes simultaneously to improve the effectiveness and accuracy of system detection.

Notes: Enabling the passive detection mode for Endpoint Unauthorized Check may impact system performance when the number of endpoints is enormous. Therefore, it is recommended to enable this function with caution.

Enabling/Disabling the Active Detection Mode

By default, this function is disabled. After enabling it, The firewall will proactively send probe packets to endpoint devices with the source address of the pre-deployed public network server according to the set period. If the pre-deployed public network server receives the probe packet, it indicates that the endpoint has unauthorized external connection behavior, and the Unauthorized External Platform will record detailed information of this behavior. the detection cycle for this mode is 30 minutes by default and can be configured according to your needs.

In the Unauthorized External Link Detection configuration mode, use the following commands to enable the active detection mode and specify the detection period:

endpoint-detect mode active enable [**period** *time-value*]

- **period***time-value* - Specifies the period for the firewall to send probe packets to the endpoint. The value range is 1 to 120 minutes. The system default is 30 minutes.

In the Unauthorized External Link Detection configuration mode, use the following commands to disable the active detection mode:

endpoint-detect mode active disable

Enabling/Disabling Passive Detection Mode

By default, this function is disabled. After enabling it, When the firewall processes access requests from endpoint devices to internal network servers, it adds the address of a pre-deployed public network server to the response packet. After the endpoint device receives this response packet, it will redirect the access to the pre-deployed public network server. If the pre-deployed public network server receives an access request, it indicates that the endpoint has unauthorized external connection behavior, and at the same time, the Unauthorized External Platform will record detailed

information about this behavior.

> **Notes:** In passive detection mode, the same IP address endpoint is detected only once within the detection period, and the detection period is set to 1 hour by default.

In the Unauthorized External Link Detection configuration mode, use the following commands to enable the passive detection function and specify the detection period:

endpoint-detect mode passive enable [**period** *time-value*]

- **period** *time-value* - Specifies the period during which the firewall detects unauthorized external connection behaviors for the same IP address endpoint. The value range is 1~120 minutes. The system default is 60 minutes.

In the Unauthorized External Link Detection configuration mode, use the following commands to disable the passive detection mode:

endpoint-detect mode passive disable

Viewing The Unauthorized External Link Detection Configuration (CLI)

In any mode, use the following command to view the Unauthorized External Link Detection configuration:

show violate-outreach-detect

Example:

```
hostname# show violate-outreach-detect
Gateway Detection: Enable (Displays the status of the Gateway Unauthorized Check function)
Gateway Detection Track: 2.2.22.2 (Displays the track object for the Gateway Unauthorized Check function)
Endpoint Active Detection: Enable (Displays the enabled status of endpoint unauthorized external active detection)
```

Endpoint Active Detection Period: 30 minutes (This shows the period for active detection of endpoint unauthorized externa link.)

Endpoint Passive Detection: Enable (indicates the status of enabling the endpoint unauthorized external passive detection)

Endpoint Passive Detection Period: 60 minutes (This shows the period for passive detection of endpoint unauthorized externa link.)

Check Code: xxx== (Displays the identification code of the firewall device)

Active Code: xxx== (Display the activation code registered for the firewall)

Detection Object Address: 1.1.1.1 (Displays the objects of Endpoint Unauthorized Check)

Supporting for Obtaining the Real MAC Address of IoT Devices via DHCP Syslog and SNMP

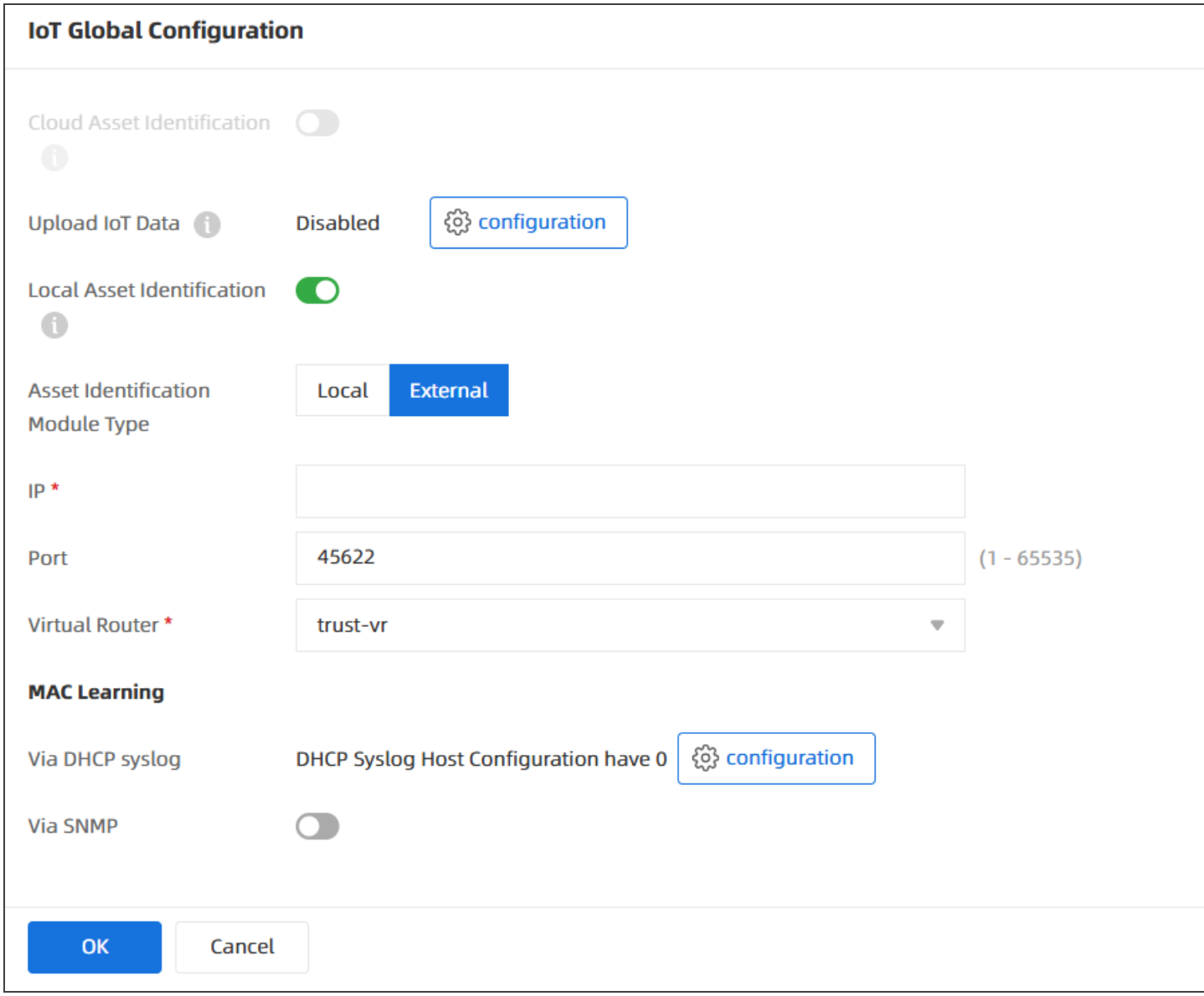
.

Configuring IoT Global Configuration (WebUI)

IoT global configuration includes:

- Enabling the Cloud Asset Identification function
- Uploading IoT data to the cloud platform of Hillstone
- Configuring local asset identification
- Configure the MAC address learning function

Select **Object** > **IoT Policy** > **Configuration**.



Option	Description
Cloud Asset Identification	Click the "Enable" button to enable the Cloud Asset Identification function. After enabling this function, the system extracts IoT device fingerprint information from the traffic passing through the device and sends it to the cloud for identifying IoT devices via the Cloud Asset Identification Service.

Option	Description
Upload IoT Data	Connect to the cloud platform and upload IoT report data and asset data to this platform for unified analysis and statistics. This option displays whether **Upload IoT Data** is enabled. You can click **Configure**. In the **Connecting to Hillstone Cloud Service Platform** panel, select the IoT report data or asset data in the Upload Data Item section.
Local Asset Identification	Identify IoT device assets by using the local asset identification module. To enable this function, turn on the switch. **Note**: If the cloud asset identification function is already enabled before enabling local asset identification, the cloud asset identification function will be automatically disabled. After disabling local asset identification, you can continue to use the cloud asset identification function.
Asset Identification Module Type	Local asset identification is divided into built-in and external types. • Local: Use the built-in asset identification module. Before you select this type, configure the Docker management function of the system to deploy the asset identification system within the firewall.This method applies only to CloudEdge deployed in a cloud environment based on X86 architecture CPU. • External: Use the asset identification system deployed on the virtual machine. Before you select this type, deploy the asset identification system in the virtual machine. **Notes:** The "Local" type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later.

Option	Description
IP	When you select "Local", this IP address is the default IP address of the built-in asset identification module: 127.0.0.1. When you select "External", enter the IP address of the virtual machine.
Port	Specifies the port number of the asset identification module. When you select "Local", this port number is the host port number of Docker. Please make sure this port number is consistent with the host port number specified in Docker. Valid values: 1-65535.
Virtual Router	If you select "External", select a VRouter to which the virtual machine belongs from the drop-down list.

Configuring the MAC Address Learning Function

In an IoT deployment environment across Layer 3 networks, IoT endpoint devices and firewalls belong to different subnets. When packets pass through the Layer 3 switch, the original MAC address of the IoT endpoint device is replaced with the MAC address of the Layer 3 switch, making it difficult for the firewall to obtain the real MAC address of the IoT endpoint device. Since the MAC address serves as a fundamental and stable attribute of the IoT endpoint device, it plays a critical role in determining the device manufacturer and endpoint identification. Therefore, the system provides a MAC address learning function to address the challenge of enabling the firewall to obtain the real MAC address of the IoT endpoint device in cross-subnet scenarios, laying a solid foundation for precise recognition of IoT endpoint devices and strengthening IoT network management and security protection.

The system supports obtaining the MAC address information of IoT devices through the following two methods. You can choose either one based on your needs or use multiple methods simultaneously. When multiple methods are enabled at the same time, the priority of obtaining the MAC address via DHCP Syslog is higher than that via SNMP.

- Obtaining MAC Addresses via DHCP Syslog
- Obtaining MAC Addresses via SNMP

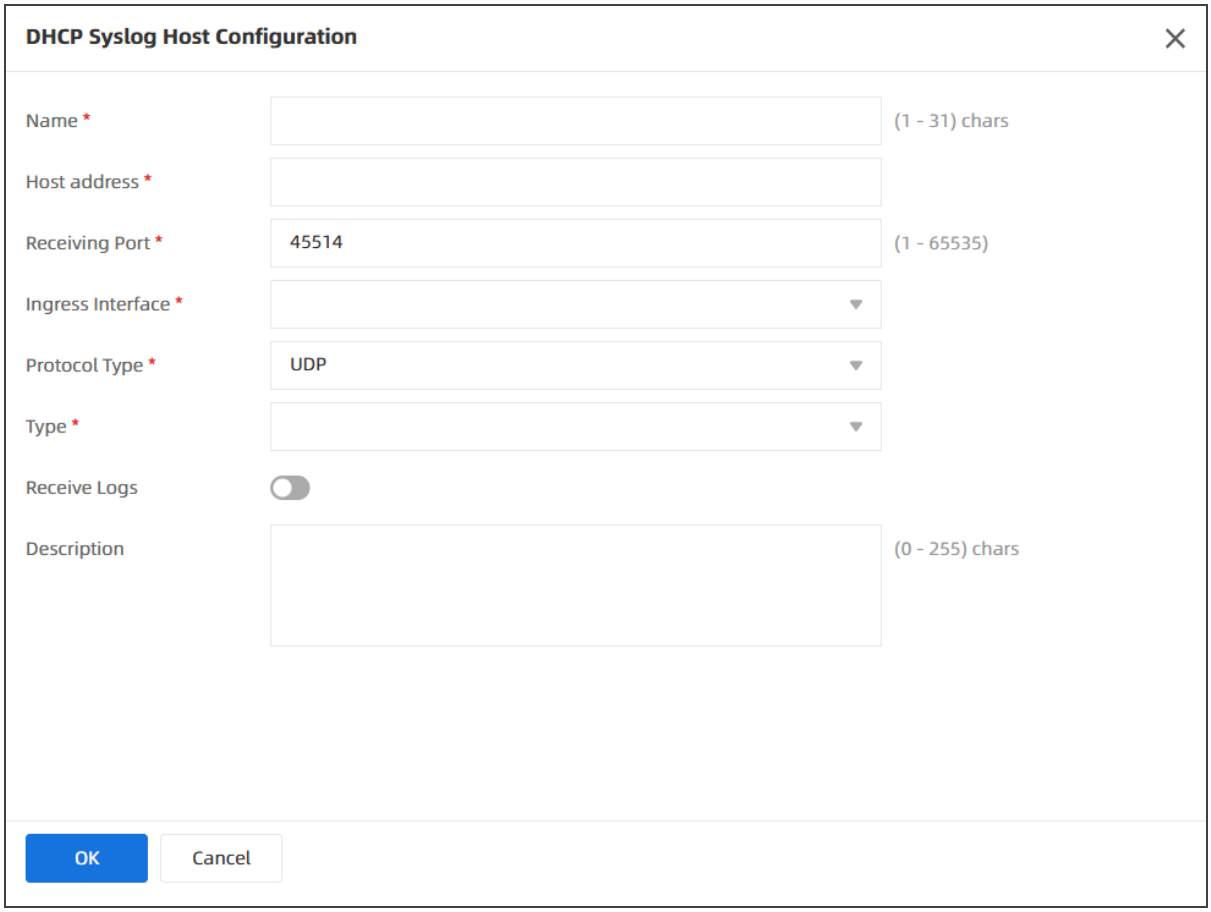
Obtaining MAC Addresses via DHCP Syslog

This method relies on the attributes of DHCP Syslog Host for sending out log data. When the DHCP Syslog Host successfully establishes a communication connection with the firewall device, it will proactively send the log data to the firewall. The firewall acts as a log server and, upon receiving the log data sent by the DHCP Syslog Host, will immediately parse it and extract key information such as the real MAC address and IP address of the device. This facilitates subsequent management of device assets in the network by you, thereby improving the efficiency of network management and providing an important guarantee for network security monitoring.

To obtain the MAC address through DHCP Syslog by take the following steps:

1. Select **Object** > **IoT Policy** > **Configuration**.
2. In the **MAC Learning** section, click the **Configuration** button after **Via DHCP syslog** to enter to the **DHCP Syslog Host Table** page.
3. Click **New** to open the **DHCP Syslog Host Configuration** page and configure the DHCP Sys-

log Host information.



Option	Description
Name	Specifies the name of the DHCP Syslog Host. The value range is 1 to 31 characters.
Host Address	Specifies the IP address of the DHCP Syslog Host, supporting both IPv4 and IPv6 addresses.
Receiving Port	Specifies the port number for the firewall to receive DHCP Syslog Host logs. The value range is 1 to 65535, with a default of 45514.
Ingress Interface	Specifies the name of the interface that the firewall uses to receive DHCP Syslog Host logs.

Option	Description
Protocol Type	Specifies the protocol type used for establishing communication connections between the firewall and the DHCP Syslog Host, including UDP, TCP, and SSL protocols. By default, UDP protocol is used for communication. **Notes:** When using the SSL protocol for encrypted communication, you need to install the firewall's CA certificate on the DHCP Syslog Host in advance for relevant services or programs with DHCP log forwarding functions to achieve encrypted authentication. The firewall's CA certificate can be exported from the "System > PKI > Trust Domain Certificate" page. For more information, see Importing/Exporting Trust Domain.
Type	Specify the DHCP Syslog Host operating system's corresponding DHCP service type. The log formats supported by different operating systems' DHCP service types vary; please configure according to your needs. **Notes:** The supported DHCP service types are controlled by the IoT feature library. There are differences in the supported DHCP service types between different versions of the IoT feature library. Please refer to the current actual version.
Receive Logs	Click the "Enable" button to enable the receiving logs func-

Option	Description
	tion.After enabling, once the firewall successfully establishes a communication connection with the DHCP Syslog Host, the firewall can receive log information sent from the DHCP Syslog host. This function is disabled by default.
Description	Add description information for the DHCP Syslog Host, with a value range of 0 to 255 characters.

4. Click **OK** to complete the DHCP syslog server configuration and return to the **DHCP Syslog Host Table** page.

> **Notes:** The system supports a maximum of 8 DHCP Syslog Hosts for configuration.

5. Click **Close**, then return to the **IoT Global Configuration** page.
6. Click **OK**.

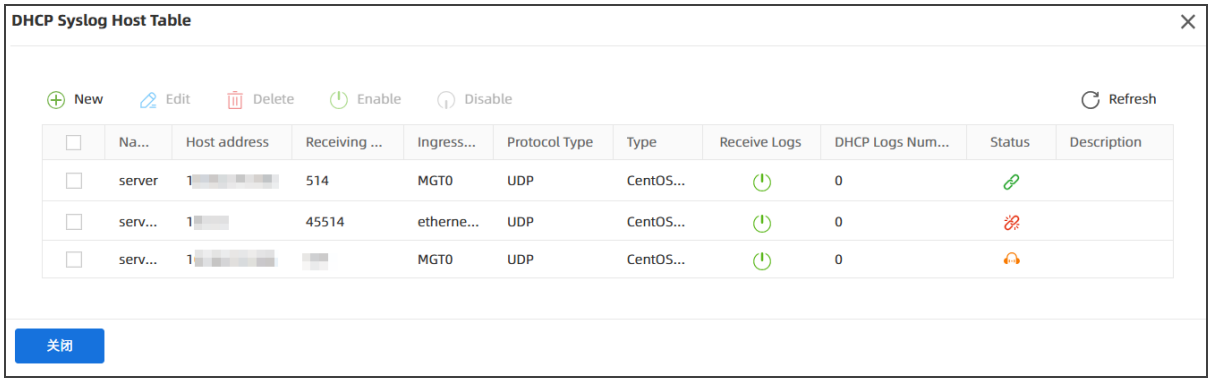
DHCP Syslog Host Management

After completing the DHCP Syslog Host configuration, you can view the DHCP Syslog Host details on the **DHCP Syslog Host Table** page, including the name, host address, protocol type, connection status, and the number of logs sent to the firewall.

The connection status of the DHCP Syslog Host is divided into three types: connected, disconnected, and listening.

- Connected : This indicates that the DHCP Syslog Host has established a communication connection with the firewall device, meaning the log data sent by the DHCP Syslog host can be successfully received by the firewall.

- Disconnected : This indicates that the DHCP Syslog Host has not established a communication connection with the firewall device.
- Listening : This indicates that the firewall has enabled the function to receive logs, but no communication connection from the DHCP Syslog Host has been received.



In the **DHCP Syslog Host Table** page, you can also perform the following operations on DHCP Syslog Hosts:

- **Enabling/Disabling the Log Receiving Function**: In the **DHCP Syslog Host Table**, select a specified DHCP Syslog Host entry and click the "Enable" or "Disable" button above the list to enable or disable the log receiving function.After enabling, once the firewall successfully establishes a communication connection with the DHCP Syslog Host, the firewall can receive log information sent from the DHCP Syslog host.
- **Editing/Deleting DHCP Syslog Hosts**: In the **DHCP Syslog Host Table**, select the specified DHCP Syslog Host entry and click the "Edit" or "Delete" button above the list to edit or delete the relevant content of the DHCP Syslog Host.

For more information, refer to the **Threat Prevention > IoT > Configuring IoT Global Configuration** section in *StoneOS WebUI User Guide*. FR 40176

Obtaining MAC Addresses via SNMP

Before you start:

- Configuring SNMP Server

The system can obtain ARP information related to devices via the SNMP server and query the corresponding real MAC address based on the IP address of the IoT device. You need to enable the SNMP function as it is disabled by default.

To enable the function to obtain MAC addresses via SNMP, Take the following steps:

1. Select **Object** > **IoT Policy** > **Configuration**.
2. In the **MAC Learning** section, click the  button after **via SNMP** to enable the MAC address acquisition via SNMP function.
3. Click **OK**.

For more information, refer to the **Threat Prevention** > **IoT** > **Configuring IoT Global Configuration** section in *StoneOS WebUI User Guide*. FR 40523

SNMP Server

You can configure the SNMP server to get the ARP information through the SNMP protocol.

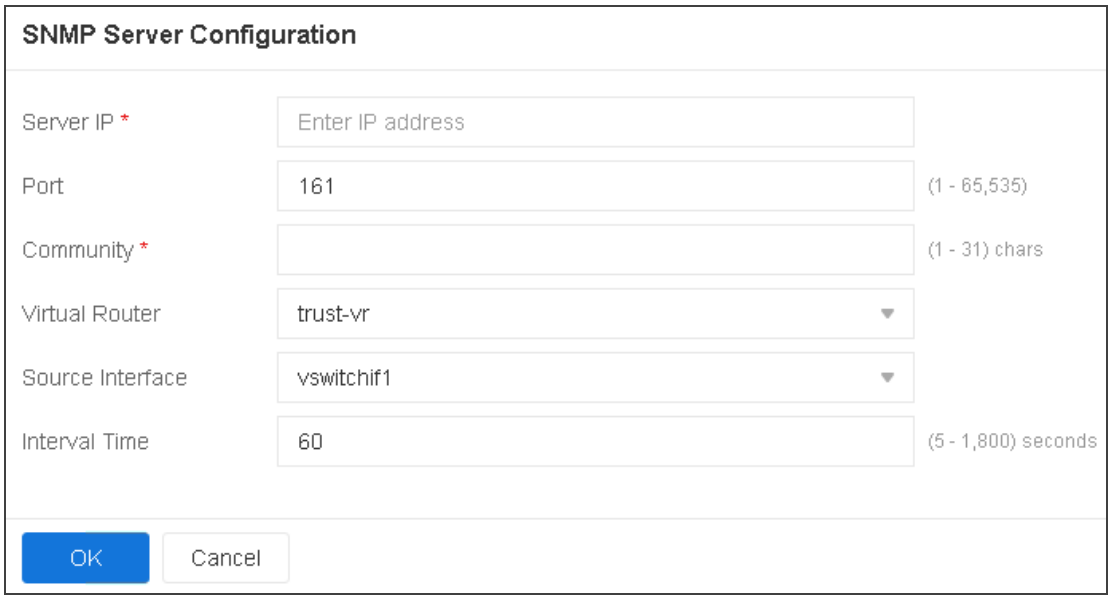
> **Notes:** You can create up to 8 SNMP Servers.

Creating an SNMP Server

To create an SNMP server, take the following steps:

1. Select **System** > **SNMP server**.

2. Click **New**.



Option	Description
Server IP	Type the SNMP server IP address into the **Server IP** box.
Port	Type the port number for the SNMP server into the **Port** box. The value range is 1 to 65535, the default value is 161.
Community	Type the community for the SNMP server into the **Community** box. This option is only effective if the SNMP version is V1 or V2C.
Virtual Router	Select the VRouter from the drop-down list.
Source Interface	Select the source interface for connecting to the SNMP server from the drop-down list. System will send and receive SNMP messages through the specified interface.
Interval Time	Specify the interval time for the firewall to send request messages to the SNMP server. The firewall will periodically send

Option	Description
	request messages to the SNMP server to obtain related ARP information. Enter the interval time in the text box, with a value range of 5 to 1800 seconds, and the default is 60 seconds.

3. Click **OK**.

For more information, refer to the **System** > **SNMP Server** section in *StoneOS WebUI User Guide*. FR 40523

Configuring Mac Address Learning Function (CLI)

In an IoT deployment environment across Layer 3 networks, IoT endpoint devices and firewalls belong to different subnets. When packets pass through the Layer 3 switch, the original MAC address of the IoT endpoint device is replaced with the MAC address of the Layer 3 switch, making it difficult for the firewall to obtain the real MAC address of the IoT endpoint device. Since the MAC address serves as a fundamental and stable attribute of the IoT endpoint device, it plays a critical role in determining the device manufacturer and endpoint identification. Therefore, the system provides a MAC address learning function to address the challenge of enabling the firewall to obtain the real MAC address of the IoT endpoint device in cross-subnet scenarios, laying a solid foundation for precise recognition of IoT endpoint devices and strengthening IoT network management and security protection.

The system supports obtaining the MAC address information of IoT devices through the following two methods. You can choose either one based on your needs or use multiple methods simultaneously. When multiple methods are enabled at the same time, the priority of obtaining the MAC address via DHCP Syslog is higher than that via SNMP.

- Obtaining MAC Addresses via DHCP Syslog
- Obtaining MAC Addresses via SNMP

Obtaining MAC Addresses via DHCP Syslog

This method relies on the attributes of DHCP Syslog Host for sending out log data. When the DHCP Syslog Host successfully establishes a communication connection with the firewall device, it will proactively send the log data to the firewall. The firewall acts as a log server and, upon receiving the log data sent by the DHCP Syslog Host, will immediately parse it and extract key information such as the real MAC address and IP address of the device. This facilitates subsequent management of device assets in the network by you, thereby improving the efficiency of network management and providing an important guarantee for network security monitoring.

To obtain the MAC address via DHCP Syslog. You need to Take the following steps:

1. Entering DHCP Syslog Host configuration mode
2. Configuring DHCP Syslog Host parameters
3. enabling the receiving logs function
4. (Optional) Viewing the DHCP Syslog Host details

Entering DHCP Syslog Host Configuration Mode

To create a DHCP Syslog Host with the specified name and enter the DHCP Syslog Host configuration mode. If the specified name already exists, enter the DHCP Syslog Host configuration mode directly.

In global configuration mode, use the following commands to create a DHCP Syslog Host and enter the DHCP Syslog Host configuration mode:

iot-monitor get-mac dhcp-syslog-host *host-name*

- *host-name* - Specifies the name of the DHCP Syslog Host. The system supports creating up to 8 DHCP Syslog Hosts.

In global configuration mode, use the following commands to delete the DHCP Syslog Host with the specified name and its configuration information:

no iot-monitor get-mac dhcp-syslog-host *host-name*

Configuring DHCP Syslog Host Parameters

To ensure that the firewall and DHCP Syslog Host can successfully establish a communication connection, you need to configure parameters such as the IP address, protocol type, and DHCP service type of the DHCP Syslog Host.

Specifying the IP Address of the DHCP Syslog Server

To specify the IP address of the DHCP Syslog Host. Use the following command in DHCP Syslog Host configuration mode:

address {*ipv4-address* | *ipv6-address*}

- *ipv4-address* - To enter the IPv4 address.
- *ipv6-address* - To enter the IPv6 address.

In DHCP Syslog Host configuration mode, use the following commands to delete the IP address configuration of the DHCP Syslog Host:

no address

Specifying the Port Number for the Firewall to Receive DHCP Syslog Host Logs

To specify the port number for the firewall to receive DHCP Syslog Host logs. In the DHCP Syslog Host configuration mode, use the following command:

port *port_number*

- *port_number* - Specifies the port number. The value range is 1 to 65535, and the default is 45514.

In the DHCP Syslog Host configuration mode, use the following commands to restore the default configuration:

no port

Specifying the Interface for the Firewall to Receive DHCP Syslog Host Logs

To specify the interface for the firewall to receive DHCP Syslog Host logs. In the DHCP Syslog Host configuration mode, use the following commands:

interface *interface-name*

- *interface-name* - Specifies the interface name for the firewall to receive DHCP Syslog Host logs.

In the DHCP Syslog Host configuration mode, use the following commands to delete the relevant configurations:

no interface

Specifying The DHCP Syslog Host Communication Protocol Type

To specify the protocol type used for communication connections between the firewall and the DHCP Syslog Host, including UDP, TCP, and SSL protocols. By default, UDP protocol is used for communication.

Notes: When using the SSL protocol for encrypted communication, you need to install the firewall's CA certificate on the DHCP Syslog Host in advance for relevant services or programs with DHCP log forwarding functions to achieve encrypted authentication. The firewall's CA certificate can be exported from the "System > PKI > Trust Domain Certificate" page. For more information, see Importing and exporting a PKI trust domain.

In the DHCP Syslog Host configuration mode, use the following commands to specify the protocol type used by the firewall when establishing a communication connection with the DHCP Syslog Host:

connect-type {**tcp** | **udp** | **ssl**}

- **tcp** - Specifies the TCP protocol.
- **udp** - Specifies the UDP protocol. The system defaults to this option.
- **ssl** - Specifies the SSL protocol.

In the DHCP Syslog Host configuration mode, use the following commands to restore the default configuration:

no connect-type

Specifying the DHCP service type

To specify the DHCP Syslog Host operating system corresponding to the DHCP service type. The log formats supported by different operating system DHCP service types vary, please configure according to your needs.

> **Notes:** The supported DHCP service types are controlled by the IoT feature library. There are differences in the supported DHCP service types between different versions of the IoT feature library. Please refer to the current actual version.

In the DHCP Syslog Host configuration mode, use the following commands to specify the DHCP service type:

type *type-name*

- *type-name* - Specifies the name of the DHCP service type.

In the DHCP Syslog Host configuration mode, use the following commands to delete the DHCP service type configuration:

no type

Adding Description Information

To add description information for the DHCP Syslog Host. In the DHCP Syslog Host configuration mode, use the following commands:

description *description*

- *description* - Addes relevant description information for the DHCP Syslog Host. The value range is 1 to 255 characters.

In the DHCP Syslog Host configuration mode, use the following commands to delete the description:

no description

Enabling/Disabling the Log Receiving Function

After completing the DHCP Syslog Host configuration, you need to enable the log reception function on the firewall device to ensure that the firewall can properly receive log information sent by the DHCP Syslog Host.After enabling, once the firewall successfully establishes a communication connection with the DHCP Syslog Host, the firewall can receive log information sent from the DHCP Syslog host. This function is disabled by default.

In DHCP Syslog Host configuration mode, use the following commands to enable/disable the log reception function:

- Enable: **enable**
- Disable: **no enable**

Viewing DHCP Syslog Host Details

To view the details of the DHCP Syslog Host, use the following commands in any mode:

show iot-monitor get-mac dhcp-syslog-host [*host-name* | **detail** | *host-name* **detail**]

- **show iot-monitor get-mac dhcp-syslog-host** - Displays the configuration information of all DHCP Syslog Hosts.

- *host-name* - Displays the configuration information of the specified DHCP Syslog Host.
- **detail** - Displays detailed information about all DHCP Syslog Hosts, including configuration information of the DHCP Syslog Host and the number of connections for the DHCP Syslog Host, etc.
- *host-name***detail** - Displays detailed information for a single DHCP Syslog Host.

Example:

```
hostname(config)# show iot-monitor get-mac dhcp-syslog-host
IoT-monitor DHCP-Syslog-Host total num: 1
==========================================-
====
DHCP Syslog Host name: server1 (Displays the name of the DHCP Sys-
log Host)
description: (Displays the description of the DHCP Syslog Host)
enable: on (Displays the status of the log receiving function being
enabled)
address: 10.1.1.1 (Displays the IP address of the DHCP Syslog server)
type: CentOS-dhcpd (Displays the DHCP Syslog Host operating system
corresponding to the DHCP service type)
connect-type: udp (This shows the protocol type used when establishing
a communication connection between the firewall and the DHCP Syslog
Host.)
port: 5144 (The port number for the firewall to receive DHCP Syslog
Host logs)
interface: MGT0 (Displays the interface name where the firewall
receives DHCP Syslog Host logs)
status: Connected (Displays the connection status of the DHCP Syslog
Host)
```

```
dhcp-log-count: 0 (Displays the number of logs sent by the DHCP Sys-
log Host to the firewall)
==========================================-
====
```

For more information, refer to the **Threat Prevention** > **IoT Monitor** section in *StoneOS CLI User Guide*. FR 40176

Obtaining MAC Addresses via SNMP

Before you start:

- Configuring SNMP Server

The system can obtain ARP information related to devices via the SNMP server and query the corresponding real MAC address based on the IP address of the IoT device. You need to enable the SNMP function as it is disabled by default.

To enable the function to obtain MAC addresses via SNMP, in global configuration mode, use the following commands:

iot-monitor get-mac snmp enable

To disable the function to obtain MAC addresses via SNMP, in global configuration mode, use the following commands:

no iot-monitor get-mac snmp enable

To view the status of the SNMP MAC address retrieval function, in any mode, use the following command:

show iot-monitor get-mac snmp

The following is an example of a return result:

```
hostname# show iot-monitor get-mac snmp
IoT-monitor gets MAC address from SNMP: enable
```

For more information, refer to the **Threat Prevention** > **IoT Monitor** section in *StoneOS CLI User Guide*. FR 40523

Configuring SNMP

Hillstone device provides the following SNMP configuration options:

.....

Configuring SNMP Server

You can configure the SNMP server to get the ARP information through the SNMP protocol.

> **Notes:** You can create up to 8 SNMP Servers.

To configure the SNMP server, in the global configuration mode, use the following command:

arp-mib-query server *ip-address* **community** *string* [**vrouter** *vrouter-name*] [**source** *interface-name*] [**port** *port-number*] [**interval** *value*]

- *ip-address* – Specifies the IP address of SNMP server.
- **community** *string* – Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.
- **vrouter** *vrouter-name* – Specifies the name of VRouter.
- **source** *interface-name* – Specify the source interface for connecting to the SNMP server. The firewall will send and receive SNMP messages through the specified interface.
- **port** *port-number* – Specifies the port number of SNMP server. The value range is 1 to 65535, the default value is 161.
- **interval** *value* – Specify the interval time for the firewall to send request messages to the SNMP server. The firewall will periodically send request messages to the SNMP server to obtain related ARP information. Enter the interval time in the text box, with a value range of 5 to 1800 seconds, and the default is 60 seconds.

To delete the SNMP server, use the command **no arp-mib-query server** *ip-address*.

For more information, refer to the **System Management** > **Simple Network Management Protocol** > **Configuring SNMP** section in *StoneOS CLI User Guide*. FR 40523

IoT Monitor (Log)

……

ID:	0x45015501
Type:	IoT
Severity:	Notifications
Message:	The firewall is connected to the DHCP Syslog Host whose IP address is *IP-address*.
Description:	The firewall is connected to the DHCP Syslog Host whose IP address is *IP-address*.
Solution:	N/A

ID:	0x45015502
Type:	IoT
Severity:	Notifications
Message:	The firewall is disconnected to the DHCP Syslog Host whose IP address is *IP-address*.
Description:	The firewall is disconnected to the DHCP Syslog Host whose IP address is *IP-address*.
Solution:	N/A

ID:	0x45015503
Type:	IoT
Severity:	Notifications
Message:	The service-connection of DHCP Syslog Host has not stopped within 1s.

Description:	The service-connection of DHCP Syslog Host has not stopped within 1s.
Solution:	N/A

ID:	0x45015401
Type:	IoT
Severity:	警告（Warnings）
Message:	中文：DHCP Syslog服务的配置重复，主机名称是*主机名称*。 英文：The configuration of DHCP Syslog service is repeated, host-name is *host-name*.
Description:	DHCP Syslog服务的配置重复，主机名称是*主机名称*。
Solution:	N/A

ID:	0x45015402
Type:	IoT
Severity:	Warnings
Message:	The parameter of DHCP Syslog service is invaild, host-name is *host-name*.
Description:	The parameter of DHCP Syslog service is invaild, host-name is *host-name*.
Solution:	N/A

ID:	0x45015403
Type:	IoT
Severity:	Warnings
Message:	The DHCP Syslog service has unknown error, host-name is *host-name*.

Description:	The DHCP Syslog service has unknown error, host-name is *host-name*.
Solution:	N/A

Support Modifying the Model and Operating System Information of IoT Devices

WebUI

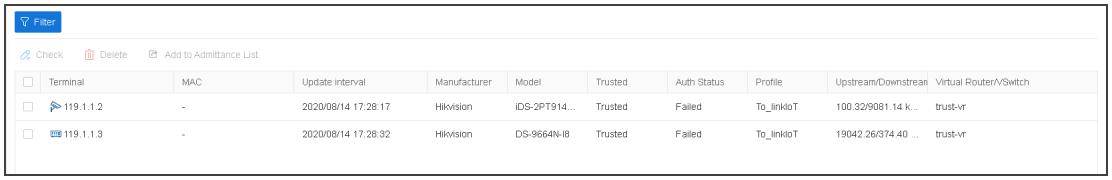
IoT Monitor

IoT Monitor function displays the manufacturers and types distribution of network video monitoring devices, as well as the detailed statistics, such as device number, IP address, MAC address, up/downstream traffic, IoT profile and device status.

.....

Details

Click **Monitor** > **IoT Monitor** > **Details** to view the detailed information of the network video monitoring devices.



- Click the Filter button to add filter conditions and the required information will be filtered out in the following list.
- Select the check box, and click **Delete** to delete the selected item.
- Select the check box, and click **Check**, then the **IoT Profile Configuration** page pops up. You can customize the manufacturer, type, model, OS family, and OS version information of IoT devices on this page, or you can select from predefined device attributes. Information you manually modify has a higher priority than recognized results.

  Note: The custom count limit for each device property is 1000.

- Select the check box and click **Add to Admittance List** to add the selected item to the target admittance list template. For the detailed steps, refer to Adding to Admittance List.
- Click **Add to Respository** to add the selected network video monitor device to the repository.
- Click **Remove From Respository** to remove the selected network video monitor device from the repository.
- For the icons in the **Terminal** list, if the icon is gray, it means that the device is offline; if the icon is blue, it means that the device is online. When you hover the mouse over the icon, you can also view the online status of the device. The icons represent the following devices respectively:
  - : The network video monitoring devices of other manufacturers.
  - : The IPC device.
  - : The NVR device.
  - Null: The item hasn't been identified.

For more information, refer to the **Threat Prevention** > **IoT** > **IoT Monitor** section in *StoneOS WebUI User Guide*. FR 40172

Device Object

The system provides a device dictionary, including information on supported vendors, types, models, os families, and os versions.You can categorize one or more IoT devices into a device collection based on multiple dimensions of the device (including the manufacturer, type, model, and operating system of the device) and assign a device object name to the device collection. The system maps the identified IoT device information with the device object attributes, and then the security policy can directly reference the device object name to control the IoT device collection.

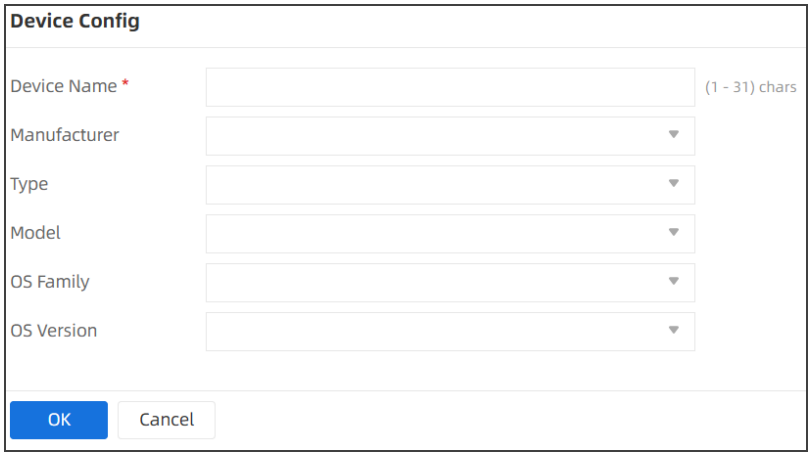
Notes:

- The device object can be configured only after you install an IoT control license.
- The device dictionary is included in the IoT device fingerprint library, and you can update the device dictionary by upgrading the IoT device fingerprint library. For more information, see "System > Upgrading System > Upgrading Signature Database" section.

Creating a Device Object

To create a device object, take the following steps:

1. Select **Object** > **Device**.
2. Click **New**.



Option	Description
Device Name	Enter the name of the device object, which needs to be 1 to 31 characters in length.
Manufacturer	Select the manufacturer type and manufacturer name. • Predefined: Select **Predefined** and then select a man-

Option	Description
	ufacturer name in the list below. You can also search for a predefined manufacturer name in the search box. • User-defined: Select **User-defined**, enter a custom manufacturer name, and then click **Add**.
Type	Select the device type and type name. • Predefined: Select **Predefined** and then select a device type name in the list below. You can also search for a predefined device type name in the search box. • User-defined: Select **User-defined**, enter a custom device type name, and then click **Add**.
Model	Select the Model. • Predefined: Select **Predefined** and then select a model name in the list below. You can also search for a predefined model name in the search box. • User-defined: Select **User-defined**, enter a custom model name, and then click **Add**
OS Family	Select the OS family type and name. • Predefined: Select **Predefined** and then select an OS family name in the list below. You can also search for a predefined OS family name in the search box. • User-defined: Select **User-defined**, enter a custom OS family name, and then click **Add**.

Option	Description
OS Version	Select the corresponding OS version. • Predefined: Select **Predefined** and then select an OS version in the list below. You can also search for a predefined OS version in the search box. • User-defined: Select **User-defined**, enter a custom OS family version, and then click **Add**.

3. Click **OK**. The newly create device object is displayed in the list.

Notes: The custom count limit for each device property is 1000.

For more information, refer to the **Threat Prevention** > **IoT** > **Device Object** section in *StoneOS WebUI User Guide*. FR 40172

CLI

IoT Monitor

IoT Monitor consists of the following parts:

- Viewing the IoT Monitor List Information
- Modifying IoT Monitor List Entry
- Deleting IoT Monitor List Entry

.....

Modifying IoT Monitor List Entry

To modify the IoT Monitor list entries, in any mode, use the following command:

exec iot-monitor modify iot-monitor-list{ **ip** *ip-address*| **ipv6** *ipv6-address*}{**vrouter** *vr-name* | **vswitch** *vs-name*} [**manufacturer***manufacturer-name*] [**type** *type-name*] [**model** *model-name*] [**os-family** *family-name* [**os-version** *version-name*]]

- *ip-address* - Modify the IoT monitor list entries of the specified IP address.
- **ipv6***ipv6-address* - Modify the IoT monitor list entries of the specified IPv6 address.
- *vr-name* - Specifies the VRouter name of the IP.
- *vs-name* - Specifies the VSwitch name of the IP.
- **manufacturer** *manufacturer-name*- Modify the manufacturers of the IoT monitor list entry of the specified IP address.
- **type** *type-name*- Modify the device type of the IoT monitor list entry of the specified IP address.
- *model-name* - Modify the device model of the IoT monitor list entry of the specified IP address.
- **os-family** *family-name* - Modify the OS Family of the IoT monitor list entry of the specified IP address.
- **os-version** *version-name* - Modify the OS Version of the IoT monitor list entry of the specified IP address.

For more information, refer to the **Threat Prevention** > **IoT Monitor** > **IoT Monitor** section in *StoneOS CLI User Guide*. FR 40172

Supporting for Protocol Independent Multicast - Dense Mode (PIM-DM) function

Configuring Protocol Independent Multicast (PIM)

The Protocol Independent Multicast (PIM) indicates that static route or any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP, can provide the routing information for IP multicast. Multicast routing is not dependent on the unicast routing protocols, as long as the multicast routing tables are generated by the unicast routing protocols.

According to different mechanisms, PIM is divided into the following two modes:

- PIM-DM (Protocol Independent Multicast-Dense Mode): applies to small-scale networks in which receivers are densely distributed.
- PIM-SM (Protocol Independent Multicast-Sparse Mode): applies to large-scale networks in which receivers are sparsely distributed.

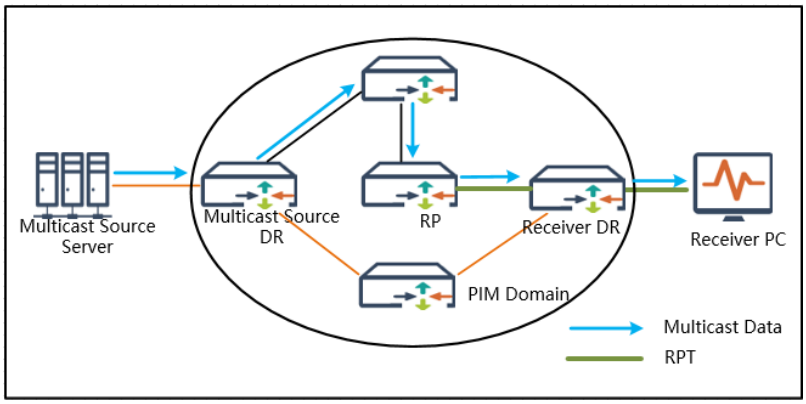
Basic Principles of PIM-SM

PIM-SM (Protocol Independent Multicast-Sparse Mode) can resolve P2MP data transmission problems in a large-scale network where users are sparsely distributed.

PIM-SM assumes that no host wants to receive multicast data. The PIM device forwards multicast data to the host only when a host requests multicast data explicitly.

PIM-SM sends the multicast information to the PIM device in the PIM domain through the configured RP (Rendezvous Point) and BSR (BootStrap Router), and then an RPT (Rendezvous Point

Tree) will be built. Multicast data can be forwarded to the receiver along the RPT through the RP.



The key concepts of PIM-SM are as follows:

- **PIM Domain**: A network formed by PIM devices.
- **DR (Designated Router)**: There are two types of DR in a PIM network.
    - **Multicast source DR**: A PIM device that is directly connected to the multicast source in a PIM-SM domain and is responsible for sending Register messages to the RP.
    - **Receiver DR**: A PIM device that is directly connected to group members (receiver hosts) and is responsible for forwarding multicast data to the group members.
- **RP (Rendezvous Point)**: An RP is the core of a PIM-SM network, which can be divided into the static RP and dynamic RP. An RPT is a shared tree with an RP as the root and members of multicast group as the leaves in a PIM-SM network.
- **BSR (BootStrap Router)**: A BSR of a PIM-SM network, which is responsible for collecting and distributing RP information.
- **RPT (Rendezvous Point Tree)**: An RPT is a multicast distribution tree (MDT) with an RP as the root and members of multicast group as the leaves.
- **SPT (Shortest Path Tree)**: A shortest path tree (SPT) is a multicast distribution tree (MDT) with the multicast source as the root and members of multicast group as leaves.

PIM-SSM

PIM-SM needs to maintain Rendezvous Points (RPs) to transmit multicast data. If receivers know the exact location of a multicast source and want to request multicast data directly from the multicast source, Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) can enable receiver hosts to rapidly join multicast groups by maintaining relationship between hosts and routers through IGMPv3. A shortest path tree (SPT) is set up between the multicast source and group members without maintaining an RP. The multicast data will be forwarded to receivers along the SPT.

Basic Principles of PIM-DM

PIM-DM (Protocol Independent Multicast-Dense Mode, Protocol Independent Multicast-Dense Mode) can effectively address the efficient distribution of multicast data in dense networks, ensuring reasonable use of network bandwidth and flexibility in dynamic group membership management.

PIM-DM assumes that the distribution of multicast receivers in the network is very dense, with potential multicast receivers on each network segment. When an active multicast source appears, it diffuses the multicast packets received from the multicast source across the entire PIM routing network and then prunes the branches where no multicast receivers exist.

PIM-DM builds and maintains a unidirectional loop-free SPT (Source Specific Shortest Path Tree) connecting multicast sources and multicast receivers by periodically performing "Flooding - Prune." If, before the next "flooding - pruning," a pruned branch wishes to restore forwarding due to new multicast receivers joining on its last-hop router, it can proactively restore forwarding of multicast packets through the Graft mechanism.

The key working mechanisms of PIM-DM include neighbor discovery, flooding, prune, graft, and assert.

Neighbor Discovery

Neighbor discovery is achieved through periodic Hello messages sent between routers. When a router enables the PIM function, it will periodically send Hello messages on all its interfaces where

PIM is enabled. These messages contain necessary protocol parameter information for establishing and maintaining neighbor relationships between directly connected routers.

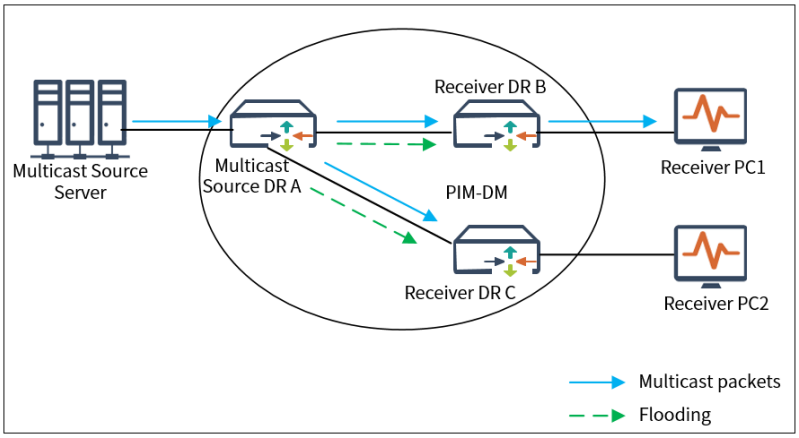
Hello messages are sent via multicast, usually to the multicast address 224.0.0.13, which is a dedicated multicast address for PIM routers. When neighboring routers receive these Hello messages, they confirm each other's neighbor identity and start exchanging PIM protocol information. This process ensures that PIM routers can discover other PIM routers within the same network segment and establish a stable neighbor relationship.

To maintain this neighbor relationship, the router will continuously listen for Hello messages from neighbors. If it does not receive a Hello message from a specific neighbor within the set time (usually called Holdtime), the neighbor relationship will be considered invalid, and the corresponding routing information will also be removed from the PIM routing table.

Diffusion (Flooding) Mechanism

When there is an active multicast source in the PIM-DM network, the multicast packets it sends will be flooded across the entire network. As shown in the figure below, when Router A (i.e., the Multicast Source DR A) receives a multicast packet sent by the multicast source Server, it performs an RPF (Reverse Path Forwarding, Reverse Path Forwarding) check based on the unicast routing table. If the RPF check passes, Router A will create a multicast routing (S, G) entry and include the interfaces connected to Router B (i.e., Receiver DR B) and Router C (i.e., Receiver DR C) in the downstream interface list. Subsequent incoming multicast packets will be forwarded to Routers B and C.

After Router B receives the multicast packet from Router A, it also performs an RPF check, creates the corresponding multicast route (S, G) table entry, and forwards the packet to the connected multicast receiver PC1. Meanwhile, after Router C receives the multicast packet from Router A, since there are no multicast receivers or PIM neighbors in its downstream network segment, Router C will prune this multicast path and stop forwarding the multicast packet. This process ensures the effective propagation of multicast packets in the network while avoiding unnecessary traffic through the pruning mechanism.



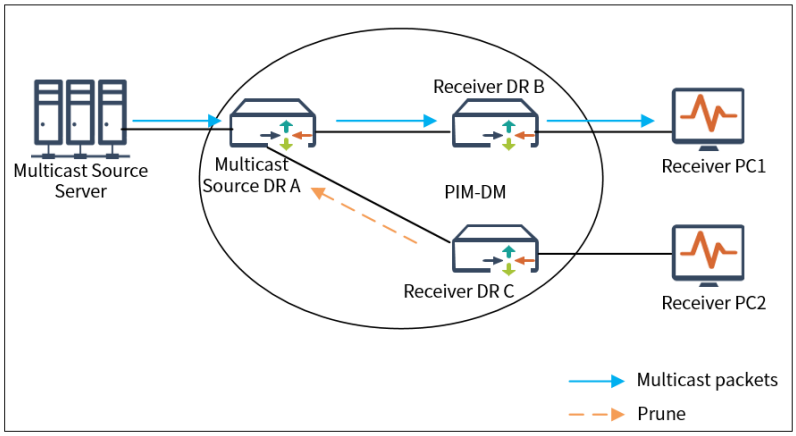
Pruning (Prune) Mechanism

When the PIM router receives a multicast packet and passes the RPF check, if it determines that there is no demand for multicast packets on the downstream network segment, the PIM router will send a prune message upstream. This notifies the upstream router to prohibit forwarding on the corresponding downstream interface and removes this interface from the downstream interface list of the multicast routing (S, G) table entry. The pruning operation is initiated by the last-hop router and proceeds hop-by-hop upstream, ultimately retaining only the branches connected to the multicast receivers in the multicast forwarding path.

The pruned downstream interfaces will start a pruning timer, and after timeout, the interface will restore the forwarding function so that newly joined multicast receivers can receive multicast packets. When there are no multicast receivers downstream, the last-hop router will initiate the pruning operation again. Through this periodic "Flooding - Prune" process, PIM-DM can periodically refresh the SPT. Additionally, if a downstream interface has been pruned and there is a new multicast receiver joining on the downstream last-hop router which expects to restore multicast packet forwarding before the next "Flooding - Prune", the grafting mechanism will be executed.

As shown in the figure below, when router C (i.e., the Receiver DR C) determines that there is no multicast packet demand in the downstream network segment, it sends a Prune message to router A (i.e., the Multicast Source DR A), notifying router A not to forward data to this downstream network segment anymore. When router A receives the Prune message, it stops forwarding data to this downstream interface and removes this downstream interface from the multicast routing (S, G) table entry. This process is referred to as pruning. Since router A still has other downstream interfaces in the forwarding state, router A continues to forward multicast packets to router B (i.e., the

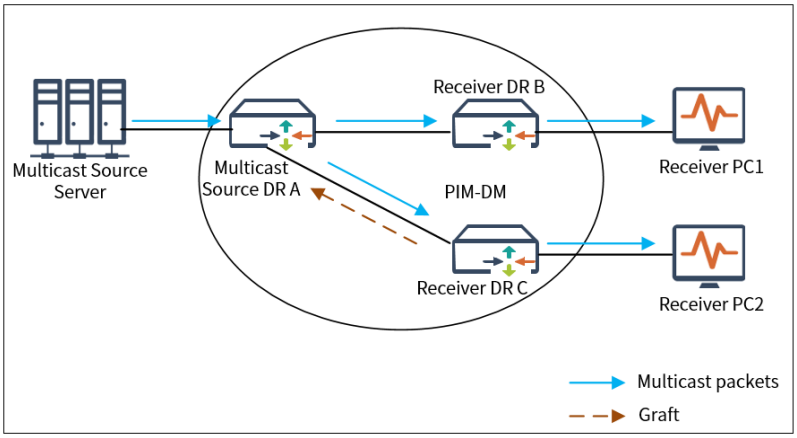
Receiver DR B), and subsequently arriving packets are only forwarded to router B, thereby achieving a unidirectional loop-free SPT connecting the multicast source and the multicast receiver.



Grafting Mechanism

The grafting mechanism in the PIM-DM protocol is designed to accelerate the process of new multicast receivers obtaining multicast data streams. When the last-hop router detects a new multicast receiver joining via the IGMP protocol, it sends a Graft message to the upstream router, requesting the restoration of forwarding the multicast data stream to this branch. After receiving the Graft message, the upstream router adds the corresponding interface to the downstream interface list of the multicast routing (S, G) table entry, thereby restoring the forwarding of the multicast data stream. This mechanism ensures that new multicast receivers can quickly receive multicast data without having to wait for the next periodic diffusion process.

As shown in the figure below, router C (i.e., the Receiver DR C) expects to restore the forwarding of multicast packets for receiver PC2 before the next "Flooding-Prune" cycle. Therefore, it sends a Graft message to its upstream router A (i.e., the Multicast Source DR A) to request the restoration of multicast packet forwarding on the corresponding outgoing interface. After receiving the Graft message, router A will restore the multicast packet forwarding on the outgoing interface connected to router C, ensuring that multicast packets can successfully reach router C through this downstream interface.



Assert Mechanism

The assertion mechanism is a part of the PIM protocol used to resolve potential conflict issues that may arise when multiple routers forward the same multicast packets to the same network segment. When multiple PIM routers forward multicast packets to the same segment, they send Assert messages to declare their forwarding priority. By comparing the size of IP addresses, an Assert Winner (i.e., the router with the larger IP address) is determined, and this router continues to forward multicast packets downstream while other routers (Assert Losers) stop forwarding. This mechanism ensures the uniqueness and validity of multicast packets in the network and allows for periodic reassessment and adjustment of forwarding rights.

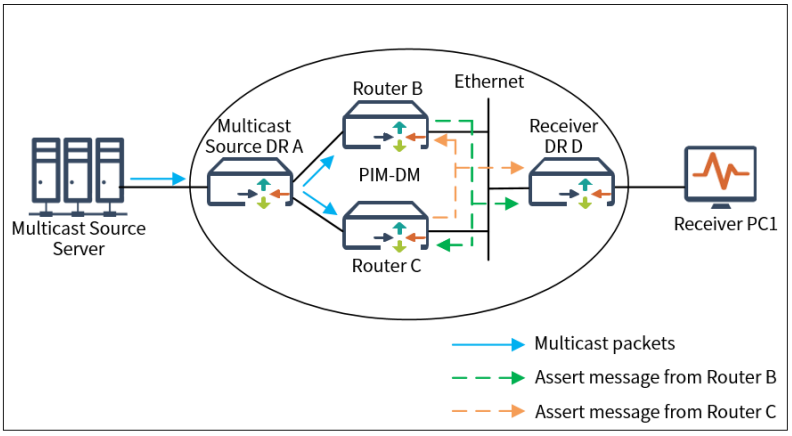
As shown in the figure below, Router B and Router C can both receive multicast packets from the multicast source Server, and both pass the RPF check, thereby creating multicast routing (S, G) entries in their respective routing tables. Since the downstream interfaces of Router B and Router C are both connected to the same network segment, they will attempt to simultaneously forward multicast data to that segment.

The assertion process is as follows:

1. Router B and router C receive multicast packets from each other's downstream interfaces. Since the RPF check fails for both, the packets will be discarded. At the same time, router B and router C send Assert messages to this network segment, respectively.

2. Router B compares its own IP address with the IP address carried in the Assert message sent by Router C. Since its IP address is larger, it wins. Subsequently, Router B continues to forward multicast packets to this network segment, and Router C still discards the packets after receiving the multicast packets due to RPF check failure.

3. Router C compares its own IP address with the IP address carried in the Assert message sent by Router B. Since its own IP address is smaller, it loses. Subsequently, Router C will stop forwarding multicast packets through this downstream interface and remove it from the downstream interface list of its own (S, G) entry.



Configuring Protocol Independent Multicast (PIM) Precautions

The configuration of PIM includes basic configuration and the configuration of PIM-SM/PIM-DM on different interfaces.

Notes:

- The PIM-SM and PIM-DM functions are mutually exclusive with the static multicast routing function or the IGMP Proxy function, respectively. Additionally, the PIM-SM and PIM-DM functions are also mutually exclusive and cannot be configured simultaneously.

- PIM-SSM function is on the basis of the PIM-SM function. Configure PIM-SM mode before configuring the PIM-SSM.
- In HA environment, PIM-SSM only supports Active-Passive (A/P) mode.
- The PIM-SM and PIM-DM functions can only be enabled on the Layer 3 interface.

Configuring Protocol Independent Multicast - Sparse Mode (PIM-SM) - WebUI

Before You Begin

- Read the "Configuring Protocol Independent Multicast (PIM)" on Page 473 introduction.
- Read the "Configuring Protocol Independent Multicast (PIM) Precautions" on Page 480.

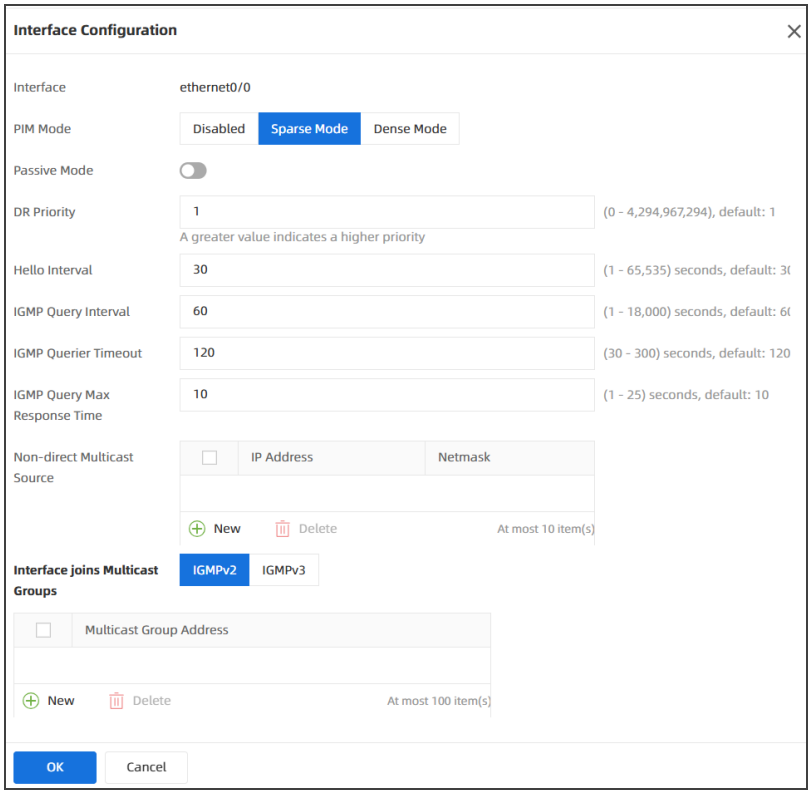
The configuration of Protocol Independent Multicast - Sparse Mode (PIM-SM) is divided into the following two parts:

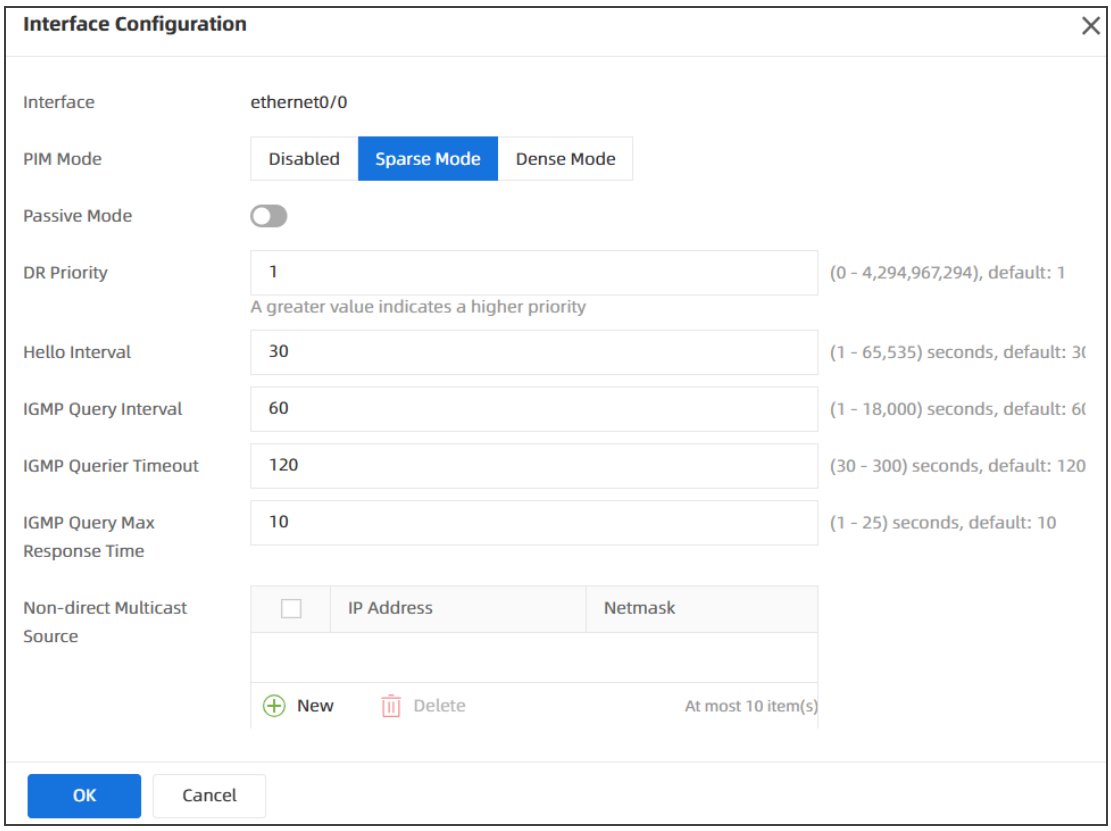
1. On the specified virtual router (VRouter), configure the PIM basic information and enable the PIM-SM function.
2. To configure the PIM-SM function on different interfaces.

Configuring PIM Basic Information and Enabling the PIM-SM Function

To configure PIM basic information and enable the PIM-SM function, take the following steps:

1. Select **Network** > **Routing** > **PIM**
2. Select a virtual router where the new PIM belongs from the **Virtual Router** drop-down list.
3. Select the **Configuration** tab to configure the basic information of PIM and enable the PIM-SM function.


Interface Configuration
Interface
ethernet0/0
PIM Mode
Disabled
Sparse Mode
Dense Mode
Passive Mode
DR Priority
1
(0 - 4,294,967,294), default: 1
A greater value indicates a higher priority
Hello Interval
30
(1 - 65,535) seconds, default: 3(
IGMP Query Interval
60
(1 - 18,000) seconds, default: 6(
IGMP Querier Timeout
120
(30 - 300) seconds, default: 120
IGMP Query Max Response Time
10
(1 - 25) seconds, default: 10
Non-direct Multicast Source
IP Address
Netmask
New
Delete
At most 10 item(s)
Interface joins Multicast Groups
IGMPv2
IGMPv3
Multicast Group Address
New
Delete
At most 100 item(s)
OK
Cancel


Interface Configuration
Interface
ethernet0/0
PIM Mode
Disabled
Sparse Mode
Dense Mode
Passive Mode
DR Priority
1
(0 - 4,294,967,294), default: 1
A greater value indicates a higher priority
Hello Interval
30
(1 - 65,535) seconds, default: 3(
IGMP Query Interval
60
(1 - 18,000) seconds, default: 6(
IGMP Querier Timeout
120
(30 - 300) seconds, default: 120
IGMP Query Max Response Time
10
(1 - 25) seconds, default: 10
Non-direct Multicast Source
IP Address
Netmask
New
Delete
At most 10 item(s)
OK
Cancel

On the Configuration tab, configure the following options.

Option	Description
Multicast Route	Turn on the switch button to enable global multicast routing.
PIM Mode	Specifies the "PIM Mode" to "Sparse Mode", which means enabling the PIM-SM function under this virtual router. **Tips:** If you do not need to enable the Protocol Independent Multicast (PIM) function under this virtual router, you can set the PIM mode to "Disabled".
Candidate RP	Select PIM devices in the PIM-SM domain to configure them as the candidate RP (Rendezvous Point). RP will be elected from the candidates. Candidate BSR should be configured at the same time and BSR will be elected from the candidate BSR (BootStrap Router). BSR is responsible for collecting and distributing RP information in the network. Candidate RP includes the following configuration: • Interface: Select the interface where the candidate RP resides from the drop-down list. The interface must be enabled with PIM-SM. • Interval: Specifies the interval for sending candidate RP messages. The range is 1 to 16,383 seconds. The default value is 60 seconds. • Priority: Specifies the priority. The smaller the value is, the higher the priority will be. In the RP election, the candidate

Option	Description
	RP with a higher priority will be elected as the RP. The range is 0 to 255 and the default priority is 0. **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is 224.0.0.0/4.
Candidate BSR	In a PIM-SM domain, you need to configure one or more candidate BSRs. BSR will be automatically generated among candidate BSRs. The BSR will collect and distribute the RP information. Candidate BSR includes the following configuration: • Interface: Select the interface where the candidate BSR resides from the drop-down list. The interface must be enabled with PIM-SM • Priority: Specifies the priority. The larger the value is, the higher the priority will be. If there is only one candidate BSR in the PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255 and the default priority is 0. **Notes:** When a dynamic RP is used, the candidate BSR must be configured and at least one candidate BSR must be configured in the PIM-SM domain.
Static RP	When there's only one Rendezvous Point (RP) in the network,

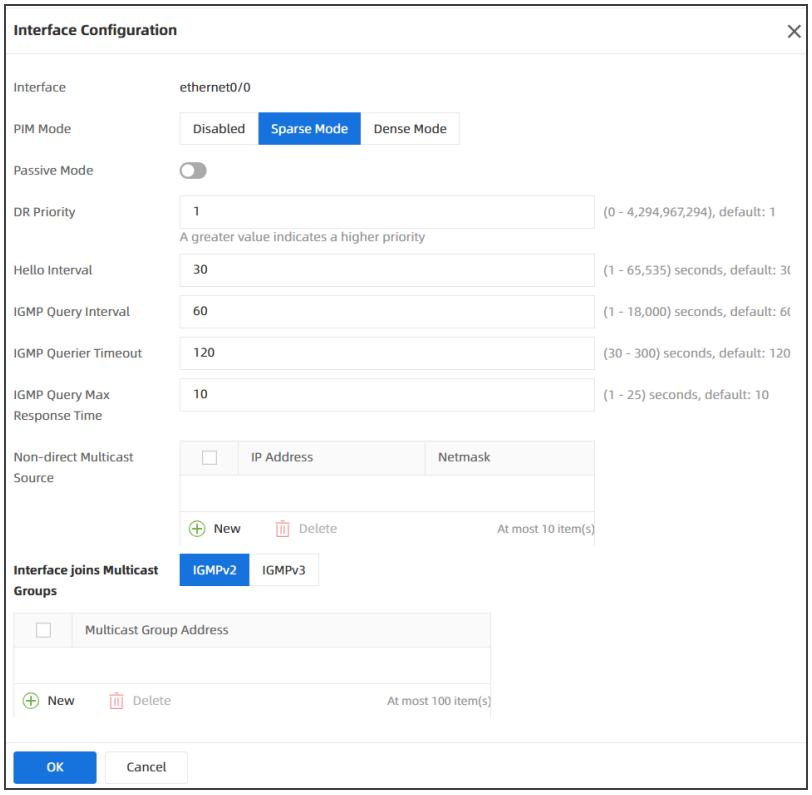
Option	Description
	you’re suggested to configure a static RP rather than a dynamic RP to save the bandwidth occupied by frequent message exchange between the Candidate RP and the BSR. In the PIM-SM domain, the static RP configured on all the devices should be the same. Click **New**. Enter the IP address of the interface where the static RP resides in the **Interface IP** textbox and the multicast address in the **Multicast Address** textbox.
RPT to SPT Switchover	Click the switch button to enable RPT to SPT Switchover. Since the RPT (Rendezvous Point Tree) in the PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.
PIM-SSM	By default, PIM-SSM is disabled. Click the switch button to enable PIM-SSM and specify the address range of PIM-SSM multicast group in the **Multicast Group Range** textbox. Ensure that the address range of PIM-SSM group configured on all PIM devices in the network are consistent. By default, the address range of PIM-SSM is 232.0.0.0/8.

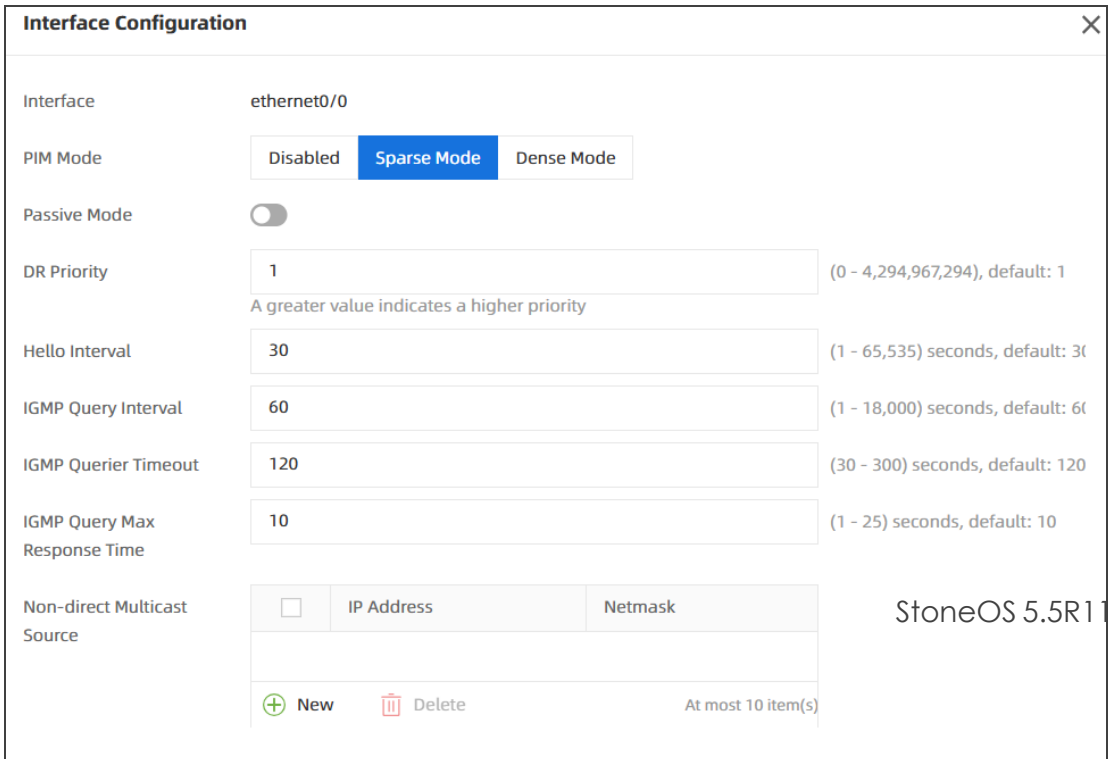
4. Click **OK**.
5. To delete configured PIM, select a virtual router from the **Virtual Router** drop-down list. Click Delete PIM to delete PIM configuration in this VR

Configuring PIM-SM on interfaces

To configure PIM-SM on interfaces, take the following steps:

1. Select **Network** > **Routing** > **PIM**.
2. Click **Interface Configuration** in the upper-right corner.
3. Double-click the interface or select the check box before the interface and click **Edit**.





Option	Description
Interface	Displays the name of the interface.
PIM Mode	Specifies the "PIM Mode" to "Sparse Mode", which means enabling the PIM-SM function on this interface. **Tips:** If you do not need to enable the Protocol Independent Multicast (PIM) function under this interface, you can set the PIM mode to "Disabled".
Passive Mode	Turn on the switch to enable the PIM passive mode of the interface. When the PIM-SM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets. The PIM passive mode is used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding. **Note:** • Before enabling this function, ensure that both the PIM-SM function and multicast routing function are enabled. • This function is only available to the PIM device interface

Option	Description
	directly connected to the user host segment, and only one PIM device can be connected to the segment. • After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.
DR Priority	Specifies the priority of DR. The larger the value is , the higher the priority will be. The default value is 1. The value range is 0 to 4,294,967,294. The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). All routers in the PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority is the same, the one with a larger IP address will be selected.
Hello Interval	With PIM-SM enabled, the interface periodically sends Hello packets. You can specify the interval for sending Hello packets on the interface as needed. The value range is 1 to 65,535 seconds. The default value is 30 seconds.
IGMP Query Interval	Specifies the interval for sending IGMP general query messages. The range is 1 to 18,000 seconds, and the default value is 60 seconds. The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain IGMP group membership of the interface. After the PIM-SM function is enabled for

Option	Description
	the interface, the querier will send IGMP general query messages to learn about the entry and exit of multicast group members.
IGMP Querier Timeout	Specifies the timeout value for IGMP general query. The range is 30 to 300 seconds, and the default value is 120 seconds. If the multicast router in the network does not receive IGMP general query messages within the specified timeout period, multicast routers will elect a querier again.
IGMP Query Max Response Time	Specifies the maximum response time for IGMP general query. The range is 1 to 25 seconds, and the default value is 10 seconds. You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the IGMP general query message twice and no response from the receiver host within the specified maximum response time, the system will delete this receiver in the multicast routing table.
Non-direct Multicast Source	Specifies the non-direct multicast source address. The system cannot establish the neighbor relationship with a multicast source as the muticast source DR across different network segments, and the muticast source DR will discard multicast packets whose network segment is different from the ingress interface. Therefore, you can configure the non-direct multicast source address to ensure that the multicast source DR and multicast source multicast across network segments when unicast routing of the multicast source is reachable for all PIM devices within the multicast domain. Click **New** and configure the multicast source address and subnet

Option	Description
	mask of non-direct multicast source. You can configure at most 10 non-direct multicast source entries. **Note**: Only root-VSYS supports to configure the multicast source address of non-direct multicast source.
Interface joins Multicast Groups	Configures the IGMP Join-group on the interface. This allows the interface of the system to join the multicast group and receive data traffic from the multicast group. You can configure at most 100 multicast groups. • IGMPv2: Select "IGMPv2" and configure the multicast group address. This way, the interface will join the specified multicast group over IGMPv2. • IGMPv3: Select "IGMPv3" and configure the multicast group address and multicast source address. This way, the interface will join the specified multicast group over IGMPv3. **Note**: To use the MSR function, you need to configure the IGMP Join-group function on the Vif interface.
Multicast Service Reflection	The MSR function supports to process multicast data forwarded to the Vif interface by converting the source address and multicast group address of the original multicast stream into a new multicast stream. When multicast traffic matches the ingress interface and pre-reflection destination IP address in the MSR entry, it can be converted to the post-reflection destination IP address and source IP address in the MSR entry. You can configure at most 100 MSR entries. To do this, click **New** and configure the following para-

Option	Description
	meters: • Ingress Interface: Select the ingress interface of the original multicast stream from the drop-down list. • Destination IP (Before Reflection): Specifies the multicast group address of the original multicast stream. • Destination IP (After Reflection): Specifies the post-reflection multicast group address. • mask (After Reflection): Specifies the post-reflection subnet mask of the multicast group address. • Source IP (After Reflection): Specifies the post-reflection multicast source address, which needs to be in the same network segment as the IP address of the Vif interface. **Note:** • Only root VSYS supports the MSR function. • When you use the MSR function, if unicast route performs route advertisement learning combined with the OSPF protocol, the OSPF network type on the Vif interface needs to be set to **point-to-point**. This allows the neighbor device to learn non-host routes. For more information about how to configure OSPF on the interface, see Configuring OSPF.

4. Click **OK**.

Configuring Protocol Independent Multicast - Dense Mode (PIM-DM) - WebUI

Before You Begin

- Read the "Configuring Protocol Independent Multicast (PIM)" on Page 473 introduction.
- Read the "Configuring Protocol Independent Multicast (PIM) Precautions" on Page 480.

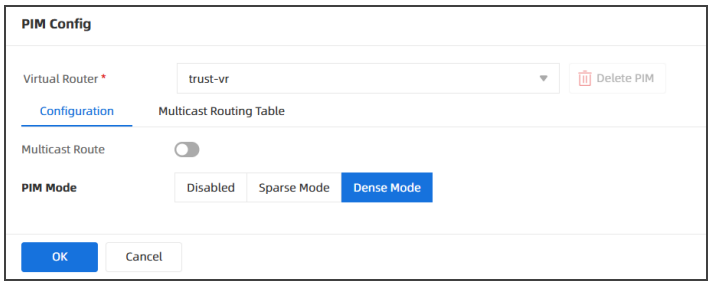
The configuration of Protocol Independent Multicast - Dense Mode (PIM-DM) is divided into the following two parts:

1. On the specified virtual router (VRouter), configure the basic PIM information and enable the PIM-DM function.
2. To configure the PIM-DM function on different interfaces.

Configuring PIM Basic Information and Enabling the PIM-DM Function

To configure PIM basic information and enable the PIM-DM function, take the following steps:

1. Select **Network** > **Routing** > **PIM**
2. Select a virtual router where the new PIM belongs from the **Virtual Router** drop-down list.
3. Select the **Configuration** tab to configure the basic information of PIM and enable the PIM-DM function.



Option	Description
Multicast Route	Turn on the switch button to enable global multicast routing.

Option	Description
PIM Mode	Specifies the "PIM Mode" to "Dense Mode", which means enabling the PIM-DM function under this virtual router. **Tips:** If you do not need to enable the Protocol Independent Multicast (PIM) function under this virtual router, you can set the PIM mode to "Disabled".

4. Click **OK**.

5. To delete configured PIM, select a virtual router from the **Virtual Router** drop-down list. Click Delete PIM to delete PIM configuration in this VR

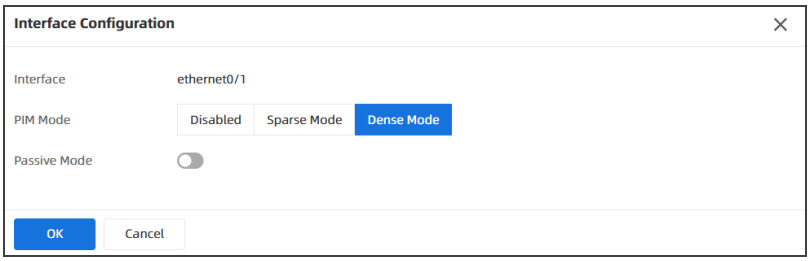
Configuring PIM-DM on interfaces

To configure the PIM-DM function on different interfaces, Take the following steps::

1. Select **Network** > **Routing** > **PIM**.

2. Click **Interface Configuration** in the upper-right corner.

3. Double-click the interface or select the check box before the interface and click **Edit**.



On the **Interface Configuration** page, configure the PIM-DM function for the interface.

Option	Description
Interface	Displays the name of the interface.
PIM Mode	Specifies the "PIM Mode" to "Dense Mode", which means enabling the PIM-DM function on this interface. **Tips:** If you do not need to enable the Protocol Independent Multicast (PIM) function under this interface, you can set the PIM mode to "Disabled".
Passive Mode	Turn on the switch to enable the PIM passive mode of the interface. When the PIM-DM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets. **Note:** • Before enabling this function, ensure that both the PIM-DM function and multicast routing function

Option	Description
	are enabled. • This function is only available to the PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment. • After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.

4. Click **OK**.

Viewing PIM Routing Information - WebUI

To view the multicast routing table, take the following steps:

1. Select **Network** > **Routing** > **PIM**.
2. Select a virtual router from the **Virtual Router** drop-down list.
3. Select the **Multicast Routing Table** tab to view the source address, multicast address, ingress interface, and egress interface of the multicast routing.

Configuring Protocol Independent Multicast - Sparse Mode (PIM-SM) - CLI

Before You Begin

- Read the "Configuring Protocol Independent Multicast (PIM)" on Page 473 introduction.
- Read the "Configuring Protocol Independent Multicast (PIM) Precautions" on Page 480.

The configuration of Protocol Independent Multicast - Sparse Mode (PIM-SM) is divided into the following two parts:

1. On the specified virtual router (VRouter), configure the PIM basic information and enable the PIM-SM function. The specific configuration includes:
    - Enabling/Disabling a Multicast Route (For details, see the Static Multicast Routing > Enabling/Disabling a Multicast Route section)
    - Enabling/Disabling the PIM-SM
    - Configuring a Candidate RP
    - Configuring a Candidate BSR
    - Configuring a Static RP
    - Configuring the Switchover to SPT
2. To configure the PIM-SM function on different interfaces. The specific configuration includes:
    - Enabling/Disabling the PIM-SM for Interfaces
    - Configuring the PIM Passive Mode of the Interface
    - Configuring the Priority of DR
    - Specifying the Interval for Sending the Hello Packets
    - Specifying the Interval for Sending IGMP General Query Messages.
    - Specifying the IGMP General Query Timeout

- Specifying the Maximum Response Time for IGMP General Query
- Specifying the Non-direct Multicast Source Address
- Configuring the Multicast Router Interface to Join the Multicast Group
- Configuring the MSR Function

Configuring PIM Basic Information and Enabling the PIM-SM Function

You can configure PIM-SM for different VRouter. To configure PIM basic information and enable the PIM-SM function must be configured in the PIM configuration mode. To enter the PIM configuration mode, in the global configuration mode, use the following commands:

ip vrouter*vrouter-name* (entering the VRouter configuration mode)

router pim(entering the PIM configuration mode)

Enabling/Disabling the PIM-SM

By default, the PIM-SM function is disabled. To enable or disable the PIM-SM function, in the PIM configuration mode, use the following commands:

- Enable: **pim-sm enable**
- Disable: **no pim-sm enable**

Configuring a Candidate RP

Select PIM devices in the PIM-SM domain to configure as the candidate RP (Rendezvous Point), and then the RP will be elected from the candidates. Configure the candidate BSR at the same time, and then the BSR will be elected from the candidate BSR (BootStrap Router), which is responsible for collecting and distributing the RP information in the network.

To configure the candidate RP, in the PIM configuration mode, use the following commands:

rp-candidate*interface-name* [**interval** *interval-time*] [**priority** *level*]

- *interface-name* – Specifies the interface where the candidate RP resides. The interface must be enabled with PIM-SM.
- *interval-time* – Specifies the interval for sending candidate RP messages. The range is 1 to 16383 seconds. The default value is 60 seconds.
- **priority** *level* – Specifies the priority (the smaller the value, the higher the priority). In the RP election, the candidate RP with the higher priority will be elected as the RP. The range is 0 to 255 and the default priority is 0.

To delete the configuration of candidate PR, in the PIM configuration mode, use the following command:

no rp-candidate

> **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is 224.0.0.0/4.

Configuring a Candidate BSR

In a PIM-SM domain, you need to configure one or more candidate BSR, and the BSR will be generated from the candidate BSR automatically. The BSR will collect and distribute the RP information.

To configure the candidate BSR, in the PIM configuration mode, use the following commands:

bsr-candidate*interface-name* [**priority** *level*]

- *interface-name* – Specifies the interface where the candidate BSR resides. The interface must be enabled with PIM-SM.
- **priority** *level* – Specifies the priority (the higher the value, the higher the priority). If there is only one candidate BSR in the PIM-SM domain, it will be become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255, the default priority is 0.

To delete the configuration of candidate BSR, in the PIM configuration mode, use the following command:

no bsr-candidate

> **Notes:** When a dynamic RP is used, the candidate BSR and at least one candidate BSR must be configured in the PIM-SM domain.

Configuring a Static RP

When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP, which can save the bandwidth occupied by message exchange between the Candidate RP and the BSR. In the PIM-SM domain, the static RP configured on all the devices should be the same.

To specify the address of static RP, in the PIM configuration mode, use the following commands:

rp-address*A.B.C.D* [*A.B.C.D/M*]

- *A.B.C.D* – Specifies the IP address of the interface where the static RP resides.
- *A.B.C.D/M* – Specifies the multicast address.

To delete the configured static RP address, in the PIM configuration mode, use the following command:

no rp-address*A.B.C.D* [*A.B.C.D/M*]

Configuring the Switchover to SPT

Since the RPT (Rendezvous Point Tree) in the PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.

Figure: Before RPT switch to SPT

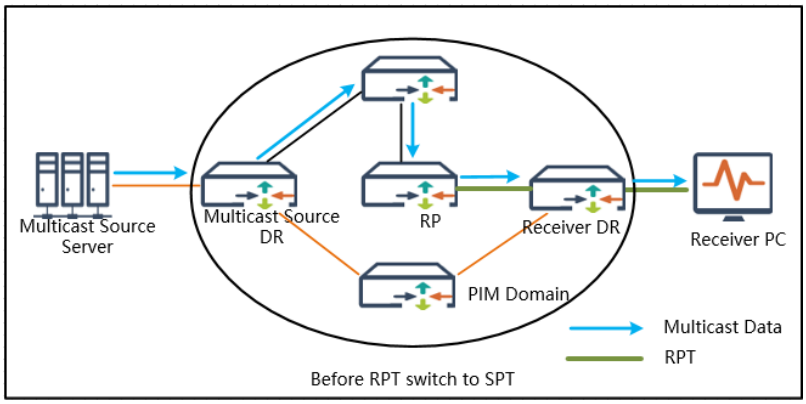
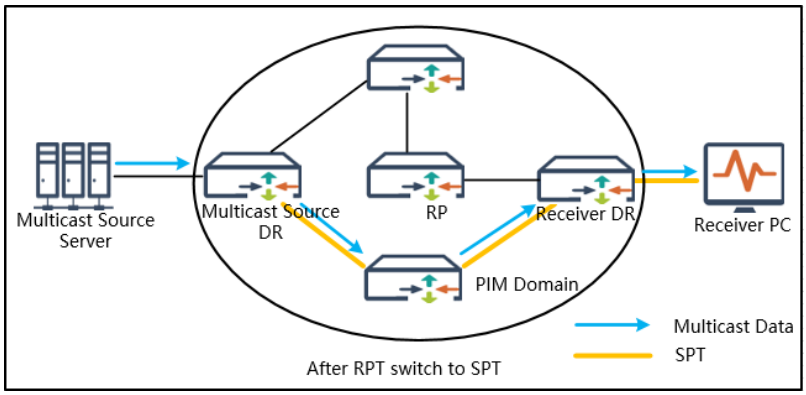


Figure: After RPT switch to SPT



To configure the switchover to SPT, in the PIM configuration mode, use the following commands:

spt-threshold {0 | **infinity**}

- 0 – Enable the switchover from RPT to SPT. This is the default option.
- **infinity** – Disable the switchover to SPT.

To restore the switchover to SPT, in the PIM configuration mode, use the following commands:

no spt-threshold

Configuring PIM-SM for Interfaces

The PIM-SM function for an interface must be configured in the interface configuration mode. The PIM-SM configurations for the interfaces include:

- Enabling/Disabling the PIM-SM for Interfaces
- Configuring the PIM Passive Mode of the Interface
- Configuring the Priority of DR
- Specifying the Interval for Sending the Hello Packets
- Specifying the Interval for Sending IGMP General Query Messages.
- Specifying the IGMP General Query Timeout
- Specifying the Maximum Response Time for IGMP General Query
- Specifying the Non-direct Multicast Source Address
- Configuring the Multicast Router Interface to Join the Multicast Group
- Configuring the MSR Function

Enabling/Disabling the PIM-SM for Interfaces

By default, the PIM-SM function for interface is disabled. To enable or disable the PIM-SM function for interface, in the interface configuration mode, use the following commands:

- Enable PIM-SM on the specified interface:**ip pim sparse-mode**
- Disable PIM-SM on the specified interface:**no ip pim sparse-mode**

Notes: The PIM-SM function only can be enabled on the Layer 3 interface.

Configuring the PIM Passive Mode of the Interface

When the PIM-SM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and

the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets.

The PIM passive mode is used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding.

Before you start

Before you configure the PIM passive mode of the interface, complete the following tasks:

- In interface configuration mode, use the **ip pim sparse-mode** command to enable the PIM-SM function of the interface.
- In VRouter configuration mode, use the **ip multicast-routing** command to enable the multicast routing function.

Notes

- This function is only available to the PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment.
- After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.

Procedure

By default, the PIM passive mode of the interface is disabled. To enable this mode, in interface configuration mode, use the following command:

ip pim passive

To disable this mode, in interface configuration mode, use the following command:

no ip pim passive

Check configuration results

After you configure the PIM passive mode of the interface, in interface configuration mode, you can use the **show this** command to view whether the configuration is successful.

Sample response:

```
hostname(config-if-eth0/3)#show this
interface ethernet0/3
ip pim passive
exit
```

Configuring the Priority of DR

The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). To specify the priority of DR, in the interface configuration mode, use the following commands:

ip pim dr-priority *level*

- *level* – Specifies the priority of the DR (the higher the value, the higher the priority). The default value is 1. The range is 0 to 4294967294. All routers in the PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority of the routers is the same, the one with a large IP address will be selected.

To restore the default priority, in the interface configuration mode, use the command**no ip pim dr-priority**.

Specifying the Interval for Sending the Hello Packets

After the PIM-SM function is enabled on an interface, Hello packets will be sent periodically. You can specify the interval for sending Hello packets on the interface as needed. In the interface configuration mode, use the following command:

ip pim query-interval *interval*

- *interval* – Specifies the interval for sending Hello packets. The range is 1 to 65535, and the default interval is 30 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim query-interval**.

Specifying the Interval for Sending IGMP General Query Messages

The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain IGMP group membership of the interface. On the Hillstone device, after the PIM-SM function is enabled for the interface, the querier will send IGMP general query messages to learn about the entry and exit of multicast group members.

To specify the interval for sending IGMP general query messages, in the interface configuration mode, use the following command:

ip pim igmp-query-interval *interval*

- *interval* – Specifies the interval for sending IGMP general query messages. The range is 1 to 18000 seconds, and the default value is 60 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-interval**.

Specifying the IGMP General Query Timeout

If the multicast router in the network does not receive IGMP general query messages within the specified timeout period, multicast routers will elect a querier again.

To specify the IGMP general query timeout value, in the interface configuration mode, use the following commands:

ip pim igmp-query-timeout *timeout-value*

- *timeout-value* – Specifies the IGMP general query timeout value. The range is 30 to 300 seconds, and the default value is 120 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-timeout**.

Specifying the Maximum Response Time for IGMP General Query

You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the IGMP general query message twice and no response from the receiver host within the specified maximum response time, system will delete the receiver in the multicast routing table.

To specify the maximum response time, in the interface configuration mode, use the following commands:

ip pim igmp-query-max-response-time*response-time*

- *response-time* – Specifies the maximum response time for IGMP general query. The range is 1 to 25 seconds, and the default value is 10 seconds.

To restore to the default interval, in the interface configuration mode, use the command**no ip pim igmp-query-max-response-time**.

Specifying the Non-direct Multicast Source Address

The system cannot establish the neighbor relationship with a multicast source as the muticast source DR across different network segments, and the muticast source DR will discard multicast packets whose network segment is different from the ingress interface. Therefore, you can configure the non-direct multicast source address to ensure that the multicast source DR and multicast source multicast across network segments when unicast routing of the multicast source is reachable for all PIM devices within the multicast domain.

To specify the non-direct multicast source address, in interface configuration mode, use the following command:

ip pim non-direct multicast source*source-address/netmask*

- *source-address/netmask* – Specifies the multicast source address and subnet mask of the non-direct multicast source.

To delete the multicast source address of the non-direct multicast source, use the **no ip pim non-direct multicast source***source-address/netmask* command.

Notes:

- Only root-VSYS supports to configure the multicast source address of non-direct multicast source.
- You can configure at most 10 non-direct multicast source entries.

Adding Multicast Router Interface to Multicast Group

In a multicast environment, multicast receivers indicate their interest of receiving multicast data by sending an IGMP report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. However, if the routers do not connect to multicast receivers or the connected multicast receivers cannot send an IGMP report, data from the source fails to reach the routers. To solve this issue, you can add the interface of multicast routers to the multicast group by configuring join-group. The interface can be added to a specified multicast group based on the IGMPv2 protocol or IGMPv3 protocol.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv2, run the following command in the interface configuration mode:

ip pim igmp join-group*group-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv2 protocol.

In the interface configuration mode, run the **no ip pim igmp join-group***group-address* command to remove the interface from the specified multicast group.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv3, run the following command in the interface configuration mode:

ip pim igmpv3 join-group*group-addresssource-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv3 protocol.

- *source-address* - Specifies the IP address of multicast source data traffic that the interface receives.

In the interface configuration mode, run the **no ip pim igmp join-group** *group-addresssource-address* command to remove the interface from the specified multicast group.

Notes:

- Only layer-3 interfaces can be added to the multicast group.
- To add an interface to the multicast group, the following requirements need to be met:
  - The PIM-SM function is enabled for the interface. For more information, refer to Enabling/Disabling the PIM-SM for Interfaces.
  - The device where the interface resides is receiver DR and has the highest priority. For more information about how to configure the priority of DR, refer to Configuring the Priority of DR.
  - The PIM-SM function is also enabled for the upstream device of the device where the interface resides.

Configuring the MSR Function

The Multicast Service Reflection (MSR) function supports to process multicast data forwarded to the Vif interface by converting the source address and multicast group address of the original multicast stream into a new multicast stream. When multicast traffic matches the ingress interface and pre-reflection destination IP address in the MSR entry, it can be converted to the post-reflection destination IP address and source IP address in the MSR entry.

To configure a MSR entry, in Vif interface configuration mode, use the following command:

ip service reflect *interface-name* **destination** *dst-address-before* **to** *dst-address-after* **mask-len** *mask-length* **source** *source-address-after*

- *interface-name* - Specifies the ingress interface of the original multicast stream.
- *dst-address-before* - Specifies the multicast group address of the original multicast stream.
- *dst-address-after* - Specifies the post-reflection multicast group address.
- *mask-length* - Specifies the post-reflection subnet mask of the multicast group address. Valid values: 0 to 32.
- *source-address-after* - Specifies the post-reflection multicast source address, which needs to be in the same network segment as the IP address of the Vif interface.

To delete the specified MSR entry, in interface configuration mode, use the following command:

no ip service reflect *interface-name* **destination** *dst-address-before* **mask-len** *mask-length*

Notes:

- Only root VSYS supports the MSR function.
- When you use the MSR function, if unicast route performs route advertisement learning combined with the OSPF protocol, the OSPF network type on the Vif interface needs to be set to **point-to-point** by using the **ip ospf network point-to-point** command. This allows the neighbor device to learn non-host routes.
- You can configure at most 100 MSR entries. To edit an existing MSR entry, the *interface-name*, *dst-address-before*, and *mask-length* fields need to keep unchanged. Otherwise, a new MSR entry is created.
- X-series devices do not support this function.

PIM-SSM

PIM-SM needs to maintain Rendezvous Points (RPs) to transmit multicast data. If receivers know the exact location of a multicast source and want to request multicast data directly from a multicast source, Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) can enable use hosts to rapidly join multicast groups. A shortest path tree (SPT) is set up between the multicast source

and group members without maintaining an RP. The multicast data will be forwarded to receivers along the SPT.

Configuring PIM-SSM

The basic configurations of PIM-SSM include:

- Enabling/Disabling a Multicast Route (For the details, refer to **Static Multicast Routing** > **Enabling/Disling a Multicast Route**)
- Configuring the range of PIM-SSM multicast group address

Notes:

- PIM-SSM function is on the basis of the PIM-SM function. Configure PIM-SM mode first before configuring the PIM-SSM (For details, refer to **Protocol Independent Multicast** > **Configuring PIM-SM**).
- In HA environment, PIM-SSM only supports Active-Passive (A/P) mode.

Configuring Address Range of PIM-SSM Multicast Group

By default, the address range of PIM-SSM is 232.0.0.0/8. You can configure the address range of the PIM-SSM multicast group as needed, and the address range of PIM-SSM group should be the same within the network. When the address range of PIM-SSM multicast group is configured, the PIM-SSM function will also be enabled.

To configure the address range of the PIM-SSM multicast group, in the PIM configuration mode, use the following command:

pim-ssm {**default** | *group-prefix/Mask* }

- **default** - Uses the default address range of PIM-SSM multicast group: 232.0.0.0/8.
- *group-prefix/Mask* - Specifies the address range of the certain PIM-SSM multicast group.

To delete the configured address range, in the PIM configuration mode, use the following command:

no pim-ssm

Configuring IGMP Packets Filtering

You can filter IGMP packets received form the interfaces with PIM-SM/PIM-SSM function enabled to allow or deny multicast source or multicast group in the certain IGMP packets. By default, all IGMP packets will be allowed to receive by interfaces.

To make interface allow or deny multicast group in the IGMPv1/IGMPv2 packets, in the interface configuration mode, use the following command:

ip pim igmp {**permit** | **deny**} *group-prefix/Mask*

- **permit**- Allow interfaces to receive multicast group in the IGMPv1/IGMPv2 packets.
- **deny**- Make the interface deny receiving multicast group in the IGMPv1/IGMPv2 packets.
- *group-prefix/Mask*- Specify the address range of multicast group.

To restore to the default values, in the interface configuration mode, use the following command:

noip pim igmp {**permit** | **deny**}

To make interface allow or deny multicast source and multicast group in the IGMPv3 packets, in the interface configuration mode, use the following command:

ip pim igmpv3 {**permit** | **deny**} {**any** |*source-prefix/Mask*}{**any** |*group-prefix/Mask*}

- **permit**- Allow the interface to receive multicast source and multicast group in the IGMPv3 packets.
- **deny**- Make the interface deny receiving multicast source and multicast group in the IGMPv3 packets.
- **any** |*source-prefix/Mask*- Specify the address range of multicast source. **any** is for any multicast source address.

- **any** | *group-prefix/Mask* - Specify the address range of multicast group. **any** is for any multicast group address.

To restore to the default values, in the interface configuration mode, use the following command:

noip pim igmpv3 {**permit** | **deny**}

Configuring Protocol Independent Multicast - Dense Mode (PIM-DM) - CLI

Before You Begin

- Read the "Configuring Protocol Independent Multicast (PIM)" on Page 473 introduction.
- Read the "Configuring Protocol Independent Multicast (PIM) Precautions" on Page 480.

The configuration of Protocol Independent Multicast - Dense Mode (PIM-DM) is divided into the following two parts:

1. On the specified virtual router (VRouter), configure the basic PIM information and enable the PIM-DM function. The specific configuration includes:
    - Enabling/Disabling a Multicast Route (For details, see the Static Multicast Routing > Enabling/Disabling a Multicast Route section)
    - Enabling/Disabling the PIM-DM
2. To configure the PIM-DM function on different interfaces. The specific configuration includes:
    - Enabling/Disabling the PIM-DM for Interfaces
    - Configuring the PIM Passive Mode of the Interface

Configuring PIM Basic Information and Enabling the PIM-DM Function

You can configure PIM-DM for different VRouter. To configure PIM basic information and enable the PIM-DM function must be configured in the PIM configuration mode. To enter the

PIM configuration mode, in the global configuration mode, use the following commands:

ip vrouter*vrouter-name* (entering the VRouter configuration mode)

router pim(entering the PIM configuration mode)

Enabling/Disabling the PIM-DM

： By default, the PIM-DM function is disabled. To enable or disable the PIM-DM function, in the PIM configuration mode, use the following commands:

- Enable: **pim-dm enable**
- Disable: **no pim-dm enable**

Configuring PIM-DM for Interfaces

The PIM-DM function for an interface must be configured in the interface configuration mode. The PIM-DM configurations for the interfaces include:

- Enabling/Disabling the PIM-DM for Interfaces
- Configuring the PIM Passive Mode of the Interface

Enabling/Disabling the PIM-DM for Interfaces

默认情况下，接口的PIM-DM功能为关闭状态。用户可以在接口配置模式下，使用以下命令，开启或关闭指定接口的PIM-DM功能：

By default, the PIM-DM function for interface is disabled. To enable or disable the PIM-DM function for interface, in the interface configuration mode, use the following commands:

- Enable PIM-DM on the specified interface: **ip pim dense-mode**
- Disable PIM-SM on the specified interface: **no ip pim dense-mode**

Notes: The PIM-DM function only can be enabled on the Layer 3 interface.

示例：

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/3)# zone trust
hostname(config-if-eth0/3)# ip address 1.1.1.1 255.255.255.0
hostname(config-if-eth0/3)# ip pim dense-mode
```

Configuring the PIM Passive Mode of the Interface

When the PIM-DM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets.

Before you start

Before you configure the PIM passive mode of the interface, complete the following tasks:

- In interface configuration mode, use the **ip pim dense-mode** command to enable the PIM-DM function of the interface.
- In VRouter configuration mode, use the **ip multicast-routing** command to enable the multicast routing function.

Notes

- This function is only available to the PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment.
- After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.

Procedure

By default, the PIM passive mode of the interface is disabled. To enable this mode, in interface configuration mode, use the following command:

ip pim passive

To disable this mode, in interface configuration mode, use the following command:

no ip pim passive

Check configuration results

After you configure the PIM passive mode of the interface, in interface configuration mode, you can use the **show this** command to view whether the configuration is successful.

Sample response:

```
hostname(config-if-eth0/3)#show this
interface ethernet0/3
ip pim passive
exit
```

Viewing PIM Information - CLI

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

show ip pim bsr-route [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the BSR information of VRouter.

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

show ip pim interface [*interface-name*]

- *interface-name* - Shows the PIM information of the specified interface.

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

show ip pim neighbor [**vrouter** *vrouter-name*]

- *vrouter-name* - Shows the PIM neighbor information of the specified VRouter.

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

show ip pim rp [**vrouter** *vrouter-name* | **mapping** [**vrouter** *vrouter-name*]]

- *vrouter-name* - Shows the RP information of the specified VRouter.
- **mapping** [**vrouter***vrouter-name*] - Shows all RP mapping information of the specified VRouter.

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

show ip pim rpf*source-address* [**vrouter** *vrouter-name*]

- *source-address* – Shows the RPF information of the specified multicast source IP address.
- *vrouter-name* - Shows the RPF information of the multicast source IP address of the specified VRouter.

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

show ip pim igmp groups [*group-address* [**vrouter** *vrouter-name*]]

- *group-address* – Shows the IGMP multicast group information of the specified IP address.
- **vrouter** *vrouter-name* – Shows the IGMP multicast group information of the specified VRouter.

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

show ip pim igmp interfaces [*interface-name*]

- *interface-name* – Shows the IGMP information of the specified interface (the interface enabled with PIM-SM/PIM-DM).

CloudEdge supports enabling/disabling the Record TOA function for SNAT rule

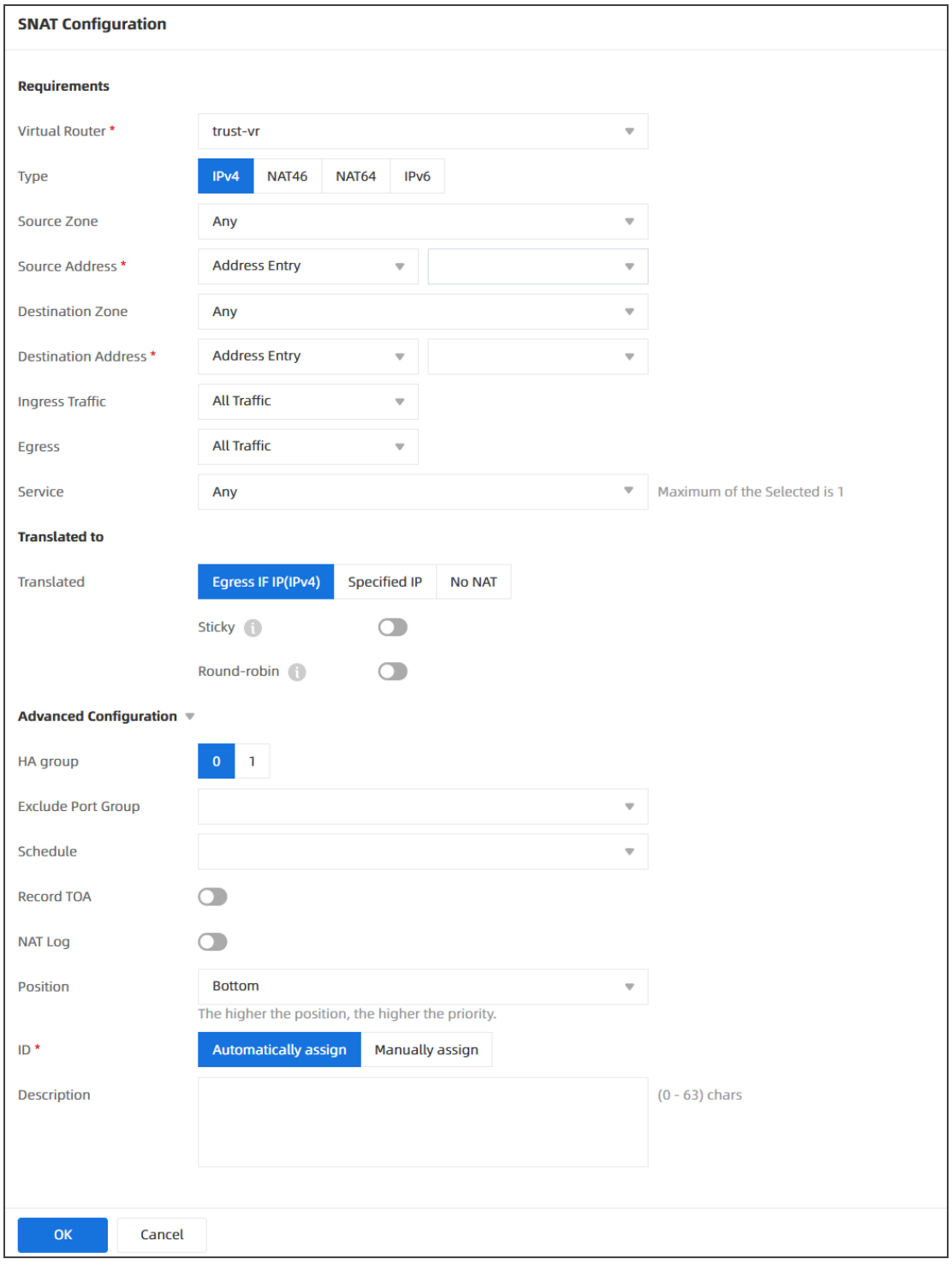
WebUI

Configuring SNAT

To create an SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Click **New** to open the SNAT Configuration page.



In this page, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the SNAT rule. The SNAT rule will take effect when the traffic flows into this VRouter and matches the SNAT rule conditions.
Type	Specifies the type of the SNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of SNAT rules may vary in this page, please refer to the actual page.
Source Zone	Specifies the security zone to which the ingress interface of traffic that matches the SNAT rule is bound. By default, Any is selected. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the SNAT rule. **Note:** The source zone needs to belong to the specified virtual router.
Source Address	Specifies the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46.

Requirements	
	• IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the SNAT rule is NAT64 or IPv6.
Destination Address	Specifies the destination IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the SNAT rule is NAT64 or IPv6.
Ingress Traffic	Specifies the ingress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the ingress traffic. Traffic from any ingress interfaces will continue to match this SNAT rule. • Ingress Interface - Specifies the ingress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will con-

Requirements	
	tinue to match this SNAT rule, while traffic from other interfaces will not.
Egress	Specifies the egress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the egress traffic. Traffic from all egress interfaces will continue to match this SNAT rule. • Egress Interface - Specifies the egress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not. • Next Virtual Router - Specifies the next virtual router of traffic. Select a virtual router from the drop-down list.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **New Service** or **New Group**.
Translated to	
Translated	Specifies the translated NAT IP address, including: • Egress IF IP (IPv4)/Egress IF IP (IPv6) - Specifies the NAT IP address to be an egress interface IP address. • Specified IP - Specifies the NAT IP address to be a specified IP address. After selecting this option, continue to specify the available IP address in the **Address** drop-down

Requirements	
	list. • No NAT - Do not implement NAT. The translated action for different types of SNAT rules may vary in this page, please refer to the actual page.
Mode	Specifies the translation mode, including: • Static - Static mode means one-to-one translation. This mode requires the translated address entry to contain the same number of IP addresses as that of the source address entry. • Dynamic IP - Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied. • Dynamic port - Called PAT. Multiple source addresses will be translated to one specified IP address in an address entry. • If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Sticky to enable Sticky. • If Round-robin is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Round-robin to enable Round-robin. • If Sticky and Round-robin are not enabled, the first

Requirements	
	address in the address entry will be used first; when the port resources of the first address are exhausted, the second address will be used. • If Track is enabled, the system will track whether the translated public address is valid, i.e., use the translated address as the source address to track if the destination website or host is accessible. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see Track Object. This function only supports SNAT of IPv4 or NAT64 type, and the translated address should be an IP address or an address in address book, as well as the translation mode is dynamicport mode. The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log. Click the **Enable** button behind Track to enable the function, and select a

Requirements	
	track object from the drop-down list • NPTv6: Select the NPTv6 mode. NPTv6 (IPv6-to-IPv6 Network Prefix Translation) is described in RFC 6296 and used to implement NAT66. When this mode is selected, NPTv6 can translate an inside IPv6 source address prefix to outside IPv6 source prefix in IPv6 packet header. The translation is based on the algorithm described in RFC 6296, which serves as a useful mechanism for implementing address independence. This mode supports a larger number of address translation and reduces resource consumption by using quick address mapping. **Note:** The Sticky function and the Round-robin function are mutually exclusive and cannot be configured at the same time. **Notes:** • The NPTv6 mode is available only when the Type parameter is set to IPv6 and the Translated parameter is set to Specified IP. • The NPTv6 mode requires that both the source address of the traffic and the translated address are either "IPv6/prefix" or address from address book. • If the source address of the traffic and the translated address are "IPv6/prefix", the

Requirements	
	IPv6 prefix needs to be 8 to 64 in length. • If the source address of the traffic and the translated address are address from address book, you can only configure one IPv6 sub-net mask member whose subnet mask is 8 to 64 in length.

Expand Advanced Configuration, configure the corresponding options.

Option	Description
HA Group	Specifies the HA group that the SNAT rule belongs to. The default setting is 0.
Exclude Port Group	Select an exclude port group that you want to bind from the drop-down list. After you bind the exclude port group to the specified SNAT rule, this SNAT rule will exclude port numbers specified in the port group. For more information about how to create an exclude port group, see Port Group. **Notes:** The exclude port group bound to SNAT rule has a higher priority than the exclude port group bound to VRouter.
Schedule	Specifies the schedule of the SNAT rule. Select a schedule from the drop-down list. In addition, fuzzy search is supported. To create a schedule, click ⊕.
Recode TOA	Click the "Enable" button to enable the Recode TOA (TCP Options Address) function for this SNAT rule. TOA is an optional field in the TCP protocol. Enabling this function in a source network address translation (SNAT) environment will cause the system to automatically embed the pre-conversion client address information into the TOA field of the non-retransmitted ACK packet during the third handshake of the TCP three-way handshake process. This allows the server to obtain the client's real IP and port before SNAT conversion through

Option	Description
	this field, thus more efficiently identifying and processing requests from the client. This function is disabled by default. **Notes:** • Only CloudEdge supports this function. • Network environments without NAT translation do not support this function. • NAT46 and NAT64 rules do not support this function. • HA peer-mode does not support this function.
NAT Log	Click the Enable button to enable the log function for this SNAT rule. The system will generate log information when there is traffic matching this NAT rule. **Note**: If the translated NAT IP address is an egress interface IP address, it is necessary to specify the egress interface of the traffic at the same time in order to generate logging information.
Position	Specifies the position of the rule. Each SNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all the rules in the SNAT rule list. By default, system will put the

Option	Description
	newly-created SNAT rule at the bottom of all SNAT rules. • Top - The rule is located at the top of all the rules in the SNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specifies the method you get the rule ID. Each rule has its unique ID. It can be automatically assigned by system or manually assigned by yourself. If you select **Manually assign** , type an ID number into the box behind.
Description	Types the description.

3. Click **OK** to save the settings.

Notes:

- When configuring a static source NAT66 rule, the minimum subnet mask must be 48 bits.
- If the SNAT rule is configured with a source zone or destination zone that is not Any, the zone cannot be deleted.

For more information, see the **Policy> NAT > Configuring SNAT** section in the *StoneOS WebUI User Guide*. FR 40674

CLI

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT on the source IP address of the matched traffic. If NAT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] [**ingress-interface** *interface-name*] [**from-zone** *zone-name*] [**to-zone** *zone-name*] **from** *src-address* **to** *dst-address* [**service** *service-name*] [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip** | **eif-ipv6**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**] | **nptv6**} [**log**] [**group** *group-id*] [**disable**] [**track** *track-name*] [**description** *description*] [**schedule** *schedule-name*] [**record-toa**]

- **id** *id* – Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.
- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be top, before id or after id. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.
- **ingress-interface** *interface-name* – Specifies the ingress interface of the SNAT rule. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, and traffic from other interfaces will not.
- **from-zone***zone-name* – Specifies the security zone to which the ingress interface of traffic that matches the SNAT rule is bound. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the SNAT rule. By default, the parameter is set to **Any**.

  Note:

- The source zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
- Only one source zone can be configured for an SNAT rule.

- **to-zone***zone-name* – Specifies the security zone to which the egress interface of traffic that matches the SNAT rule is bound. After the configuration is completed, only the traffic that flows through the interface bound to this security zone can continue to match the SNAT rule. By default, the parameter is set to **Any**.
  Note:
  - The destination zone must belong to the specified virtual router. In NAT configuration mode, VRouter is **trust-vr**.
  - Only one destination zone can be configured for an SNAT rule.
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions include:
  - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book(IPv4 type or IPv6 type).
  - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IP address (IPv4 type or IPv6 type) or an address entry in the address book (IPv4 type or IPv6 type).
  - **service** *service-name* – Specifies the service type of the traffic. *service-name* should be a service defined in the service book.
  - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.

- **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip** | **eif-ipv6**} – Specifies the translated IP address. It can be an ipv4 address, IPv6 address, an address entry in the address book or the address of the egress interface (**`eif-ip`** or **eif-ipv6**).

- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky** | **round-robin**] | **nptv6**} – Specifies the translation mode. StoneOS supports four translation modes: static, dynamicip, dynamicport, and nptv6. For more details, see the table below:

Mode	Description
static	Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same number of IP addresses as that of the source address entry (*src-address*). **Notes:** When configuring a static source NAT66 rule, the minimum subnet mask must be 48 bits.
dynamicip	Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
dynamicport	Namely PAT. Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. If Round-robin, all sessions from an IP address will be polled to map the IP address. If Sticky and Round-robin are not enabled, the system will select an IP address in the address entry, when port resources of the first address are exhausted, the second address will be used. **Note**: Sticky function and Round-robin function are mutually exclusive and cannot be configured at the same time.

Mode	Description

nptv6	NPTv6 (IPv6-to-IPv6 Network Prefix Translation) is described in RFC 6296 and used to implement NAT66. When this mode is selected, NPTv6 can translate an inside IPv6 source address prefix to outside IPv6 source prefix in IPv6 packet header. The translation is based on the algorithm described in RFC 6296, which serves as a useful mechanism for implementing address independence. This mode supports a larger number of address translation and reduces resource consumption by using quick address mapping.
	
	Notes:
	• The NPTv6 mode is available only when the Type parameter is set to IPv6 and the Translated parameter is set to Specified IP.
	• The NPTv6 mode requires that both the source address of the traffic and the translated address are either "IPv6/prefix" or address from address book.
	  • If the source address of the traffic and the translated address are "IPv6/prefix", the IPv6 prefix needs to be 8 to 64 in length.
	  • If the source address of the traffic and the translated address are address from address book, you can only configure one IPv6 subnet mask member whose subnet mask is 8 to 64 in length.

- **log** – Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule). **Note**: If the translated NAT IP address is an egress interface IP address (**eif-ip** or **eif-ipv6**), it is necessary to specify the egress interface of the traffic (**eif** *egress-interface*) at the same time in order to generate logging information.
- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.
- **disable** – Enter this command to disable the SNAT rule.
- **track** *track-name* – Specifies a track object name that is configured in the system. After configuring this option, the system will track whether the translated public address is valid. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see Configuring a Track Object of System Management. This function only supports dynamicport mode, and the translated address should be an IP address or an address in address book (i.e., **trans-to address book** *trans-to-address*). The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log.
- **description** *description* – Specifies the description for this SNAT rule. You can specify at most 63 characters.
- **schedule***schedule-name* – Specifies the schedule for the SNAT rule.
- **record-toa** - Enable the Recode TOA (TCP Options Address) function for this SNAT rule. TOA is an optional field in the TCP protocol. Enabling this function in a source network address translation (SNAT) environment will cause the system to automatically embed the pre-

conversion client address information into the TOA field of the non-retransmitted ACK packet during the third handshake of the TCP three-way handshake process. This allows the server to obtain the client's real IP and port before SNAT conversion through this field, thus more efficiently identifying and processing requests from the client. This function is disabled by default.

Notes:

- Only CloudEdge supports the Recode TOA function .
- Network environments without NAT translation do not support the Recode TOA function .
- NAT46 and NAT64 rules do not support the Recode TOA function.
- HA peer-mode does not support this function.

For example, you can use the following command to implement SNAT translation. If traffic over the internal network accesses the Internet, the traffic will be SNATed based on the security zone to which the ingress interface of the traffic is bound and the security zone to which the egress interface of the traffic is bound.

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from-zone trust to-zone untrust from ip 192.168.2.23 to 1.1.12.3 trans-to ip 1.1.10.6 mode static
 (trust is the security zone to which the ingress interface of traffic that matches the SNAT rule is bound, untrust is the security zone to which the egress interface of traffic that matches the SNAT rule is bound, 192.168.2.23 is the source IP address, 1.1.12.3 is the destination IP address, and 1.1.10.6 is the SNATed source IP address.)
 (SNAT translation: If traffic over the internal network accesses the Internet from 192.168.2.23 to 1.1.12.3, when the traffic matches the SNAT rule, the source address is converted to 1.1.10.6 and the destination address remains unchanged.)
```

```
snat service not set, set to default Any
rule ID=1
```

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# snatrule from any to any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT, in the NAT configuration mode, use the following command:

For more information, refer to the **Firewall** > **NAT** > **Configuring a NAT Rule** section in *StoneOS CLI User Guide*. FR 40674

Creating an SNAT Rule

SNAT rules are used to specify whether to implement NAT-PT on the source IPv6/IPv4 address of the matched traffic. If NAT-PT is implemented, you also need to specify the translated IP address and translation mode. To configure an SNAT rule for NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip** | **eif-ipv6**} **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**] [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*] } [**log**] [**group** *group-id*] [**description** *description*] [**record-toa**]

- **id** *id* – Specifies the ID of the SNAT rule. Each SNAT rule has a unique ID. If the ID is not specified, the system will automatically assign one. If the specified SNAT ID exists, the original rule will be overwritten.

- **before** *id* | **after** *id* | **top** – Specifies the position of the rule. The position can be **before** *id*, **after** *id*, **top**. If the position is not specified, the rule would be located at the end of all the SNAT rules. By default, the newly-created SNAT rule is located at the end of all the rules.
- **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] – Specifies conditions of the rule that the traffic should be matched. The conditions include:
  - **from** *src-address* - Specifies the source IP address of the traffic. *src-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **to** *dst-address* - Specifies the destination IP address of the traffic. *dst-address* should be an IPv4 address, IPv6 address or an address entry in the address book.
  - **eif** *egress-interface* | **evr** *vrouter-name* - Specifies the egress interface (**eif** *egress-interface*) or the next-hop VRouter (**evr** *vrouter-name*) of the traffic.
- **trans-to** {**ip** *ip-address* | **addressbook** *trans-to-address* | **eif-ip**| **eif-ipv6**} – Specifies the translated IP address. It can be an IPv4 or IPv6 address, an address entry in the address book, the IP address of the egress interface (**eif-ip**), or the IPv6 address of the egress interface (**eif-ipv6**). When you configure the NAT46, system does not support to specifies the **eif-ip**. When you configure the NAT64, system does not support to specifies the **eif-ipv6**..
- **mode** {**static** | **dynamicip** | **dynamicport** [**sticky**] [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*] } – Specifies the translation mode. StoneOS supports three modes for the translation between IPv4 and IPv6 addresses: static, dynamicip and dynamicport. For more details, see the table below:
  - **static** - Static mode means one-to-one translation. This mode requires the translated address entry (*trans-to-address*) contains the same number of IP addresses as that of the source address entry (*src-address*).

- **dynamicip** - Dynamic IP mode means many-to-many translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
- **dynamicport** - Namely NAPT-PT (Network Address Port Translation - Protocol Translation). Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is not enabled, the system will select an IP address in the address entry, when port resources of the first address are exhausted, the second address will be used. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. When configuring the SNAT rule of NAT64, you can specify the static port block mapping mode by configuring [**fixed-block start** *start-port* **end** *end-port* **size** *port-block-size*. The static port block mapping mode means each source IP address corresponds to a fixed port block of the mapped IP. **start** *start-port* **end** *end-port* specifies the start port and end port of the available port range. The value range is 1024 to 65535. **size** *port-block-size* specifies the size of the port block. The value range is 64 to 64512, and the value must be the integer multiple of 64.

- **log** − Enables the log function for this SNAT rule (Generating a log when the traffic is matched to this NAT rule).
- **group** *group-id* - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0.
- **description***description* - Specifies the description for this SNAT rule. You can specify at most 63 characters.
- **record-toa** - Enable the Recode TOA (TCP Options Address) function for this SNAT rule. TOA is an optional field in the TCP protocol. Enabling this function in a source network address translation (SNAT) environment will cause the system to automatically embed the pre-conversion client address information into the TOA field of the non-retransmitted ACK packet

during the third handshake of the TCP three-way handshake process. This allows the server to obtain the client's real IP and port before SNAT conversion through this field, thus more efficiently identifying and processing requests from the client. This function is disabled by default.

Notes:

- Only CloudEdge supports the Recode TOA function .
- Network environments without NAT translation do not support the Recode TOA function .
- NAT46 and NAT64 rules do not support the Recode TOA function.
- HA peer-mode does not support this function.

For example, the following example achieves the interface-based NAT of ethernet0/0 in the untrust zone:

```
hostname(config-vrouter)# snatrule from ipv6-any to ipv6-any eif ethernet0/0 trans-to eif-ip mode dynamicport
rule id=1
```

To configure an SNAT rule that disables NAT-PT, in the VRouter configuration mode, use the following command:

snatrule [**id** *id*] [**before** *id* | **after** *id* | **top**] **from** *src-address* **to** *dst-address* [**eif** *egress-interface* | **evr** *vrouter-name*] **no-trans** [**group** *group-id*]

For more information, refer to the **IPv6 > Configuring NAT-PT** section in *StoneOS CLI User Guide*. FR 40674

CloudEdge supports switching IPv4/IPv6 virtual IP via Huawei Cloud Platform API to achieve HA switching in IPv4/IPv6 scenarios

WebUI

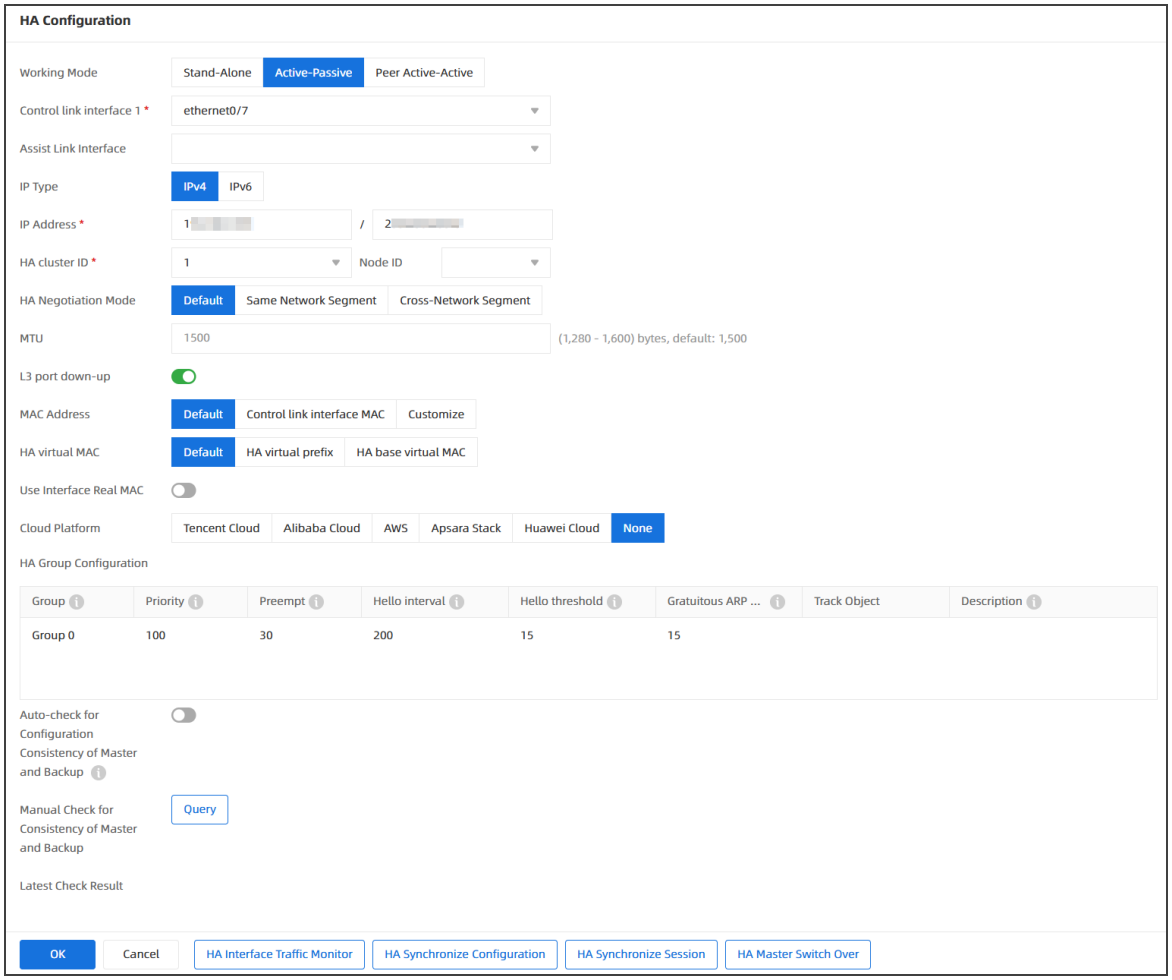
Configuring HA Active-Passive (A/P) Mode

The main configuration steps of the HA Active-Passive (A/P) mode include:

1. Configure an HA Virtual Forward Interface. For more information on configuring the interface, see Configuring an Interface.
2. Configure the HA working mode as Active-Passive.
3. Configure the HA link, including an HA link interface and an HA link IP address, for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the HA VMAC prefix(optional) , HA cluster ID and HA node ID to enable the HA function.
5. Configure an HA group. Specify the priority for devices (for selecting the master) and HA messages parameters.

To configure HA Active-Passive (A/P) mode, take the following steps:

1. Go to **System > HA**.
2. Select the HA working mode as Active-Passive, which means that one device in the HA cluster works in active mode and the other works in backup mode.



Configure HA Active-Passive (A/P) mode.

Option	Description
Control link interface 1	Specifies the name of the HA control link interface 1. The control link interface is used to synchronize all data between two devices.
Control link interface 2	Specifies the name of HA control link interface 2 (Backup interface). **Note**: You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.
Control link	X-seriesK20803 devices by default use the interface on the System

Option	Description

interface 1, 2, 3, 4	Control Modules (SCMs) as HA control link interface. These control link interfaces cannot be deleted or modified. To configure the HA link interface of X-seriesK20803 devices, you need to pay attention to the following
	• You can only synchronize the data information through HA date link interface.
	• By default, all HA interfaces (HA0 and HA1) of SCMs will be configured as the the HA control link automatically, and you don't need to configure. To connect the HA control link, take the following methods
	  • Connect the HA0 of master SCM on the master device with the HA0 of the master SCM on the backup device.
	  • Connect the HA1 of master SCM on the master device with the HA0 of the backup SCM on the backup device.
	  • Connect the HA0 of backup SCM on the master device with the HA1 of the master SCM on the backup device.
	  • Connect the HA1 of backup SCM on the master device with the HA1 of the backup SCM on the backup device.

Control link	Specifies the name of interface on I/O modules as the HA control

Option	Description
interface 5	link interface 5, in order to avoid the abnormal HA heartbeat and synchronization message due to the abnormal link of the interface on SCMs.
Control link interface 6	Specifies the name of interface on I/O modules as the HA control link interface 6 (Backup device). **Note**: You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.
Assist link interface	Specifies the name of the HA assist link interface to receive and send heartbeat packets (Hello packets) and ensure the main and backup device of HA switches normally when the HA link fails. **Notes**: • Before the HA link is restored, the HA assist link interface can only receive and send heartbeat packets and the data packets cannot be synchronized. You are advised not to modify the current configurations. After the HA link is restored, manually synchronize session information. • The HA assist link interface must use an interface other than the HA link interface and be bound to the zone. • You need to specify the same interface as the HA assist link interface for the main and backup device, and ensure that the interface of the main and backup device belongs to the same VLAN.
Data link interface 1	Specifies the name of the HA data link interface 1. The data link interface is used to synchronize the data packet information, such

Option	Description
	as session information. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link.
Data link interface 2	Specifies the name of the HA data link interface 2 (backup interface). Notes: • You can specify at most one aggregate interface as the HA data link interface, or at most two physical interfaces as the HA data link interface. • When both the control link interface and data link interface are configured, you are advised to configure the data link interface as being an aggregate interface to prevent session synchronization failures at a data link failure.
IP Type	Specifies the IP address type of the HA link. This option is available only when the device's IP version is IPv6.
IP Address/IPv6 Address	Specifies the IP address of the HA link, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type is IPv4 or the device's IP version is IPv4, specifies the IPv4 address and netmask of the HA link interface, in format A.B.C.D/M. The value of M can be an integer ranging from 1 to 32 or a string in dotted decimal notation.

Option	Description
	• When the IP address type is IPv6, specifies the IPv6 address and prefix length of the HA link interface, in format X.X.X.X::X/M. X.X.X.X::X is the IPv6 address prefix. M is the prefix length. The value range of the prefix length is 1 to 128.
HA Virtual MAC	Specifies the virtual MAC address of the HA device interface: • Default: Use the system default generated HA dummy MAC address generated by the system. • HA virtual prefix: Specifies the prefix of the HA base MAC in hexadecimal format. Its length can only be configured as seven or eight. If more than 8 HA clusters in a network segment need to be configured, you can configure the prefix of the HA virtual base MAC address, i.e., the HA virtual MAC prefix, in order to avoid the HA virtual MAC address duplication. By default, the HA virtual MAC prefix is 0x001C54FF. After the configuration is completed, the configuration will take effect after reboot. • HA base virtual MAC: Specifies the HA base virtual MAC address. To ensure unique system-generated HA virtual MAC addresses and simplify future maintenance, you can assign specific HA virtual MAC addresses by specifying HA base virtual MAC. It is recommended that you use the system-recommended HA base virtual MAC. No device reboot is required for the configuration to take effect.

Option	Description
	Note: • The HA virtual prefix is only supported for CloudEdge. • HA base virtual MAC function is supported only in HA A/P mode and needs to be configured before the HA function is enabled. • 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid. • HA virtual prefix and HA base virtual MAC functions are mutually exclusive and the two cannot be configured at the same time. It is recommended that you prioritize the configuration of the HA base dummy MAC function. • IF the HA function enabled and you want to modify the HA virtual MAC prefix or HA base virtual MAC, you may need to disable the HA function first.
HA cluster ID	Specifies an ID for HA cluster. Saving the configuration of an HA cluster ID will enable the HA function. Deleting the configuration of it will disable the HA function. The value ranges from 1~8.When the length of prefix is set to 7 hexadecimal, the ID ranges from 1~128. When the length of prefix is set to 8 or by default, the ID ranges from 1~8.
Node ID	Specify the node ID. The two devices should be configured with different node IDs. The value range is 0 to 1. Certain devices sup-

Option	Description
	port automatic negotiation of the node ID. It is recommended to manually configure the node ID.
HA Negotiation Mode	Specifies the HA negotiation mode. Valid values: Default, Same Network Segment, and Cross-Network Segment. • Default: indicates that devices in the same network segment use multicast communication for HA negotiation. This is the default option. • Same Network Segment: indicates that devices in the same network segment use layer-2 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address, or configure both the HA peer IP address and MAC address. • Cross-Network Segment: indicates that devices in different network segments use layer-3 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address and next-hop gateway.
HA Peer IP/HA Peer IPv6	Specifies the IP address of the peer device, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type of HA link is IPv4 or the device's IP version is IPv4, enter the IPv4 address of HA peer device. • When the IP address type of HA link is IPv6, enter the IPv6 address of HA peer device.

Option	Description
HA Peer MAC	Enter the MAC address of HA peer device, i.e. the MAC address of the heartbeat interface.
Next-hop Gateway	When the HA Negotiation Mode parameter is set to Cross-Network Segment, you need to specify the next-hop gateway address, which can be an IPv4 address or IPv6 address. The type of this address needs to be the same as that of the HA peer IP address.
MTU	Specifies the MTU value of HA link interface. If the size of the message exceeds the MTU value of the HA link interface, the sender will fragment and send the message and the receiver will reassemble the fragments. Valid values: 1280 to 1600. Unit: bytes. Default value: 1500.
L3 port down-up	If this function is disabled, the following types of physical interfaces do not perform down-up operations when the device is switched from a master device to a backup device for HA switchover: • The physical interface that is bound to a Layer 3 zone. • The physical interface that belongs to a redundant interface, and the redundant interface is bound to a Layer 3 zone. • The physical interface that belongs to an aggregate interface, and the aggregate interface is bound to a Layer 3 zone.
MAC Address	Specifies the source MAC address for the HA device to send heartbeats (Hello packets) to other devices in HA group: • Default: The system uses the default MAC address to send

Option	Description
	Hello packets. • Control link interface MAC: Specifies the MAC address of control link interface as the MAC address of HA link interface. When there are multiple configured control link interfaces, the system will use the MAC address of the first control link interface as the MAC address of HA link interface. • Customize: Specifies a custom MAC address as the MAC address of HA link interface. If this option is selected, enter the custom MAC address in the MAC field.
Use Interface Real MAC	After you enable this function, the device uses the real MAC address of interface (except HA link interface and the interface configured with the Local property). By default, the interface forwards traffic with the virtual MAC address assigned by the system. However, after this function is enabled, each interface uses its real MAC address for communication. **Note:** If a custom HA MAC address (HA VMAC) is configured for an interface, the interface forwards traffic based on the custom HA MAC address, and other interfaces forward traffic based on this function.
Cloud Platform	Select the cloud platform where the current CloudEdge resides. Valid values: Tencent Cloud, Alibaba Cloud, AWS, Apsara Stack, Huawei Cloud and None. Then, configure the corresponding options based on your deployment mode.

Option	Description
Deploy Mode	Select the mode in which HA is deployed on the cloud platform. The system supports the Accesskey and HAVIP modes. If you set the mode to Accesskey, you need to configure the AccessKey ID and password. • Accesskey: indicates that the AccessKey authentication mode is used in CloudEdge to access the cloud platform. Then, the secondary IP address is used to deploy an HA scenario of CloudEdge. • HAVIP: indicates that HA virtual IP (HAVIP) is configured on the cloud platform to deploy an HA scenario of CloudEdge.
Control Center	Enter the access address of the cloud platform control center, which can be a domain name or an IP address. The value range is 1 to 255 characters. **Notes:** Currently, only in the CloudEdge HA scenario deployed on Huawei Cloud is it necessary to configure the access address and port of the cloud platform control center.
Control Center Port	Enter the access port for the cloud platform control center. The value range is 0 to 65535. The default configuration is 0, which means no specific port is specified, and the default port of the protocol will be used during access.
Accesskey ID	Enter the AccessKey or APPID applied on the cloud platform.

Option	Description
Accesskey Secret	Enter the password of the AccessKey or APPID.
Change Access-key Secret	This function is available when you edit the HA configuration. After you enable this function, the password field is displayed. To change the password, enter a new password and save the con-figuration.
Check Con-nection	Click this button to test the connectivity between the system and the cloud platform API.
Verify AccessKey ID and Secret	Click this button to check whether the AccessKey ID and pass-word are valid.
HA group con-figuration	HA group configuration consists of the following items: • Group: After you specify the HA working mode, the group ID is automatically generated and cannot be changed. In A/P mode, only Group 0 is available. • Priority: Specifies the priority of the current device in the HA group. The device with the highest priority (the lowest value) is elected as the primary device. Valid values: 1 to 254. • Preempt: Specifies whether to enable the preempt mode and the preempt time. If you enable this mode, the device will upgrade itself to the primary device once its priority is higher than the current primary device, and the current

Option	Description
	primary device becomes a secondary device. If you enter a value of 0, it indicates that you disable the preempt mode. In this case, the device can only substitute the primary device in case of primary device failure even if the priority of the device is higher than that of the primary device. Valid values: 0 to 600. Unit: seconds. • Hello interval: Specifies the Hello interval value. The Hello interval indicates the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. Valid values: 50 to 10000. Unit: milliseconds. • Hello threshold: Specifies the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device, it will suppose the other device's heartbeat stops. Valid values: 3 to 255. • Gratuitous ARP packet number: Specifies the number of gratuitous ARP packets. When the backup device is elected as the primary device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. Valid values: 10 to 180. • Track Object: Specifies the track object you have configured or click ⊕ to create a track object. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take

Option	Description
	the corresponding action. • Description: Specifies the description of the HA group.
Auto-check for Configuration Consistency of Master and Backup	Enable this function to automatically check whether configurations between the master and the backup devices are the same. After this function is enabled, the system will perform one check immediately and afterward at the interval of 1 hour. After every check, the system will refresh the Latest Check Result option. If a configuration inconsistency is found, a log will be also recorded. To view inconsistency details, you can perform a check again via the Manual Check for Consistency of Master and Backup option. This function is disabled by default. **Note**: Please enable the "Auto-check for Configuration Consistency of Master and Backup" function on the master device after the HA negotiation is successful. When this function is enabled, the backup device synchronizes the configuration.
Manual Check for Consistency of Master and Backup	Click **Query** to perform one-time configuration consistency check between the master and the backup devices. After the check is finished, the Latest Check Result option will be automatically refreshed. If different configurations exist, a page showing detailed configuration differences will be prompted. **Notes**: • On devices supporting the VSYS function and loaded with the VSYS license, click **Details** to view the details for each VSYS. In other conditions, the details are directly displayed.

Option	Description
	• Please perform one-time configuration consistency check on the master device after the HA negotiation is successful.
Latest Check Result	Displays the configuration consistency check result, check time and query type.

3. Click **OK.**

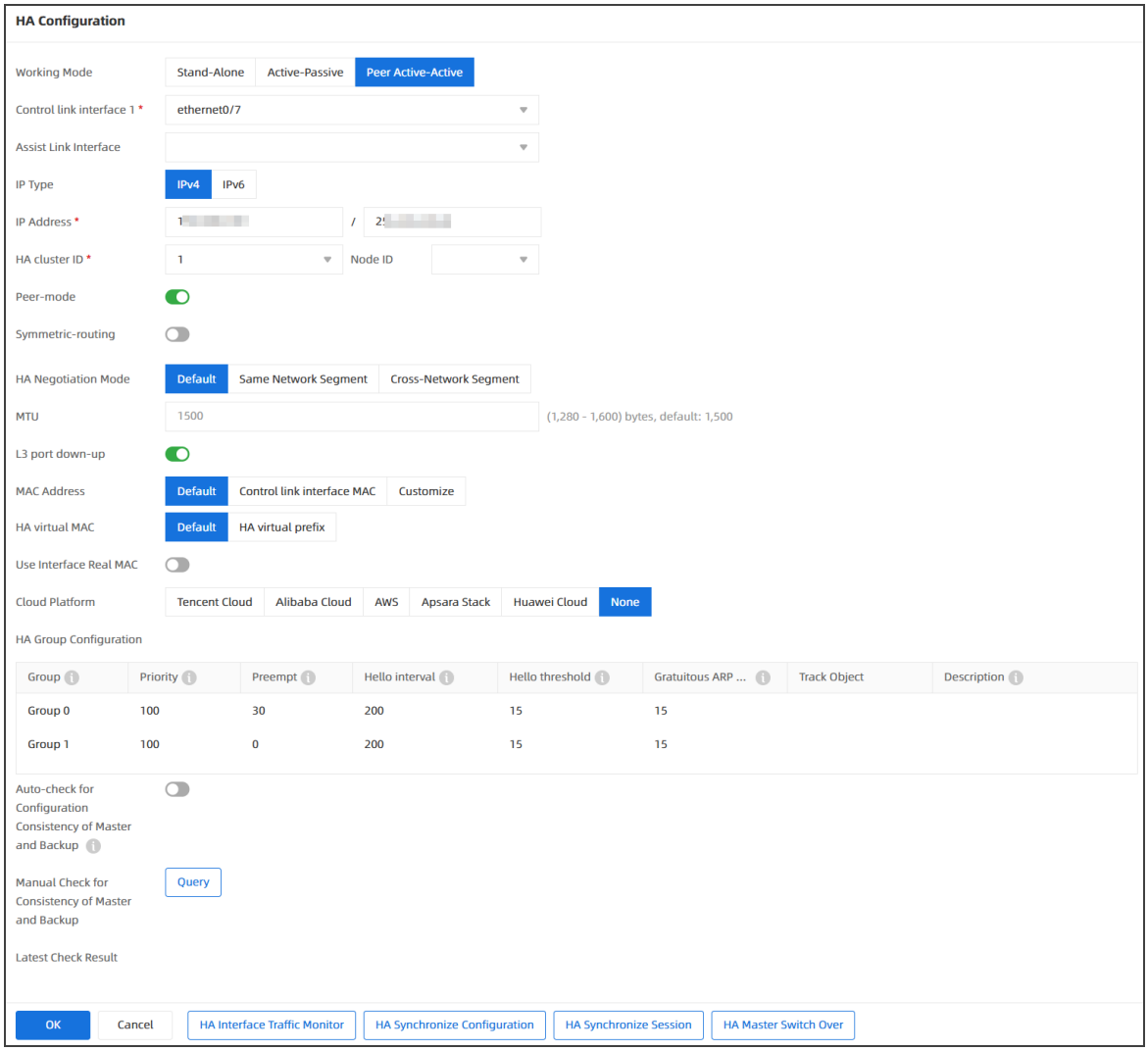
Configuring HA Peer Active-Active (A/A) Mode

The main configuration steps of the HA Peer Active-Active (A/A) mode include:

1. Configure an HA Virtual Forward Interface. For more information on configuring the interface, see Configuring an Interface.
2. Configure the HA working mode as Peer Active-Active.
3. Configure the HA link, including an HA link interface and an HA link IP address, for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the HA VMAC prefix (optional), HA cluster ID and HA node ID to enable the HA function.
5. Enable the HA peer mode.
6. Configure an HA group. Specify the priority for devices (for selecting the master) and HA messages parameters.

To configure HA Peer Active-Active (A/A) mode, take the following steps

1. Go to **System > HA**.
2. Select the HA working mode as Peer Active-Active, which means that both devices in the HA cluster work in active mode.



Configure HA Peer Active-Active (A/A) mode.

Option	Description
Control link interface 1	Specifies the name of the HA control link interface 1. The control link interface is used to synchronize all data between two devices.
Control link interface 2	Specifies the name of HA control link interface 2 (Backup interface). **Note:** You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.

Option	Description
Control link interface 1, 2, 3, 4	X-seriesK20803 devices by default use the interface on the System Control Modules (SCMs) as HA control link interface. These control link interfaces cannot be deleted or modified. To configure the HA link interface of X-seriesK20803 devices, you need to pay attention to the following • You can only synchronize the data information through HA date link interface. • By default, all HA interfaces (HA0 and HA1) of SCMs will be configured as the the HA control link automatically, and you don't need to configure. To connect the HA control link, take the following methods • Connect the HA0 of master SCM on the master device with the HA0 of the master SCM on the backup device. • Connect the HA1 of master SCM on the master device with the HA0 of the backup SCM on the backup device. • Connect the HA0 of backup SCM on the master device with the HA1 of the master SCM on the backup device. • Connect the HA1 of backup SCM on the master device with the HA1 of the backup SCM on the backup device.

Option	Description
Control link interface 5	Specifies the name of interface on I/O modules as the HA control link interface 5, in order to avoid the abnormal HA heartbeat and synchronization message due to the abnormal link of the interface on SCMs.
Control link interface 6	Specifies the name of interface on I/O modules as the HA control link interface 6 (Backup device). **Note**: You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.
Assist link interface	Specifies the name of the HA assist link interface to receive and send heartbeat packets (Hello packets) and ensure the main and backup device of HA switches normally when the HA link fails. **Notes**: • Before the HA link is restored, the HA assist link interface can only receive and send heartbeat packets and the data packets cannot be synchronized. You are advised not to modify the current configurations. After the HA link is restored, manually synchronize session information. • The HA assist link interface must use an interface other than the HA link interface and be bound to the zone. • You need to specify the same interface as the HA assist link interface for the main and backup device, and ensure that the interface of the main and backup device belongs to the same VLAN.

Option	Description
Data link interface 1	Specifies the name of the HA data link interface 1. The data link interface is used to synchronize the data packet information, such as session information. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link.
Data link interface 2	Specifies the name of the HA data link interface 2 (backup interface). Notes: • You can specify at most one aggregate interface as the HA data link interface, or at most two physical interfaces as the HA data link interface. • When both the control link interface and data link interface are configured, you are advised to configure the data link interface as being an aggregate interface to prevent session synchronization failures at a data link failure.
IP Type	Specifies the IP address type of the HA link. This option is available only when the device's IP version is IPv6.
IP Address/IPv6 Address	Specifies the IP address of the HA link, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type is IPv4 or the device's IP version is IPv4, specifies the IPv4 address and netmask of the HA link interface, in format A.B.C.D/M. The value of M can be an integer ranging from 1 to 32 or a string in dotted decimal

Option	Description
	notation. • When the IP address type is IPv6, specifies the IPv6 address and prefix length of the HA link interface, in format X.X.X.X::X/M. X.X.X.X::X is the IPv6 address prefix. M is the prefix length. The value range of the prefix length is 1 to 128.
HA cluster ID	Specifies an ID for HA cluster. Saving the configuration of an HA cluster ID will enable the HA function. Deleting the configuration of it will disable the HA function. The value ranges from 1~8.When the length of prefix is set to 7 hexadecimal, the ID ranges from 1~128. When the length of prefix is set to 8 or by default, the ID ranges from 1~8.
Node ID	Specify the node ID. The two devices should be configured with different node IDs. The value range is 0 to 1. Certain devices support automatic negotiation of the node ID. It is recommended to manually configure the node ID.
Peer-mode	Click to enable the HA peer mode. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is 1 will be in the disabled status. The group 1 in the device whose HA Node ID is 1 will be active and the group 1 in the device whose HA Node ID is 0 will be in the disabled status.
Symmetric-routing	Enable this function to make the device work in the symmetrical routing environment. It is recommended to enable this function

Option	Description
	when the inbound and outbound packets of a session are processed on the same device. When enabled, the system will simplify the session processing process. This function is disabled by default, that is, the device works in asymmetric routing mode by default.
HA Negotiation Mode	Specifies the HA negotiation mode. Valid values: Default, Same Network Segment, and Cross-Network Segment. • Default: indicates that devices in the same network segment use multicast communication for HA negotiation. This is the default option. • Same Network Segment: indicates that devices in the same network segment use layer-2 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address, or configure both the HA peer IP address and MAC address. • Cross-Network Segment: indicates that devices in different network segments use layer-3 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address and next-hop gateway.
HA Peer IP/HA Peer IPv6	Specifies the IP address of the peer device, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type of HA link is IPv4 or the device's IP version is IPv4, enter the IPv4 address of HA peer device.

Option	Description
	• When the IP address type of HA link is IPv6, enter the IPv6 address of HA peer device.
HA Peer MAC	Enter the MAC address of HA peer device, i.e. the MAC address of the heartbeat interface.
Next-hop Gateway	When the HA Negotiation Mode parameter is set to Cross-Network Segment, you need to specify the next-hop gateway address, which can be an IPv4 address or IPv6 address. The type of this address needs to be the same as that of the HA peer IP address.
MTU	Specifies the MTU value of HA link interface. If the size of the message exceeds the MTU value of the HA link interface, the sender will fragment and send the message and the receiver will reassemble the fragments. Valid values: 1280 to 1600. Unit: bytes. Default value: 1500.
L3 port down-up	If this function is disabled, the following types of physical interfaces do not perform down-up operations when the device is switched from a master device to a backup device for HA switchover: • The physical interface that is bound to a Layer 3 zone. • The physical interface that belongs to a redundant interface, and the redundant interface is bound to a Layer 3 zone. • The physical interface that belongs to an aggregate interface, and the aggregate interface is bound to a Layer 3 zone.
MAC Address	Specifies the source MAC address for the HA device to send heart-

Option	Description
	beats (Hello packets) to other devices in HA group: • Default: The system uses the default MAC address to send Hello packets. • Control link interface MAC: Specifies the MAC address of control link interface as the MAC address of HA link interface. When there are multiple configured control link interfaces, the system will use the MAC address of the first control link interface as the MAC address of HA link interface. • Customize: Specifies a custom MAC address as the MAC address of HA link interface. If this option is selected, enter the custom MAC address in the MAC field.
HA virtual prefix	Specifies the prefix of the HA base MAC in hexadecimal format. Its length can only be seven or eight. If more than 8 HA clusters in a network segment need to be configured, you can configure the prefix of the HA virtual base MAC address, i.e., the HA virtual MAC prefix, in order to avoid the HA virtual MAC address duplication. By default, the HA virtual MAC prefix is 0x001C54FF. It should be noted that 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid. After the configuration is complete, the configuration will take effect after reboot. **Note**: To modify the HA virtual MAC prefix with the HA function enabled first, you need to disable the HA function first.

Option	Description
Use Interface Real MAC	After you enable this function, the device uses the real MAC address of interface (except HA link interface and the interface configured with the Local property). By default, the interface forwards traffic with the virtual MAC address assigned by the system. However, after this function is enabled, each interface uses its real MAC address for communication. **Note:** If a custom HA MAC address (HA VMAC) is configured for an interface, the interface forwards traffic based on the custom HA MAC address, and other interfaces forward traffic based on this function.
Cloud Platform	Select the cloud platform where the current CloudEdge resides. Valid values: Tencent Cloud, Alibaba Cloud, AWS, Apsara Stack, Huawei Cloud and None. Then, configure the corresponding options based on your deployment mode.
Deploy Mode	Select the mode in which HA is deployed on the cloud platform. The system supports the Accesskey and HAVIP modes. If you set the mode to Accesskey, you need to configure the AccessKey ID and password. • Accesskey: indicates that the AccessKey authentication mode is used in CloudEdge to access the cloud platform. Then, the secondary IP address is used to deploy an HA scenario of CloudEdge. • HAVIP: indicates that HA virtual IP (HAVIP) is configured on the cloud platform to deploy an HA scenario of

Option	Description
	CloudEdge.
Control Center	Enter the access address of the cloud platform control center, which can be a domain name or an IP address. The value range is 1 to 255 characters. **Notes:** Currently, only in the CloudEdge HA scenario deployed on Huawei Cloud is it necessary to configure the access address and port of the cloud platform control center.
Control Center Port	Enter the access port for the cloud platform control center. The value range is 0 to 65535. The default configuration is 0, which means no specific port is specified, and the default port of the protocol will be used during access.
Accesskey ID	Enter the AccessKey or APPID applied on the cloud platform.
Accesskey Secret	Enter the password of the AccessKey or APPID.
Change Accesskey Secret	This function is available when you edit the HA configuration. After you enable this function, the password field is displayed. To change the password, enter a new password and save the configuration.
Check Connection	Click this button to test the connectivity between the system and the cloud platform API.
Verify AccessKey ID	Click this button to check whether the AccessKey ID and password are valid.

Option	Description
and Secret	
HA group configuration	HA group configuration consists of the following items: • Group: After you specify the HA working mode, the group ID is automatically generated and cannot be changed. In peer A/A mode, both Group 0 and Group 1 are available. • Priority: Specifies the priority of the current device in the HA group. The device with the highest priority (the lowest value) is elected as the primary device. Valid values: 1 to 254. • Preempt: Specifies whether to enable the preempt mode and the preempt time. If you enable this mode, the device will upgrade itself to the primary device once its priority is higher than the current primary device, and the current primary device becomes a secondary device. If you enter a value of 0, it indicates that you disable the preempt mode. In this case, the device can only substitute the primary device in case of primary device failure even if the priority of the device is higher than that of the primary device. Valid values: 0 to 600. Unit: seconds. • Hello interval: Specifies the Hello interval value. The Hello interval indicates the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. Valid values: 50 to 10000. Unit: milliseconds.

Option	Description
	• Hello threshold: Specifies the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device, it will suppose the other device's heartbeat stops. Valid values: 3 to 255. • Gratuitous ARP packet number: Specifies the number of gratuitous ARP packets. When the backup device is elected as the primary device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. Valid values: 10 to 180. • >Track Object: Specifies the track object you have configured or click ⊕ to create a track object. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take the corresponding action. • Description: Specifies the description of the HA group.
Auto-check for Configuration Consistency of Master and Backup	Enable this function to automatically check whether configurations between the master and the backup devices are the same. After this function is enabled, the system will perform one check immediately and afterward at the interval of 1 hour. After every check, the system will refresh the Latest Check Result option. If a configuration inconsistency is found, a log will be also recorded. To view inconsistency details, you can perform a check again via the Manual Check for Consistency of Master and Backup option. This function is disabled by default. **Note**: Please enable

Option	Description
	the "Auto-check for Configuration Consistency of Master and Backup" function on the master device after the HA negotiation is successful. When this function is enabled, the backup device synchronizes the configuration.
Manual Check for Consistency of Master and Backup	Click **Query** to perform one-time configuration consistency check between the master and the backup devices. After the check is finished, the Latest Check Result option will be automatically refreshed. If different configurations exist, a page showing detailed configuration differences will be prompted. **Notes**: • On devices supporting the VSYS function and loaded with the VSYS license, click **Details** to view the details for each VSYS. In other conditions, the details are directly displayed. • Please perform one-time configuration consistency check on the master device after the HA negotiation is successful.
Latest Check Result	Displays the configuration consistency check result, check time and query type.

3. Click **OK**.

For more information, refer to the **HA** section in *StoneOS WebUI User Guide*. FR 40481

CLI

Configuring HA

……

Specifying the Cloud platform of HA deploying

For CloudEdge , When "AccessKey/AppID" way is configured , you need continue to specify the cloud platform that CloudEdge is deployed , in the global configuration mode , use the following command:

ha cloud-deploy platform { **tencent** | **aliyun** |**aws** | **apsara-stack** | **huaweicloud**}

In the global configuration mode , use the command **no ha cloud-deploy platform** to delete the cloud platform .

Configuring the Cloud Platform Control Center Access Address and Port

To deploy the CloudEdge HA scenario on Huawei Cloud, you need to configure the access address and port of the cloud platform control center. In the global configuration mode, use the following commands:

ha cloud-deploy controller host {*domain-name* | *ip-address*} [**port** *port-number*]

- *domain-name* | *ip-address* - Enter the access address of the cloud platform control center, which can be a domain name or an IP address.
- **port** *port-number* - Enter the access port for the cloud platform control center. The value range is 1 to 65535. The default configuration is 0, which means no specific port is specified, and the default protocol port is used during access.

In global configuration mode, use the command **no ha cloud-deploy controller** to delete the access address and port of the cloud platform control center.

For more information, refer to the **High Availablity (HA)** > **Configuring HA** section in *StoneOS CLI User Guide*. FR 40481

Supporting retrieving the hit rate of NAT rules via SNMP

HILLSTONE-NAT-MIB

The following tables is the parsing results of HILLSTONE-NAT-MIB.

Name	OID	Value
hillstoneSnatRuleId	.1.3.6.1.4.1.28557.2.33.1.1.1.1.1	Data type: Unsigned32 Description: SNAT Resource Index
hillstoneSnatTotalTcpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.2	Data type: Unsigned32 Description: Total TCP resource
hillstoneSnatUsedTcpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.3	Data type: Unsigned32 Description: Used TCP resource
hillstoneSnatTotalUdpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.4	Data type: Unsigned32 Description: Total UDP resource
hillstoneSnatUsedUdpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.5	Data type: Unsigned32

Name	OID	Value
		Description: Used UDP resource
hillstoneSnatTotalIcmpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.6	Data type: Unsigned32 Description: Total ICMP resource
hillstoneSnatUsedIcmpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.7	Data type: Unsigned32 Description: Used ICMP resource
hillstoneSnatHitinfoTable: SNAT rule hit information		
hillstoneSnatRuleId	.1.3.6.1.4.1.28557.2.33.1.1.2.1.1	Data type: Integer Description: SNAT rule ID
hillstoneSnatHitCount	.1.3.6.1.4.1.28557.2.33.1.1.2.1.2	Data type: Integer Description: The number of hits of SNAT rules
hillstoneSnatFirstHitTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.3	Data type: Octet String Description: The time when the SNAT rule

Name	OID	Value
		was first hit
hillstoneSnatLastHitTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.4	Data type: Octet String Description: The time when the SNAT rule was last hit
hillstoneSnatCreateTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.5	Data type: Octet String Description: The time when the SNAT rule was created
hillstoneSnatHitRate	.1.3.6.1.4.1.28557.2.33.1.1.2.1.6	Data type: Integer Description: The rate of hitting SNAT rules and creating new sessions, in units of hit/s.
hillstoneDnatServerTabe：DNAT server information		
hillstoneDnatServerIndex	.1.3.6.1.4.1.28557.2.33.1.2.1.1.1	Data type: Integer Description: SLB server index
hillstoneDnatServerIPAndPort	.1.3.6.1.4.1.28557.2.33.1.2.1.1.2	Data type: DisplayString

Name	OID	Value
		Description: IP address and port information of SLB server
hillstoneDnatServerVrName	.1.3.6.1.4.1.28557.2.33.1.2.1.1.3	Data type: DisplayString Description: VRouter of SLB server
hillstoneDnatServerConnectionNum	.1.3.6.1.4.1.28557.2.33.1.2.1.1.4	Data type: Integer Description: Connection number of SLB server
hillstoneDnatServerStatus	.1.3.6.1.4.1.28557.2.33.1.2.1.1.5	Data type: Integer Description: Status of SLB server • 0 - Unknown • 1 - OK • 2 - Failed • 3 - Full load
hillstoneDnatServerGroup	.1.3.6.1.4.1.28557.2.33.1.2.1.1.6	Data type: Integer

Name	OID	Value
		Description: HA group of SLB server
hillstoneDnatHitinfoTable: DNAT rule hit information		
hillstoneDnatRuleId	.1.3.6.1.4.1.28557.2.33.1.2.2.1.1	Data type: Integer Description: DNAT rule ID
hillstoneDnatHitCount	.1.3.6.1.4.1.28557.2.33.1.2.2.1.2	Date type: Integer Description: The number of hits of DNAT rules
HillstoneDnatFirstHitTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.3	Date type: Octet String Description: The time when the DNAT rule was first hit
HillstoneDnatLastHitTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.4	Date type: Octet String Description: The time when the DNAT rule was last hit
hillstoneDnatCreateTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.5	Date type: Octet String

Name	OID	Value
		Description: The time when the DNAT rule was created
hillstoneDnatHitRate	.1.3.6.1.4.1.28557.2.33.1.2.2.1.6	Data type: Integer Description: The rate of hitting DNAT rules and creating new sessions, in units of hit/s.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 44445

Adjusting the Maximum Configurable Range for Each IP/User's Minimum and Maximum Bandwidth within the iQoS Pipe

WebUI

Configuring a Pipe

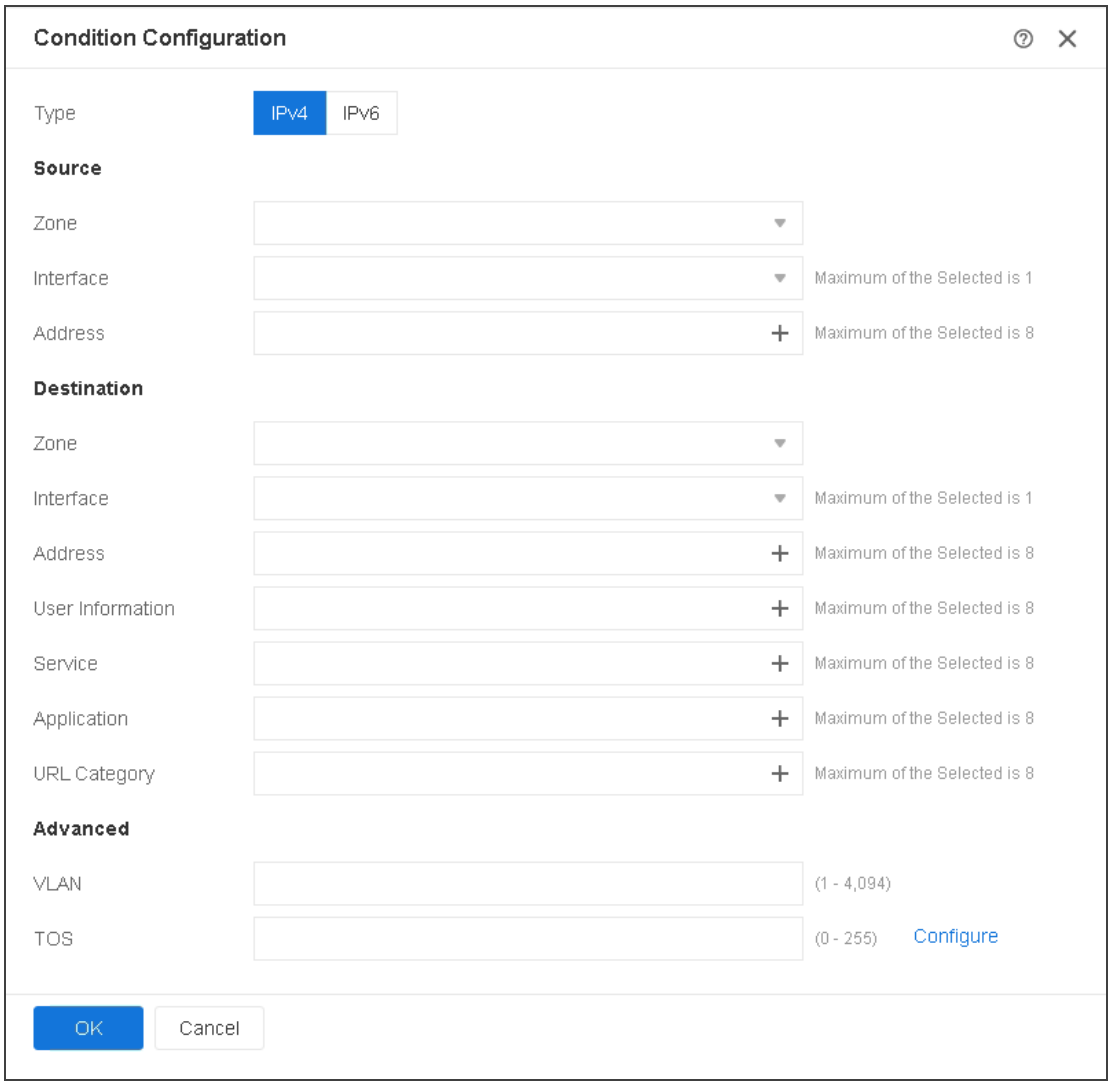
To configure a pipe, take the following steps:

1. According to the methods above, create a root pipe or sub pipe. The Pipe Configuration page appears.
2. In this page, specify the basic pipe information.

Option	Description
Parent Pipe/Control Level	Displays the control level or the parent pipe of the newly created pipe.
Pipe Name	Specify a name for the new pipe.
Mode	Shape, Policy, or Stat. • The Shape mode can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority adjusting for the traffic within the root pipe. • The Policy mode will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority adjusting, and cannot guarantee the minimum bandwidth.

Option	Description
	• Bandwidth borrowing: All of the sub pipes in a root pipe can lend their idle bandwidth to the pipes that are lacking bandwidth. The prerequisite is that their bandwidth must be enough to forward the traffic in their pipes. • Priority adjusting: When there is traffic congestion, system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and system will deal with the traffic in order of precedence. • The Stat mode will monitor the matched traffic, generate the statistics, and will not control the traffic.
Description	Specify the description of this pipe.
Schedule	Specifies a schedule when the pipe will take effect. Select a desired **schedule** from the Schedule drop-down list. **Notes**: Please check the associated schedule in each pipe configuration to avoid the situation where the effective sub-pipe bandwidth exceeds the root pipe configuration during a certain period, which may cause abnormal operation of iQos.

3. In Condition, click **New**.

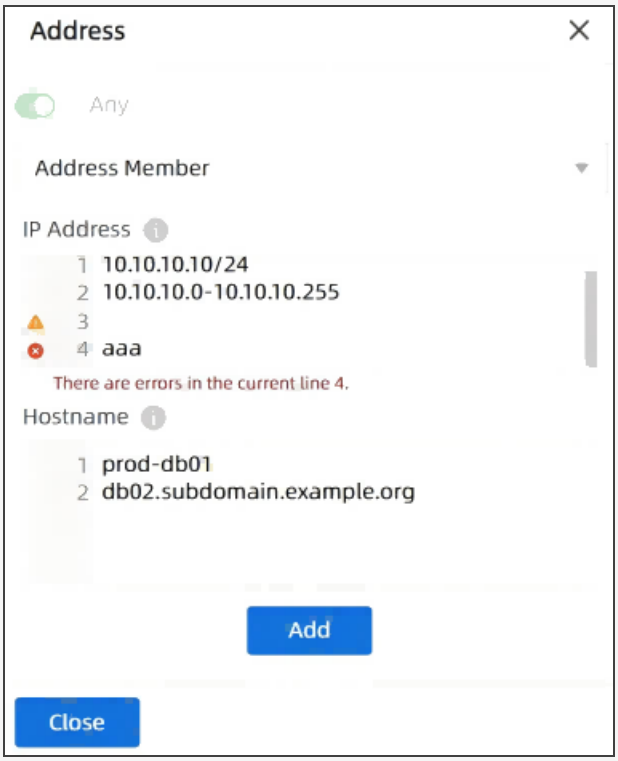


Option	Description
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type IP. If IPv6 is selected, all the IP/netmask, IP range, address entry configured should be in the IPv6 format.
Source Information	

Option	Description
Zone	Specify the source zone of the traffic. Select the zone name from the drop-down menu.
Interface	Specify the source interface of the traffic. Select the interface name from the drop-down menu. **Notes:** iQoS does not support to configure a tunnel interface. To limit the speed of tunnel traffic, use the method of policy-based IPSec VPN. For more information, see Configuring an IPSec VPN。
Address	Specify the source address of the traffic. 1. Click **Address** to select the address book or address member type from the **Address** dialog. 2. If you select the address book type, you can directly select an address book; If you select the address member type, you can enter an IP address or hostname in the corresponding text box. 3. Click **Add** to add the IP address or hostname to the left pane. 4. After adding the desired addresses, click **Close** to complete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ to create a new address entry.

Option	Description
	• When selecting the **Address Book** type, you can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **Address Member** type, the system allows you to batch add address members. As shown in the figure below, you can enter multiple address members in the text box, with each entry on a new line by pressing Enter. When entering multiple address members, you may input duplicate or incorrect entries. In such cases, the system will display the icon to the left of the corresponding line number. If a blank line is entered, the icon will appear.

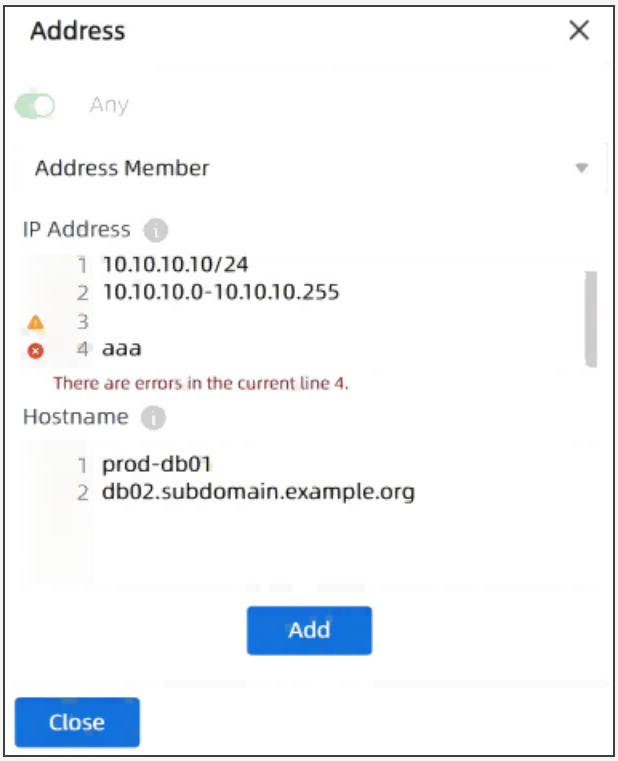
Option	Description

	Hovering the mouse over an icon will display the reason for the error or warning, making it easier for you to correct the entries.
	
	
	• When entering IP addresses, different formats are required for IPv4 and IPv6 address types, as follows:
	  • For the IPv4 address type, you need to enter an address member in the 'IP/Mask' or 'IP Range' format in the 'IP Address' text box. For example: 10.10.10.10/24 or 10.10.10.0-10.10.10.255.
	  • For IPv6 address types, you need to enter an

Option	Description
	address member in the 'IPv6/Prefix Length' or 'IPv6 Range' format in the 'IP Address' text box. For example: 11::11/128 or 11::11-11::12.
Destination Information	
Zone	Specify the destination zone of the traffic. Select the zone name from the drop-down menu.
Interface	Specify the destination interface of the traffic. Select the interface name from the drop-down menu.
Address	Specify the destination address of the traffic. 1. Click **Address** to select the address book or address member type from the **Address** dialog. 2. If you select the address book type, you can directly select an address book; If you select the address member type, you can enter an IP address or hostname in the corresponding text box. 3. Click **Add** to add the IP address or hostname to the left pane. 4. After adding the desired addresses, click **Close** to complete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ to create a new address entry.

Option	Description
	• You can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **Address Member** type, the system allows you to batch add address members. As shown in the figure below, you can enter multiple address members in the text box, with each entry on a new line by pressing Enter. When entering multiple address members, you may input duplicate or incorrect entries. In such cases, the system will display the icon to the left of the corresponding line number. If a blank line is entered, the icon will appear. Hovering the mouse over an icon will display the reason for the error or warning, making it easier for you to correct the

Option	Description

	entries.
	
	
	• When entering IP addresses, different formats are required for IPv4 and IPv6 address types, as follows:
	  • For the IPv4 address type, you need to enter an address member in the 'IP/Mask' or 'IP Range' format in the 'IP Address' text box. For example: 10.10.10.10/24 or 10.10.10.0-10.10.10.255.
	  • For IPv6 address types, you need to enter an address member in the 'IPv6/Prefix Length' or 'IPv6 Range' format in the 'IP Address' text

Option	Description
	box. For example: 11::11/128 or 11::11-11::12.
User Inform-ation	Specify a user or user group that the traffic belongs to. 1. From the **User** drop-down menu, select the AAA server where the users and user groups reside. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, and enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the user information configuration.
Service	Specify a service or service group that the traffic belongs to. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search for the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click them to add them to the right pane. 4. After adding the desired objects, click **Clos**e to complete the service configuration. You can also perform other operations:

Option	Description
	• To add a new service or service group, select **User-defined** from the "Predefined" drop-down list, and click ⊕. • The default service configuration is any. To restore the configuration to this default one, select the **any** check box.
Application	Specify an application, application group, or application filters that the traffic belongs to. 1. From the **Application** drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click them to add them to the left pane. 3. After adding the desired objects, click **Close** complete the application configuration. You can also perform other operations: • To add a new application group, click ⊕. • To add a new application filter, click ⊕. **Note**: Deprecated predefined applications cannot be added.
URL Category	Specifies the URL category that the traffic belongs to. After the user specifies the URL category, the system matches the traffic according to the specified category.

Option	Description
	1. In the "URL category" drop-down menu, the user can select one or more URL categories, up to 8 categories. 2. After selecting the desired filters, click the blank area in this page to complete the configuration. To add a new URL category, click ⊕ , the page will pop up "URL category" page. In this page, the user can configure the category name and URL.
Advanced	
VLAN	Specify the VLAN information of the traffic.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum cost. • Reserved: Specify the normal service.
TrafficClass	Specify the TOS fields of the traffic.

4. If you are configuring root pipes, you can specify the white list settings based on the description of configuring conditions.

5. Configuring the trigger threshold for the maximum floating bandwidth.

Option	Description
Lower threshold of a root pipe's bandwidth utilization	Specifies the lower threshold of the bandwidth utilization for a root pipe. When the bandwidth utilization is lower than the lower threshold, the maximum floating bandwidth of sub pipes is triggered. The value range is 20%-75%. The default lower threshold is 40%.
Upper threshold of a root pipe's bandwidth utilization	Specifies the upper threshold of the bandwidth utilization for a root pipe. When the bandwidth utilization is higher than the upper threshold, the maximum floating bandwidth of sub pipes will not be triggered. The value range is 76%-90%. The default lower threshold is 80%.

6. In Action, configuring the corresponding actions.

Forward (From source to destination)	
The following configurations control the traffic that flows from the source to the destination. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe: • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select **Enable Reserved Bandwidth**. • Max Bandwidth: Specify the maximum bandwidth.

Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:
	• Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**.
	  • **No Limit** represents that system will not limit the bandwidth for each IP or each user.
	  • **Limit Per IP** represents that system will limit the bandwidth for each IP. In the Limit by section, select **Source IP** to limit the bandwidth of the source IP in this pipe; or select **Destination IP** to limit the bandwidth of the destination IP in this pipe.
	  • **Limit Per User** represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users.
	• When configuring the root pipe, you can select the **Enable Average Bandwidth** check box to make each source IP, destination IP, or user to share an average bandwidth.

Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth or the maximum bandwidth: • Min Bandwidth: Specify the minimum bandwidth. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.

	• Max Bandwidth: Specify the maximum bandwidth. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps. • Maximum Floating Bandwidth: Specifies the maximum floating bandwidth. • Delay: Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
Advanced	
Priority	Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost.

	• Reserved: Specify the normal service.
TrafficClass	Specifies the value of the TrafficClass field for IPv6 traffic, The TrafficClass field value of IPv6 traffic matching successfully will be set to the specified value.
Limit Opposite Bandwidth	Click the **Enable** button to configure the value of limit-strength.The smaller the value, the smaller the limit.
Backward (From condition's destination to source)	
The following configurations control the traffic that flows from the destination to the source. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe: • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select **Enable Reserved Bandwidth**. • Max Bandwidth: Specify the maximum bandwidth.
Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP: • Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**. • **No Limit** represents that system will not limit the bandwidth for each IP or each user.

	• **Limit Per IP** represents that system will limit the bandwidth for each IP. In the Limit by section, select **Source IP** to limit the bandwidth of the source IP in this pipe; or select **Destination IP** to limit the bandwidth of the destination IP in this pipe. • **Limit Per User** represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users. • When configuring the root pipe, you can click the **Enable Average Bandwidth** button to make each source IP, destination IP, or user to share an average bandwidth.
Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth or the maximum bandwidth: • Min Bandwidth: Specify the minimum bandwidth. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps. • Max Bandwidth: Specify the maximum bandwidth. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps. • Maximum Floating Bandwidth: Specifies the maximum floating bandwidth.

	• Delay： Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
Advanced	
Priority	Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
Limit Opposite Bandwidth	Click the **Enable** button to configure the value of limit-strength.The smaller the value, the smaller the limit.

7. Click **OK** to save the settings.

For more information, refer to the **Policy** > **iQoS** > **Configuring iQoS** topic in *StoneOS WebUI User Guide*. FR 43189

CLI

Configuring iQoS

……

Configuring Traffic Management Actions for a Root Pipe

To configure traffic management actions for a root pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* **[per-ip-min***min-value***] [per-ip-max***max-value* **[delay***delay-time***] [flex-per-max {Kbps | Mbps}** *value***]] [per-ip-using {src-ip | dst-ip}] [tos-marking***tos-value***] [traffic-marking***traffic-class-value***] [mode aggressive [strength-level***level-value***]] [priority***value***]**

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps} *bandwidth-value* **[per-user-min***min-value***] [per-user-max***max-value* **[delay***delay-time***] [flex-per-max {Kbps | Mbps}** *value***]] [tos-marking***tos-value***] [traffic-marking***traffic-class-value***] [mode aggressive [strength-level***level-value***]] [priority***value***]**

pipe-rule {forward | backward} bandwidth {Kbps | Mbps | Gbps}*bandwidth-value* **average-using {src-ip | dst-ip | user} [tos-marking** *tos-value***] [traffic-marking***traffic-class-value* **] [mode aggressive [strength-level** *level-value***]][priority** *value***]**

- **forward** – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- **backward** -Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.
- - Specify the minimum bandwidth of the pipe. When selecting Kbps, the bandwidth ranges from 32 to 100,000,000. When selecting Mbps, the bandwidth ranges from 1 to 100,000. When selecting Gbps, the bandwidth ranges from 1 to 100.

- **per-ip-min** *min-value* - Specify the minimum bandwidth of each IP. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **per-ip-max** *max-value* - Specify the maximum bandwidth of each IP. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **per-ip-using** {**src-ip**|**dst-ip**} - Limit the bandwidth to each source IP address or destination IP address. This configuration can take effect after you have configured the per-ip-min min-value and per-ip-max max-value parameters.
- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 16000000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 16000Mbps.
- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. When selecting **Kbps**, the value ranges from 32Kbps to 16000000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 16000Mbps.
- **delay** *delay-time* – Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
- **flex-per-max** {**Kbps** | **Mbps**} – Specifies the maximum floating bandwidth, which should be larger than the maximum bandwidth of each IP/user. The maximum floating bandwidth is triggered when a root pipe's bandwidth utilization is lower than the lower threshold. If Kbps is selected, the value range is from 32Kbps to 1000,000Kbps. If Mbps is selected, the value range is from 1Mbps to 1000Mbps.
- **tos-marking***tos-value* - Specify the TOS filed.

- **traffic-marking***traffic-class-value*] - Specifies the value of the TrafficClass field for IPv6 traffic, ranging from 0-255. The TrafficClass field value of IPv6 traffic matched is set to the specified value.
- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device.When the peer quench function is enabled,the default value of strength-level is 1,whose value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.
- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.
- **average-using** {**src-ip** | **dst-ip** | **user**} - Allocate the bandwidth equally to each source IP address or each destination IP address in the pipe.

Use the no form of the above command to delete the traffic management actions of a specified direction.

Notes:

- You cannot limit the bandwidth to each user and each IP address at the same time.
- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

Configuring Traffic Management Actions for a Sub Pipe

To configure traffic management actions for a sub pipe, in the root pipe configuration mode, use the following actions:

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**}*value* **max** {**percent** | **Kbps** | **Mbps** | **Gbps**}*max-value*[**per-ip-min** *min-value*] [**per-ip-max** *max-value*[**delay** *delay-time*]] [**flex-per-max {Kbps | Mbps}** *value*] [**per-ip-using** {**src-ip** | **dst-ip**}] [**tos-marking** *tos-value*] [**traffic-marking***traffic-class-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

pipe-rule {**forward** | **backward**} {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**}*min-value* **max {percent** | **Kbps** | **Mbps** | **Gbps}** *max-value* [**per-user-min** *min-value*] [**per-user-max** *max-value*[**delay** *delay-time*]] [**flex-per-max** {**Kbps** | **Mbps**} *value*] [**tos-marking** *tos-value*] [**traffic-marking***traffic-class-value*] [**mode aggressive** [**strength-level** *level-value*]] [**priority** *value*]

- **forward** – Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the source to the destination.
- **backward** - Specify the traffic control actions to the traffic that matches the traffic matching conditions and whose direction is from the destination to the source.
- {**min** | **reserve-bandwidth**} {**percent** | **Kbps** | **Mbps** | **Gbps**}*value* - Specify the minimum bandwidth of the pipe, or set the reserved bandwidth of the pipe. `min` represents the minimum bandwidth and **reserve-bandwidth** represents the reserved bandwidth. When configuring the minimum bandwidth or the reserved bandwidth, **percent**represents that the minimum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**, the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps** the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.
- **max** {**percent** | **Kbps** | **Mbps** | **Gbps**}*max-value* - Specify the maximum bandwidth of the pipe or the maximum percentage of its parent pipe. **percent**represents that the maximum percentage of the parent pipe bandwidth. The value ranges from 1 to 100. When selecting **Kbps**,

the value ranges from 32Kbps to 100,000,000Kbps. When selecting **Mbps**, the value ranges from 1Mbps to 100,000Mbps. When selecting **Gbps**, the value ranges from 1Gbps to 100Gbps.

- **per-ip-min** *min-value* - Specify the minimum bandwidth of each IP address. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **per-ip-max** *max-value* - Specify the maximum bandwidth of each IP address. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **per-ip-using** {**src-ip**|**dst-ip**} - Specify which kind of IP addresses will be controlled by the bandwidth limit you configured by the per-ip-max max-value and per-ip-min min-value commands. src-ip represents the source IP address, and dst-ip represents the destination IP address.
- **per-user-min** *min-value* - Specify the minimum bandwidth of each user. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **per-user-max** *max-value* - Specify the maximum bandwidth of each user. When you select **Kbps**, valid values are 32Kbps to 16000000Kbps. When you select **Mbps**, valid values are 1Mbps to 16000Mbps.
- **delay** *delay-time* – Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
- **flex-per-max** {**Kbps** | **Mbps**} – Specifies the maximum floating bandwidth, which should be larger than the maximum bandwidth of each IP/user. The maximum floating bandwidth is triggered when a root pipe's bandwidth utilization is lower than the lower threshold. If Kbps is selected, the value range is from 32Kbps to 1000,000Kbps. If Mbps is selected, the value range is from 1Mbps to 1000Mbps.

- **tos-marking***tos-value* - Specify the TOS filed.
- **traffic-marking***traffic-class-value*] - Specifies the value of the TrafficClass field for IPv6 traffic, ranging from 0-255. The TrafficClass field value of IPv6 traffic matched is set to the specified value.
- **mode aggressive** [**strength-level** *level-value*] - Enable the peer quench function. By default, this function is disabled. According to the distributed bandwidth by the user, the peer quench function makes the traffic that arrives at the device be the same as the distributed bandwidth as possible as it can, which reduces the missed packets of the device. When the peer quench function is enabled, the default value of strength-level is 1,which value ranges from 1 to 8. A bigger value represents a higher strength-level and a lesser lost of packets.
- **priority** *value* - Specify the priority of the pipe. The value ranges from 0 to 7. The default value is 7. A smaller value represents a higher priority and the system will first arrange the traffic in a a pipe with a higher priority and will first borrow the idle bandwidth from other pipes with a lower priority.

Notes:

- You cannot limit the bandwidth to each user and each IP address at the same time.
- You cannot enable the peer quench function in the positive and negative traffic management direction at the same time. The peer quench function only be supported in a end-pipe.

For more information, refer to the **Traffic Management** > **iQoS** > **Configuring iQoS** topic in *StoneOS CLI User Guide*. FR 43189

Supporting to Deploy ZTNA Authorization Policies by Using the Radius Server

WebUI

ZTNA Policy

ZTNA policy is a network security policy based on the principle of "never trust, always verify." It requires strict authentication and authorization of each user and device, ensuring that only authorized entities that comply with security policies can access specified network resources.

ZTNA policies are divided into ZTNA authorization policies and custom ZTNA policies. The system supports up to 2,000 ZTNA policies (the total of ZTNA authorization policies and custom ZTNA policies).

- ZTNA authorization policy: In a ZTNA scenario, when a user successfully authenticates through a RADIUS server, the server creates one or more ZTNA policies for this authenticated user based on the user configuration in the server. These policies include endpoint tags, application resources, and behaviors, and are referred to as ZTNA authorization policies. If an authenticated user needs to adjust the ZTNA authorization policies without interrupting the ZTNA connection, simply modify or add the corresponding configurations in the RADIUS server. This enables the RADIUS server to send CoA request messages, thereby dynamically adjusting or deploying new ZTNA authorization policies. The ZTNA authorization policies created by the RADIUS server for the authenticated user will appear at the end of the list on the **ZTNA Policy** page, where users can view the details of these policies. ZTNA authorization policies cannot be edited but can be deleted. The system allows for the manual deletion of ZTNA authorization policies on the **ZTNA Policy** page and can also automatically delete the corresponding ZTNA authorization policies when the authenticated user disconnects the ZTNA connection. The RADIUS server can create up to 16 ZTNA authorization policies per authenticated user.

Notes: To enable ZTNA authorization policies, please ensure the following:

- Ensure that the user configuration information in the RADIUS server includes the ZTNA policy string, and that the endpoint tags and application resources specified by this string have been successfully configured in the firewall in advance. More information about the ZTNA policy string configuration format, see the ZTNA Policy String Format.
- The RADIUS server used for ZTNA user authentication needs to have the Authorization Policy function enabled. For more information, see the AAA Server > **Configuring Radius Server** section.
- If an authenticated user needs to adjust the ZTNA authorization policies without interrupting the ZTNA connection, ensure that the RADIUS dynamic authorization function is enabled. For more information, see the AAA Server > **Configuring Radius Dynamic Authorization** section.
- When configuring the ZTNA gateway, reference the RADIUS server that has the "Authorization Policy" function enabled in the "Access User" option. For more information, see the **Configure ZTNA Gateway** topic.

- Custom ZTNA policies: They are ZTNA policies that users manually create on the **ZTNA Policy** page. Users can perform operations such as editing and deleting these manually created ZTNA policies.

A ZTNA policy functions based on the matching condition and action. It supports the following dimensions as matching conditions:

- User/User group: When a user/user group matches the one configured in the ZTNA policy, this user/user group is considered to meet the matching condition.

- Endpoint tag: When the endpoint tag carried with an authenticated user matches the one configured in the ZTNA policy, this endpoint tag is considered to meet the matching condition.
- Application resource/Application resource group: When a requested application resource/application resource group matches the one configured in the ZTNA policy, this application resource/application resource group is considered to meet the matching condition.
- Schedule: When the user access time matches the one configured in the ZTNA policy, the access time is considered to meet the matching condition.

ZTNA policy can be configured with one or multiple matching conditions. For a ZTNA policy configured with multiple matching conditions, the policy is considered to be hit and the traffic will be processed based on the action specified in the policy only when all matching conditions are met. When a matching condition is not configured in a ZTNA policy, all objects are considered to meet this matching condition. The policy action includes two types (at least one must be configured):

- permit: User traffic hitting a specified ZTNA policy will be granted access to resources configured in the policy.
- deny: User traffic hitting a specified ZTNA policy will be denied access to resources configured in the policy.

User traffic that does not hit any ZTNA policies will hit the ZTNA default policy and be processed based on the default action.

Description about ZTNA Policy Matching

For Internet access scenarios, the following traffic will experience ZTNA policy matching, while other traffic will experience firewall security policy matching:

- Traffic that enters from a ZTNA tunnel interface, and the zone service type of the traffic's egress interface, as found based on the route, is not a WAN zone.

For intranet access scenarios, if the traffic meets any of the following conditions, ZTNA policy matching is performed, and firewall security policy matching is performed for other traffic:

- The zone service type of the traffic's ingress interface is a ZTNA zone, and the zone service type of the traffic's egress interface, as found based on the route, is not a WAN zone.
- The zone service type of the traffic's egress interface, as found based on the route, is a ZTNA zone.

For more information about how to configure a zone service type, see Specifying the Service Type of Zone.

Ztna Policy String Format

The format of the ZTNA policy string configured for users in the Radius server or sent in a CoA request message is as follows:

ztna-rule *rule-name* {**permit** | **deny**} [**endpoint-tag** *tag-name*] [**app-resource** *resource-name*] [**app-resource-group** *group-name*] [**log** {**policy-deny** | **session-start** | **session-end** | **policy-deny session-start** | **policy-deny session-end** | **session-start session-end** | **policy-deny session-start session-end**}] [**Description** *dsecription*]

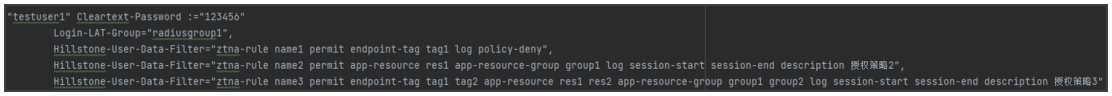
- **ztna-rule** - Fixed prefix used to distinguish between regular policies and ZTNA policies.
- *rule-name* - Specify the name of the ZTNA policy, uniquely identifying a ZTNA policy. The value range is 1 to 95 characters.
- **permit** | **deny** - Specify the control action of the ZTNA policy. **permit** indicates allowing access to the application resources bound to the ZTNA policy; **deny** indicates denying access to the application resources bound to the ZTNA policy.
- [**endpoint-tag** *tag-name*] - Specify the endpoint tag name, with a length of 1 to 95 characters. You can enter multiple tags but no more than 10. When entering multiple tags, separate them with spaces. For example: **endpoint-tag tag1 tag2**
- [**app-resource** *resource-name*] - Specify the application resource name, with a length of 1 to 95 characters. You can enter multiple names but no more than 10. When entering multiple names, separate them with spaces. For example: **app-resource res1 res2 res3**

- [**app-resource-group** *group-name*] - Specify the application resource group name, with a length of 1 to 95 characters. You can specify multiple names, but no more than 10. When specifying multiple names, separate them with spaces. For example: **app-resource-group group1 group2**
- [**log** {**policy-deny** | **session-start** | **session-end** | **policy-deny session-start** | **policy-deny session-end** | **session-start session-end** | **policy-deny session-start session-end**}] - Specify the scenarios that require logging.
    - **policy-deny** - This indicates logging information for ZTNA policy denied traffic;
    - **session-start** - Indicates the logging information for ZTNA session establishment;
    - **session-end** - Indicates the log information for the end of a ZTNA session;
    - **policy-deny session-start** - This indicates logging information for ZTNA policy denied traffic and ZTNA session establishment;
    - **policy-deny session-end** - This indicates logging information for ZTNA policy denied traffic and ZTNA session end;
    - **session-start session-end** - This indicates logging information for ZTNA session establishment and session termination;
    - **policy-deny session-start session-end** - This indicates logging information for ZTNA policy denial, ZTNA session establishment, and ZTNA session termination.
- [**Description** *dsecription*] - Specify the description information for the ZTNA policy. The value range is 1 to 255 characters.

Notes:

- The size of a single ZTNA policy string cannot exceed 255 bytes.
- The size of a single Radius packet cannot exceed 4096 bytes.

The following is an example of the ZTNA policy string included in the user configuration information in the Radius server:



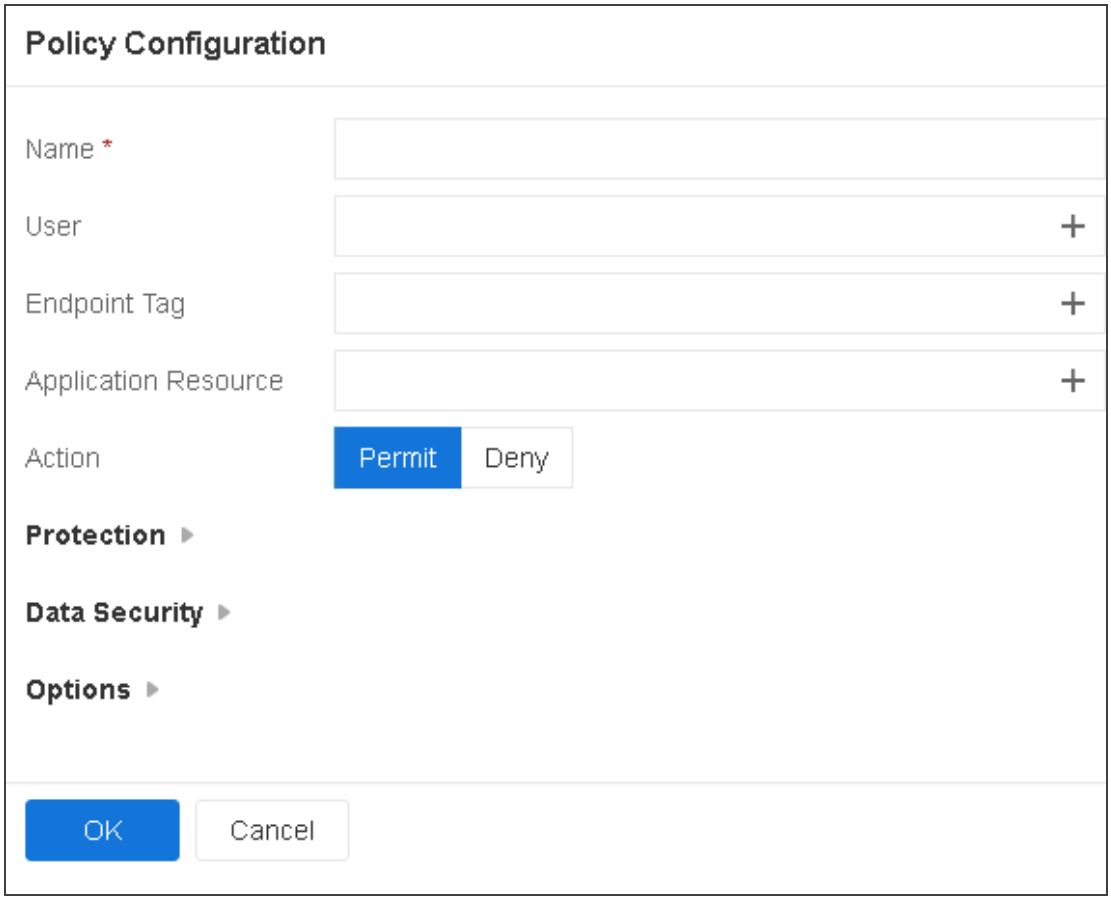
Configuring ZTNA Policy

Before you start

- **Read** ZTNA Policy**.**

To configure a ZTNA policy, take the following steps:

1. Select **ZTNA** > **Policy**.
2. Click **New**.



In the Policy Configuration tab, configure the corresponding options.

Option	Description
Name	Type the name of the ZTNA policy. The length is 1 to 95 characters.
User	Select the user/user group to be bound. • AAA Server: Specifies the AAA server that a user/user group belongs to. Select an existing AAA server from the drop-down list. Or, click **New** to create a AAA server. For information about AAA server configuration, refer to Configuring AAA.

Option	Description
	• Select User/Select User Group: Select existing users/user groups. Or, click **New** to create a user/user group. • Input User/User Group: Type the user name/user group name, and then click **Add**. The user name length is 1 to 63 characters. The user group name length is 1 to 127 characters. At most 8 users and 8 user groups can be added.
Endpoint Tag	Select the endpoint tags to be bound. You can select from existing endpoint tags. Or, click **New** to create one. For information about endpoint tag configurations, see Configuring Endpoint Tags. Each policy can be bound with 10 endpoint tags.
Application Resource	Select the application resources/application resource groups to be bound. You can select from existing application resources and application resource groups. Or, click **New** to create one. For information about application resource/application resource group configurations, see Configuring Application Resource/Application Resource Group. Each policy can be bound with 10 application resources and 10 application resource groups.
Action	Select the action to be performed on user traffic hitting the policy, i.e. permitting or denying access to the bound application resources.

Click Threat Prevention to add threat prevention configurations

Option	Description
Anti-Virus	When the system is installed with the anti-virus license, click to

Option	Description
	enable the anti-virus function and bind an anti-virus profile to a ZTNA policy to achieve virus detection on traffic matching the ZTNA policy and process the detected viruses based on the Anti-Virus Profile. For information about file filter, please refer to Anti Virus.
Sandbox	When the system is installed with the sandbox license, click to enable the sandbox function and bind a sandbox profiles to a ZTNA policy to achieve sandbox detection on traffic matching the ZTNA policy. By using the cloud sandbox and the local sandbox technology, the system analyzes the suspicious file and collects the actions of the suspicious file, verifies the legality of the file, gives the analysis result to the system and deals with the malicious file based on the actions set by system. For information about file filter, please refer to Sandbox.
IPS	When the system is installed with the IPS license, click to enable the IPS function and bind an IPS profile to a ZTNA policy to detect network attacks in traffic matching the ZTNA policy and perform actions such as blocking on the attacks based on the IPS Profile. For information about file filter, please refer to Intrusion Prevention System.

Click Data Security to add data security configurations

Option	Description
File Filter	Click to enable the file filter function and bind a file filter profile to the ZTNA policy so as to perform file detection on traffic match-

Option	Description
	ing the ZTNA policy and perform control actions on the file matching the filter conditions based on the file filter profile. For information about file filter, please refer to File Filter.
File Content Filter	Click to enable the file content filter function and bind a file content filter profile to the ZTNA policy so as to perform file content detection on traffic matching the ZTNA policy and perform control actions such as blocking or logging based on the file content filter profile. For information about file filter, please refer to File Content Filter.

Click Options to configure advanced policy configurations.

Option	Description
Schedule	Specify the schedules to be matched. You can select from existing ones. Or, click **New** to create a schedule. For information about schedule configurations, see Creating a Schedule. Each policy can be configured with up to 10 schedules.
Log	You can log ZTNA policy matching in the system logs as required. Multiple options are available. • Deny: Generates logs when the traffic matching the policy is denied. • Session start: Generates logs when the traffic matching the policy starts its session. • Session end: Generates logs when the traffic matching the policy ends its session.

Option	Description
Position	Select a policy position from the **Position** drop-down list. Each ZTNA policy is labeled with a unique ID or name. When ZTNA traffic flows into a device, the device will query for the policy rules by turn, and processes the traffic according to the first matched rule. However, the policy ID is not related to the matching sequence during the query. The sequence displayed in ZTNA policy list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. The default position is the bottom.
Description	Type description for the policy. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.

4. On the Policy page, you can view the configuration information of all policies and manage policy configurations.

   Manage policy configurations on the Policy page

Option	Description
Filter	Select filter conditions from the drop-down list. The policy table will display the policies matching the filter conditions.
Edit/View	• When you select a manually created ZTNA policy, you can click **Edit** to change the policy configuration. • When you select a ZTNA authorization policy, you can click **View** to view details about the ZTNA authorization policy.

Option	Description
	Notes: The ZTNA authorization policy cannot be edited.
Delete	Select a policy and click **Delete** to manually delete the selected policy.
Copy, Paste	Select a policy, click **Copy** and then **Paste**. Select the position from the drop-down list to add a policy with the same configuration and place it at the specified position.
Move	Select a policy, click **Move** and select the position from the drop-down list to change the policy position.

Click " ┆ " and select an option.

Option	Description
Enable	Select a disabled policy and click **Enable** to enable it.
Disable	Select an enabled policy and click **Disable** to disable it.
Default Policy Action	Specify the action to be performed on user traffic that does not hit any ZTNA policies. Select this option. Then, in the displayed dialog box, you can view default policy statistics and configure the following options: • Default Action: Permit or deny access. • Log: Click this button to enable logging of traffic hitting the default policy.
Clearing Policy Hit Count	Select this option. In the displayed dialog box, you can clear corresponding policy statistics by selecting "All Policies", "Default

Option	Description
	Policy" or specifying the policy ID or name.

For more information, refer to the **ZTNA** > **ZTNA Policy** topic in *StoneOS WebUI User Guide*.
FR 44051

Supporting the Huawei Cloud SMS Gateway

WebUI

SMS Gateway

Hillstone Network's security devices can send messages to users via the carrier's SMS gateway or its proxy server. Before configuring this function, you need to first obtain information, such as the SMS gateway address and the device ID for sending short messages, from the carrier.

Notes: These are limitations of Huawei Cloud's SMS gateway. To configure the Huawei Cloud SMS gateway, please read the following restrictions carefully:

- Within any 1-minute period, the Huawei Cloud SMS gateway can send a maximum of 2 SMS messages to the same mobile phone number.
- Within any 24-hour period, the Huawei Cloud SMS gateway can send a maximum of 50 SMS messages to the same mobile phone number.

Prerequisites

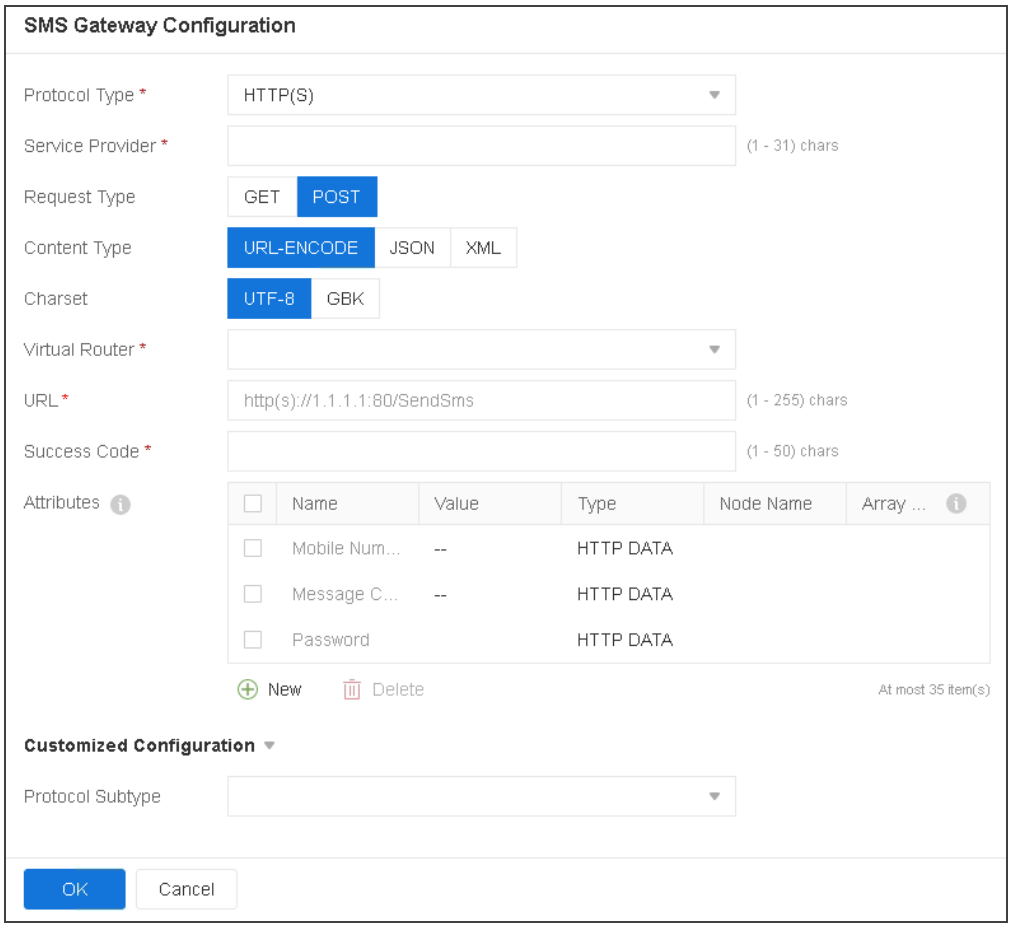
Before sending SMS messages to a specified mobile phone number via the Huawei Cloud SMS gateway and the Alibaba Cloud SMS gateway, please synchronize the system's time and time zone. For more information about how to configure the system time, see the **System Time** or **Configuring NTP** topic.

Configuring SMS Gateway

To configure the SMS gateway, take the following steps:

1. Select **System > SMS Parameters >SMS Gateway**.

2. Click **New**.



Option	Description
Protocol Type	Specifies the protocol of SMS gateway. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates

Option	Description
	the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. ChinaMobileMusic indicates the SMS platform of China Mobile Music. HTTP(S) indicates HTTP/HTTPS protocol.
Service Provider	Specifies the name of the SMS gateway instance. The value range is 1 to 31.
Request Method	When the HTTP (S) protocol type is specified for the SP instance, you need to specify the method of sending HTTP requests tothe SMS gateway. The default request method is POST.
Content Type	When the HTTP (S) protocol type is specified for the SP instance, you need to specify the content type of HTTP Post requests sent to the SMS gateway. By default, URL-ENCODE is selected. • URL-ENCODE - Sets the content type of HTTP POST requests to application/x-www-from-urlencode. • JSON - Sets the content type of HTTP POST requests to application/json. • XML - Sets the content type of HTTP POST requests to XML.
Charset	When the HTTP (S) protocol type is specified for the SP instance, you need to specify the charset of HTTP(S). The

Option	Description
	default charset is UTF-8.
UMS Protocol	When the protocol type is specified as "UMS", users can specify the UMS protocol type. The default protocol type is HTTPS.
Protocol	When the protocol type is specified as "ACC", "ALIYUNSMS", "CAS" or BEIKE, users can specify the protocol type. When the protocol type is specified as "CAS", the default protocol type is HTTPS. The default protocol type is HTTP for ACC and ALIYUNSMS, and HTTPS for BEIKE.
Virtual Router	Specifies the VRouter which gateway belongs to. The system supports multi-VR, and the default VR is trust-vr.
URL	When the HTTP (S) or the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the URL of HTTP(S). You need to enter a complete access path, such as "http(s)://1.1.1.1:80/SendSms". The system requests to communicate with the SMS gateway based on the specified URL address. The range is 1 to 255 characters.
Source Mobile Number	When the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the mobile number used to send verification code messages. The value can be an 8-digit to 21-digit number.
Platform ID	When the ChinaMobileMusic protocol type is specified for the

Option	Description
	SP instance, you can configure the ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. The ID is a 4-digit number.
Platform Password	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the password used to log in to China Mobile Music SMS Platform. The password is provided by China Mobile Music SMS Platform. The password is 1 to 64 characters.
Confirm Password	Re-type the password into the **Confirm Password** box.
Platform Subsystem ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the subsystem ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. The ID is a 3-digit number or 7-digit number.
Template ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the template ID of verification code messages, which is provided by China Mobile Music SMS Platform. The ID is a 1-digit to 21-digit number.
Success code	When the HTTP (S) protocol type is specified for the SP instance, you can specify the success code of HTTP(S). Success code is used to determine whether the SMS gateway successfully sent an authentication message. Refer to the status code in the SMS gateway manual. For example, if an SMS gateway sent an authentication message successfully, the status

Option	Description
	code returned is "OK: 325689", and if failed, the status number returned is "ERROR: eUser". In this instance, you can specify the success code as "OK". The range is 1 to 50 characters.
Root Node	When the protocol type is specified as HTTP(S), request method is specified as POST, and content type is specified as XML, specify the name of the root node of the XML messages sent from the system to the SMS gateway. The name can be 1 to 20 characters in length.
Attributes	When the HTTP (S) protocol type is specified for the SP instance, you can configure attributes to communicate with the SMS gateway. • The mobile number field specifies the parameter name of the mobile number. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The message content field specifies the parameter name of the authentication message. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The password field specifies the parameters of password to log in the SMS gateway. The parameter name and parameter value must exist at the same time or be empty. This is an optional attribute. The range of parameter name is 1 to 20 characters and the range of parameter value is 1 to 255 characters. You can also

Option	Description

	configure Node Name and Array Object for the field.
	• Click **New** and configure the parameter name, parameter value, parameter type, node name, and array object of the custom attribute of the user to log in to the SMS gateway.
	  • Name: The range is 1 to 20 characters.
	  • Value: The range is 1 to 255 characters.
	  • Type: You can set the type to HTTP DATA or HTTP HEADER. If the type is set to HTTP DATA, the attribute will be used as data content of HTTP. If the type is set to HTTP HEADER, the attribute will be added to the header of HTTP.
	  • Node Name: Enter the node name, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system constructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON or XML format. You can configure 10 different node names.
	• Array Object: Sets the attribute to array object. This way, the parameter values are stored in array. To do this, click ×. When ✓ is displayed, it indicates that the attrib-

Option	Description
	ute is set to array object. You can create new attributes as needed, with up to 32 at the same time. Select the check box of the attributes bar and click "Delete". Note: • Node name and array object can be configured only when the method is POST, content type is JSON, and parameter type is HTTP DATA. • For the attribute fields with the same node name, the array object configurations need to be consistent. • The parameter name of the mobile number field, message content field, and password field can be the same. For other attributes, the parameter name can be the same only if the parameter types are different.
Protocol Subtype	If the protocol type is set to HTTP(s), you can select MAS, EMAY, ZGC, ESB, or HW from the drop-down list to connect the Hillstone device to the mobile cloud MAS SMS platform, EMAY SMS, ZGC SMS, ESB SMS platform, or Huawei Cloud SMS platform. To specify the MAS protocol subtype, you need to configure the following attributes in the Attributes section above: • mobiles: Sets the name of the mobile number field to mobiles. This attribute is required.

Option	Description
	• content: Sets the name of the SMS content field to content. This attribute is required. • secretKey: Specifies the name and value of the password used to log in to the SMS gateway. The name needs to be "secretKey" and the value can be 1 to 255 characters in length. This attribute is required. • apId: Click **New** and specify the name, value, and type of the username used to log in to the SMS gateway. The name needs to be "apId", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • ecName: Click **New** and specify the name, value, and type of the enterprise name field. The name needs to be "ecName", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • sign: Click **New** and specify the name, value, and type of the signature code field. The name needs to be "sign", the value is provided by China Mobile Cloud MAS SMS Platform, and the type needs to be "HTTP DATA". This attribute is required. • addSerial: Click **New** and specify the name, value, and type of the extension code field. The name needs to be

Option	Description
	"addSerial", the value is provided by China Mobile Cloud MAS SMS Platform, and the type needs to be "HTTP DATA". This attribute is optional. To specify the ESB protocol subtype, you need to configure the following attributes in the Attributes section above: • MOBILE: Sets the name of the mobile number field to MOBILE. This attribute is required. • MSG: Sets the name of the SMS content field to MSG. This attribute is required. • Password: Sets the parameter name and value of the password field of the ESB SMS platform. You can customize the parameter name, and the parameter value is provided by the ESB SMS platform. This attribute is optional. • CHANNEL_CODE: Click **New** and specify the parameter name, value, and type of the channel name. The parameter name needs to be specified as "CHANNEL_CODE", the parameter value is provided by the ESB SMS platform, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required. • SYS_HEAD: Click **New** and specify the node name "SYS_HEAD" that needs to be included in the XML

Option	Description
	message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value is filled based on the requirements, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required. • BODY: Click **New** and specify the node name "BODY" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value is filled based on the requirements, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required. To specify the HW protocol subtype, you need to configure the following attributes in the Attributes section above: • MOBILE: Sets the name of the mobile number field. You can customize the name. This attribute is required. • MSG: Sets the name of the SMS content field. You can customize the name. This attribute is required.

Option	Description
	• APP_Secret: Specifies the name and value of the password used to log in to the SMS gateway. The name needs to be "APP_Secret" and the value is provided by the Huawei Cloud SMS platform. This attribute is required. • APP_Key: Click **New** and specify the name, value, and type of the username used to log in to the SMS gateway. The name needs to be "APP_Key", the value is provided by the Huawei Cloud SMS platform, and the type needs to be "HTTP DATA". This attribute is required. • sender: Click **New** and specify the name, value, and type of the signature channel code field. The name needs to be "sender", the value is provided by the Huawei Cloud SMS platform, and the type needs to be "HTTP DATA". This attribute is required. • templateId: Click **New** and specify the name, value, and type of the SMS template ID. The name needs to be "templateId", the value is provided by the Huawei Cloud SMS platform, and the type needs to be "HTTP DATA". This attribute is required. Note: • When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS

Option	Description
	platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the charset needs to be "UTF-8". • When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON". • When you specify the ESB protocol subtype, to connect the Hillstone device to the ESB SMS platform, the request type needs to be "POST" and the content type needs to be "XML". • When you specify the HW protocol subtype, to connect the Hillstone device to the Huawei Cloud SMS platform, the request type needs to be "POST".
Host	Specifies the gateway address.
Port	Specifies the port number of the gateway. When the protocol type is specified as "SGIP", the default port number is 8801; When the protocol type is specified as "ACC", the default port number is 80; When the protocol type is specified as "BEIKE", the default port number is 8086; When the protocol type is specified as "UMS", the default port number is 9600. When the protocol type is specified as "XUANWU" or "CAS", the default port number is 8080.
Device Code	Specifies the device code, the range is 1 to 4294967295. When the protocol type is specified as "SGIP", and before con-

Option	Description
	figuring the SMS gateway, you have to ask your supplier to provide the device ID of SP, which sends the SMS messges.
Source Number	When the protocol type is specified as "SGIP", and aftering enabling the SMS Authentication function, the system will send an Auth-message to the mobile phone number. Specifies the user's phone number, the range is 1 to 21.
Company Code	When the protocol type is specified as "UMS", users can specify the enterprise code registered on the UMS platform. The range is 1 to 31 digits.
Username	Specifies the username to log in SMS gateway. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Password	Specifies the password for the user. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Template Name	Specifies the template parameter of BEIKE SMS gateway.
Confirm Password	Re-type the password into the **Confirm Password** box to confirm.
Change Password	When you edit the SMS gateway, you can see the Change Password function. After you enable this function, the Password field is displayed. To change the password, enter a new one in this field and save the configuration.

Option	Description
SMS Limit/hour	Defines the maximum message number the gateway can send in one hour.
SMS Limit/day	Defines the maximum messages number the gateway can send in one day.
AccessKeyId	Specifies the AccessKeyId which will be used as the username for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the template AccessKeyId applied in the SMS of Alibaba Cloud.
AccessKeySecret	Specifies the AccessKeySecret which will be used as the password for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the template AccessKeySecret applied in the SMS of Alibaba Cloud.
Confirm AccessKeySecret	Re-type the AccessKeySecret to confirm.
Trading Code	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the trading code. The range is 1-7.
Channel	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the channel. The range is a-z.
Request Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the request type. The range is 1-6.

Option	Description
Organization Code	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the organization code. The range is 1-31.
SMS Service Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the SMS service type. The range is 1-31.
Send Sign Code	When the protocol type is specified as "ACC", select the **Enable** check box to enable the Send Sign Code function. When this function is enabled, the ACC SMS gateway will add a sign code field when sending a request to the ACC server, which will prevent the content of the SMS from being tampered with.

Testing SMS

To test if the message sending works, you can send a test text to a mobile.

To send a text message to a specified mobile number, take the following steps:

1. Select **System > SMS Parameters >SMS Gateway**.
2. Click the "SMS test" link in the **SMS Test** column of the SMS gateway list.
3. In the **Mobile Phone Number** dialog box, enter a mobile phone number in the text box.
4. In the **Test Message Content** dialog box, enter the content of text messages sent to the specified phone number. The default value is "This is a test message, please don't feedback!".
    - If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the value range of the content of text messages is 0 to 6 characters.

- If you are sending a test message to a specified mobile phone number via the Huawei Cloud SMS gateway, you do not need to perform this step and can proceed directly to the next step.

5. Click **Send**. If the SMS modem is correctly configured and connected, the phone using that number will receive a text message; if it fails, an error message will indicate where the error is.

For more information, refer to the **System Management** > **SMS Parameters** > **SMS Gateway** topic in *StoneOS WebUI User Guide*. FR 42378

CLI

SMS Gateway Authentication

Hillstone Network's security devices can send messages to users via the carrier's SMS gateway or its proxy server. Before configuring this function, you need to first obtain information, such as the SMS gateway address and the device ID for sending short messages, from the carrier.

SMS gateway authentication configuration includes:

1. Create a Service Provider(SP) instance.
2. Bind the SP instance to a configured SSL VPN tunnel, and enable the SMS gateway authentication function.

Notes: These are limitations of Huawei Cloud's SMS gateway. To configure the Huawei Cloud SMS gateway, please read the following restrictions carefully:

- Within any 1-minute period, the Huawei Cloud SMS gateway can send a maximum of 2 SMS messages to the same mobile phone number.
- Within any 24-hour period, the Huawei Cloud SMS gateway can send a maximum of 50 SMS messages to the same mobile phone number.

Creating an SP Instance

In the SP instance configuration mode, you can configure as follows:

- Specifying the VRouter
- Specifying the Request Method
- Specifying the Charset
- Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol
- Specifying the URL
- Specifying Source Mobile Number
- Configuring Platform ID
- Configuring Platform Password
- Configuring Platform Subsystem ID
- Configuring Template ID
- Specifying the Success Code
- Configuring the root node
- Specifying the Attributes
- Configuring the protocol subtype
- Specifying the Gateway Address and Port Number
- Specifying the Number to Send Auth-message
- Specifying the Device ID
- Specifying the Username and Password

- Specifying the Template Parameter
- Specifying a Maximum SMS Number
- Enabling/Disabling the Sending Sign Code Function
- Sending a test message
- Specifying the Company Code
- Specifying the AccessKeyId
- Specifying the AccessKeySecret
- Specifying Instance of SMS Gateway
- Enabling/Disabling SMS Gateway Authentication
- Specifying the Sender Name or Sign Name
- Specifying the Template Code
- Specifying the Request Type
- Specifying the Organization Code
- Specifying the SMS Service Type
- Specifying the Trading Code
- Specifying the Channel

……

Configuring the Protocol Subtype

When the SP instance uses the HTTP(s) protocol type, you can configure the MAS, EMAY, ZGC, ESB, or HW protocol subtype to connect the Hillstone device to the mobile cloud MAS SMS

platform, EMAY SMS platform, ZGC SMS, ESB SMS platform, or Huawei Cloud SMS platform. To configure the protocol subtype, run the following command in SP instance configuration mode:

subtype { **mas** | **emay** | **zgc** | **esb** | **hw**}

In SP instance configuration mode, run the **no subtype** command to delete the MAS, EMAY, ZGC, ESB, or HW protocol subtype configuration.

When you specify the MAS protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- mobiles: In SP instance configuration mode, run the **default-attribute phone-attr-name mobiles** command to set the name of the mobile number field to mobiles. This attribute is required.
- content: In SP instance configuration mode, run the **default-attribute msg-content-attr-name content** command to set the name of the SMS content field to content. This attribute is required.
- secretKey: In SP instance configuration mode, run the **password-attribute secretKey** *password-value* command to set the name of the password used to log in to the SMS gateway to secretKey. The *password-value* can be 1 to 255 characters in length. This attribute is required.
- apId: In SP instance configuration mode, run the **user-attribute apId** *value* command to set the username used to log in to the SMS gateway to apId. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.
- ecName: In SP configuration mode, run the **user-attribute ecName** *value* command to set the name of the enterprise name field to ecName. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.
- sign: In SP instance configuration mode, run the **user-attribute sign** *value* command to set the name of the signature code field to sign. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is required.

- addSerial: In SP instance configuration mode, run the **user-attribute addSerial** *value* command to set the name of the extension code field to addSerial. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is optional.

To specify the ESB protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- MOBILE: In SP instance configuration mode, use the **default-attribute phone-attr-name MOBILE** command to set the parameter name of the mobile number field to "MOBILE". This attribute is required.
- MSG: In SP instance configuration mode, use the **default-attribute msg-content-attr-name MSG** command to set the parameter name of the SMS content field to "MSG". This attribute is required.
- Password: In SP instance configuration mode, use the **password-attribute***password-name password-value* command to specify the parameter name and parameter value of the password field of the ESB SMS platform. You can customize the parameter name *password-name*, and the parameter value *password-value* is provided by the ESB SMS platform. This attribute is optional.
- CHANNEL_CODE: In SP instance configuration mode, use the **user-attribute CHANNEL_CODE***value* command to specify the parameter name "CHANNEL_CODE" of the channel name; the parameter value *value* is provided by the ESB SMS platform; the parameter type is "HTTP DATA" by default. This attribute is required.
- SYS_HEAD: In SP instance configuration mode, use the **user-attribute** {*parameter-name value*} [**node SYS_HEAD**] command to specify the node name "SYS_HEAD" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name *parameter-name* is provided by the ESB SMS platform and needs to be capitalized

when configuring, the parameter value *value* is filled based on the requirements, and the parameter type is specified as "HTTP DATA" by default. This attribute is required.

- BODY: In SP instance configuration mode, use the **user-attribute** {*parameter-name value*} [**node BODY**] command to specify the node name "BODY" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name *parameter-name* is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value *value* is filled based on the requirements, and the parameter type is specified as "HTTP DATA" by default. This attribute is required.

To specify the HW protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- MOBILE: In SP instance configuration mode, use the **default-attribute phone-attr-name***phone-attr-name* command to set the parameter name of the mobile number field. This attribute is required.
- MSG: In SP instance configuration mode, use the **default-attribute msg-content-attr-name** *msg-content-name* command to set the parameter name of the SMS content field. This attribute is required.
- APP_Secret: In SP instance configuration mode, use the **password-attribute APP_Secret***password-value* command to set the parameter name of the user password field used to log in to the SMS gateway to "APP_Secret"; and the value *password-value* is provided by the Huawei Cloud SMS platform. This attribute is required.
- APP_Key: In SP instance configuration mode, use the **user-attribute APP_Key***value* command to set the parameter name of the username used to log in to the SMS gateway to "APP_Key"; and the value *value* is provided by the Huawei Cloud SMS platform. By default, the parameter type is "HTTP DATA". This attribute is required.

- sender: In SP instance configuration mode, use the **user-attribute sender***value* command to set the parameter name of the signature channel code to "sender"; and the value *value* is provided by the Huawei Cloud SMS platform. The parameter type is "HTTP DATA". This attribute is required.
- templateId: In SP instance configuration mode, use the **user-attribute templateId***value* command to set the parameter name of the SMS template ID to "templateId", and the value *value* is provided by the Huawei Cloud SMS platform. The parameter type is "HTTP DATA". This attribute is required.

Notes:

- When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the chartset needs to be "UTF-8".
- When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON".
- When you specify the ESB protocol subtype, to connect the Hillstone device to the ESB SMS platform, the request type needs to be "POST" and the content type needs to be "XML".
- When you specify the HW protocol subtype, to connect the Hillstone device to the Huawei Cloud SMS platform, the request type needs to be "POST".

Sending a Test Message

To test if the device works properly, you can send a test message to a phone number. To send a test message, in any mode, use the following command:

exec sms sp *sp-name* **send test-message to** *phone-number* [**test-msg-content** *content*]

- *sp-name* - Specifies the phone number.
- *phone-number* – Specifies the tunnel name which bound the SP instance.
- *content* – Specifies the content of the test message. The default value is "This is a test message, please don't feedback!". The range is 1 to 64 characters.

> **Notes:** When you send a test message to the specified mobile number via the Huawei Cloud SMS gateway, you need to execute the **exec sms sp***sp-name***send test-message to***phone-number* command.

If the phone of the test number does not receive the test message, the system will record a log with description about failure reason.

For more information, refer to the **VPN** > **SSL VPN** > **Configuring SSL VPN Server** > **Two-Step Verification** > **SMS Authentication** section in *StoneOS CLI User Guide*.

Optimizing the Link Load Balancing Function

WebUI

Outbound Link Load Balancing

In the outbound direction, for multi-ISP links, the system can reasonably allocate traffic to the corresponding ISP link based on the ISP of the destination address; it can also use real-time link monitoring technology, dynamic link detection technology, and other load balancing algorithms to distribute traffic across different links, achieving a more balanced bandwidth utilization.

You can configure flexibleSLA profiles and LLB Profiles and bind them with routing (the system only supports destination-based routes and policy-based routes) to form LLB rules, which can control and load balance outbound link traffic.

Notes: If an LLB rule is bound to both an LLB profile and an SLA profile, the SLA profile will only take effect when any of the options in the LLB profile's preferred scheduling algorithm, secondary scheduling algorithm, or alternative scheduling algorithm use the "Dynamic Proximity" algorithm.

Outbound Load Balancing Procedure

Currently, the load balancing procedure for outbound link traffic by SG-6000 A seriesK series (except K9180/K6580)CloudEdge is as follows:

1. For outbound link traffic, match the session persistence and load balancing algorithms in sequence.
2. If session persistence matches, the device will directly select the link in the session persistence.
3. If session persistence is not matched, the device will select routes for outbound traffic based on the load balancing algorithm among the less busy links.
4. If the ISP load balancing algorithm matches, the device selects routes based on the ISP to which the traffic destination address belongs. If multiple available ISP links match, the device then continues to select routes for the traffic based on the secondary load balancing algorithm; if no corresponding ISP link matches, the device will select routes for the traffic based on the alternative load balancing algorithm.
5. If it matches other load balancing algorithms, the device selects routes based on the specified load balancing algorithm.
6. The device forwards traffic through the selected link.

Notes:

- If the session persistence function is enabled, when selecting the outbound link for outbound traffic, session persistence is prioritized for matching. Then, the link matched in the session persistence table is used to forward the traffic.
- If no session persistence table match is found or the session persistence function is not enabled, the system will select an outbound link for traffic based on the load balancing algorithm among the non-busy links; if all links are busy, the system will select the route to forward the traffic based on ECMP.

The load balancing procedure for outbound link traffic by SG-6000 X seriesK9180/K6580 is as follows:

1. LLB calculates the cost of each link based on key parameters such as the delay weight, packet loss weight, jitter weight, and bandwidth weight of each link.
2. The system allocates more outbound traffic to links with lower overhead, while reducing traffic allocation on links with higher overhead, achieving efficient and balanced outbound traffic load.

Configuration Method

Please follow the steps below to configure outbound load balancing:

1. Configure the link information of the interface to ensure that the system can achieve intelligent routing based on the priority, weight, and bandwidth threshold of link load balancing configured for the interface. For more information, see the **Interface > Configuring an Interface** topic.
2. Configure an LLB profile

   The LLB profile contains parameters for multiple load balancing algorithms and algorithms, allowing you to flexibly configure settings such as preferred scheduling algorithm, secondary

algorithm, backup scheduling algorithm, priority scheduling policy, balancing mode, bandwidth utilization threshold, detection switch, detection mode, balancing direction, and the impact factor of link Cost value. The system will select links and balance traffic based on the specified load balancing algorithm and related configuration. In the following example, the "dynamic proximity" is used and the link detection function is enabled:

- For SG-6000 X seriesK9180/K6580, if the balancing mode is the compatibility mode, the system will select the original link (cached link) for traffic forwarding. This mode is suitable for businesses sensitive to link switching, such as banking services.
- For SG-6000 A seriesK series (except K9180/K6580)CloudEdge, if the session persistence function is enabled, the system prioritizes matching session persistence when selecting outbound links for outbound traffic. It then uses the link matched in the session persistence table to forward the traffic. This mode is suitable for businesses sensitive to link switching, such as banking services.
- When the preferred load balancing algorithm is "Dynamic Proximity,", if the link detection function is enabled and no domain name book is bound in the LLB rule, the system will detect the network link status based on the configured parameters to select the optimal link:
    - When the link's bandwidth utilization is below the specified threshold, the system calculates link quality based on latency weight, packet loss weight, and jitter weight, prioritizing links with a higher quality.
    - When the link's bandwidth utilization exceeds the specified threshold, the system calculates link quality based on latency weight, packet loss weight, jitter weight, bandwidth weight, link bandwidth, and bandwidth utilization, prioritizing links with a higher quality.

- When the preferred load balancing algorithm is "Dynamic Proximity,", if link detection is enabled and LLB rules are bound to a domain name book, the system will use real-time detection technology for domain names to ensure more accurate route selection. This method is suitable for link selection within specific domain name:
    - When the client's access request matches the bound domain name book, the system will actively detect the quality of the corresponding outbound link and use the results of the active detection as the basis for route selection.
    - When the client's access request does not match the bound domain book, if the link bandwidth utilization is below the specified bandwidth utilization threshold, the system will calculate the link quality based on delay weight, packet loss weight, and jitter weight, and prioritize selecting high-quality links; if the link bandwidth utilization is above the configured bandwidth utilization threshold, the system will calculate the link quality based on delay weight, bandwidth weight, link bandwidth, and bandwidth utilization, and prioritize selecting high-quality links.

> **Notes:** By default, link detection is enabled. You can use the **show llb profile** command to view the status of link detection. If the function is disabled, it can be enabled by using the **dynamic-extra-confdetect enable** command.

3. Configure an LLB rule

   By configuring LLB rules, LLB profiles are bound to routes (the system only supports destination-based routes and policy-based routes) to control and load balance outbound link traffic.

If you need to filter the outbound links for traffic based on customized link quality criteria (such as latency, jitter, and packet loss rate), you can configure an SLA Profile. By using the SLA Profile to filter out links that meet the SLA standards, and binding the SLA Profile together with the LLB Profile to the route, you can achieve more precise control and balancing of link traffic.

Link Load Balancing Algorithm

The system supports multiple link load balancing algorithms for outbound traffic, including:

Algorithm	Description
Dynamic Proximity	When the LLB rule is not bound to a domain name book, the device will adopt a passive detection method to obtain the delay, jitter, packet loss rate, and bandwidth utilization of each link. • Link detection function enabled: When the link bandwidth utilization is below the specified interface bandwidth threshold, the system will only calculate the link quality based on latency, packet loss, and jitter, prioritizing links with higher quality; when the link bandwidth utilization exceeds the specified interface bandwidth threshold, the system will take into account latency, packet loss, jitter, and bandwidth utilization to calculate the link quality, prioritizing links with higher quality. • Link detection function disabled: The system selects routes based solely on the bandwidth utilization of each egress link, prioritizing links with lower bandwidth utilization.
	When the LLB rule is bound to the domain name book, the device will adopt a combination of active and passive detection methods to obtain the latency, jitter, packet loss rate, and bandwidth utilization of each link.

Algorithm	Description
	• Link detection function enabled: ◦ If the client's access request matches the bound domain name book, the system will actively detect the quality of the corresponding egress link and then use the results of the active detection as the basis for route selection. ◦ If the client's access request does not match the bound domain book, when the link bandwidth utilization is below the specified interface bandwidth threshold, the system will only calculate the link quality based on latency, packet loss, and jitter, prioritizing the link with higher quality; when the link bandwidth utilization is above the specified interface bandwidth threshold, the system will comprehensively consider latency, packet loss, jitter, and bandwidth utilization to calculate the link quality, prioritizing the link with higher quality. • Link detection function disabled: The system selects routes based solely on the bandwidth utilization of each egress link, prioritizing links with lower bandwidth utilization.
Hash Dst IP	Hash the destination address of the traffic, and select the route based on the result of the hash operation.
Weighted Hash Dst IP	Based on the hash of the destination IP, the device selects routes based on the weight of the interfaces in proportion.

Algorithm	Description
	When new outbound traffic arrives, the greater the interface weight, the more traffic is forwarded through the corresponding egress link.
Hash Src IP	Hash the source address of the traffic, and select the route based on the result of the hash operation.
Weighted Hash Src IP	Based on the source IP hash, the device selects routes based on the weight of the interfaces in proportion. When new outbound traffic arrives, the greater the interface weight, the more traffic is forwarded through the corresponding egress link.
Hash Src IP Port	Hash the source address and port of the traffic, and select the route based on the result of the hash operation.
Weighted Hash Src IP Port	Based on the source IP port hash, the device selects routes based on the weight of the interfaces in proportion. When new outbound traffic arrives, the greater the interface weight, the more traffic is forwarded through the corresponding egress link.
ISP	Match the destination address of the traffic with ISP information of the system, and route based on the matching results.
Least Bandwidth	The device records the upstream bandwidth, downstream bandwidth, or the total of upstream and downstream bandwidth on each interface. When new outbound traffic arrives, the device will select the interface with the minimum bandwidth or total bandwidth for forwarding.
Weighted Least Bandwidth	On the basis of minimum bandwidth, the device selects routes based on the weight of the interfaces in proportion. When new outbound traffic arrives, it will select the link with the smallest

Algorithm	Description
	ratio of current bandwidth (total) to interface weight. (Calculation method: upstream bandwidth, downstream bandwidth, or the total of upstream and downstream bandwidth divided by the interface weight).
Least Connection	The device records the number of connections on each interface. When new outbound traffic arrives, the device will select the interface with the fewest connections for forwarding.
Weighted Least Connection	On the basis of least connection distribution, the device selects routes based on the weight values of the interfaces in proportion. When new outbound traffic arrives, it will choose the link with the smallest ratio of current connections to interface weight (Calculation method: number of connections on the interface divided by interface weight).
Round Robin	The device distributes traffic in rotation to each egress link.
Weighted Round Robin	On a polling basis, the device selects routes based on the weight of the interface. The greater the interface weight, the more egress link traffic it corresponds to.

Configuring Outbound Link Load Balancing

Before you start

- **Read** Outbound Link Load Balancing
- **Read** Outbound Load Balancing Procedure
- **Read** Link Load Balancing Algorithm

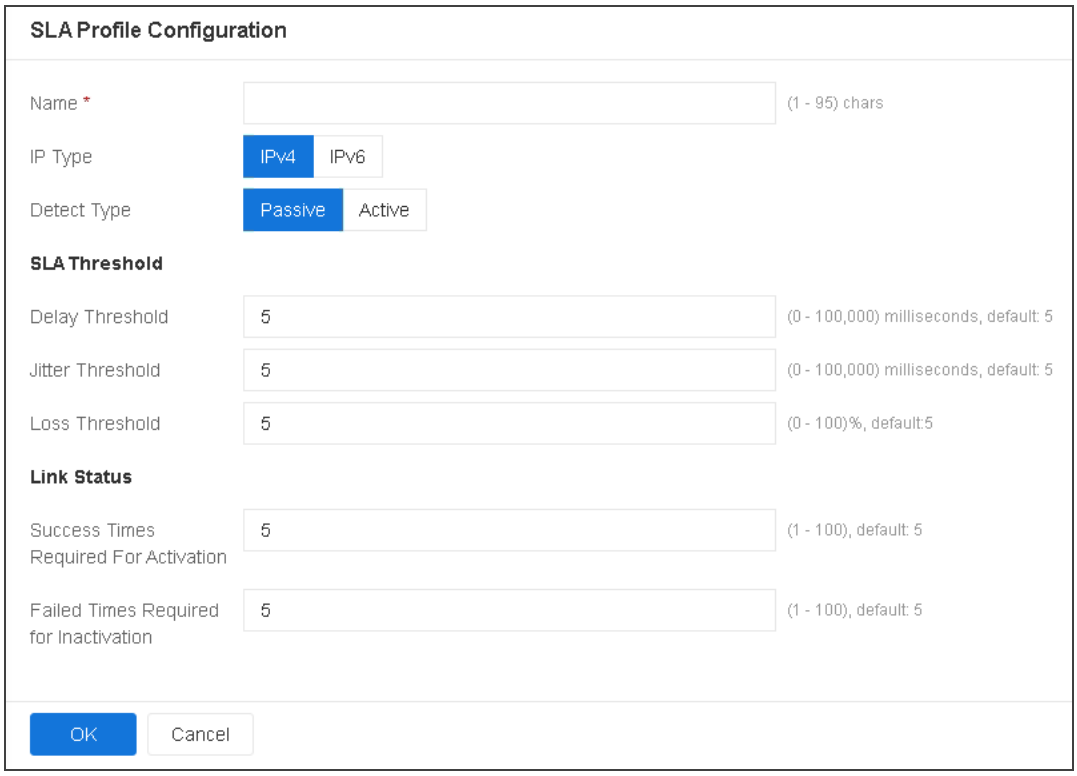
Prerequisites

Complete the link configuration of the interface in advance to ensure that the system can achieve intelligent routing based on information such as the priority, weight, and bandwidth threshold of the link load balancing. For more information, see **Interface** > **Configuring an Interface**.

Configuring SLA Profile

To configure an SLA profile, take the following steps:

1. Select **Network** > **Outbound LLB** > **SLA Profile**.
2. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The

Option	Description
	default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode. • Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detec-

Option	Description
	tion mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.
SLA Threshold	
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available

Option	Description
	outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

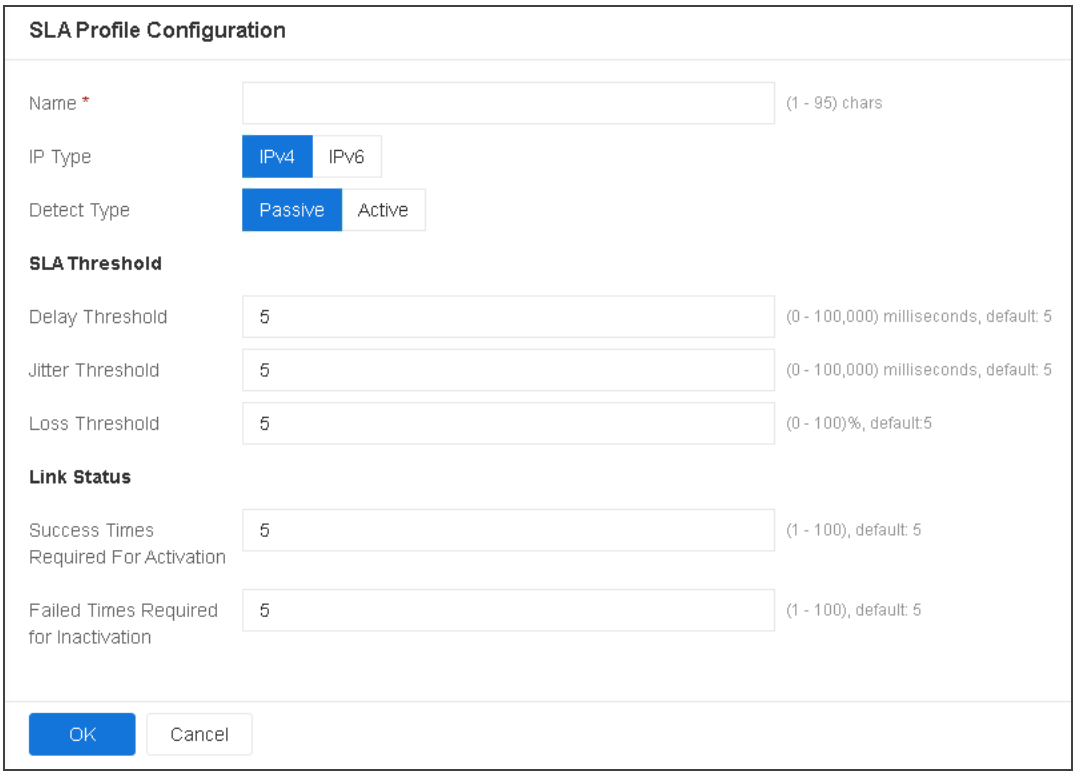
3. Click **OK**.

4. On the **SLA Profile** page, you can also perform the following operations:

    - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
    - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
    - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
    - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.

5. Select **Network** > **Outbound LLB** > **SLA Profile**.

6. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.

Option	Description
	• Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.
SLA Threshold	
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is per-

Option	Description
	formed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deac-

Option	Description
	tivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

7. Click **OK**.
8. On the **SLA Profile** page, you can also perform the following operations:
    - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
    - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
    - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
    - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.
9. Select **Network** > **Outbound LLB** > **SLA Profile**.

10. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.

Option	Description
	• Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.
SLA Threshold	
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is per-

Option	Description
	formed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deac-

Option	Description
	tivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

11. Click **OK**.

12. On the **SLA Profile** page, you can also perform the following operations:

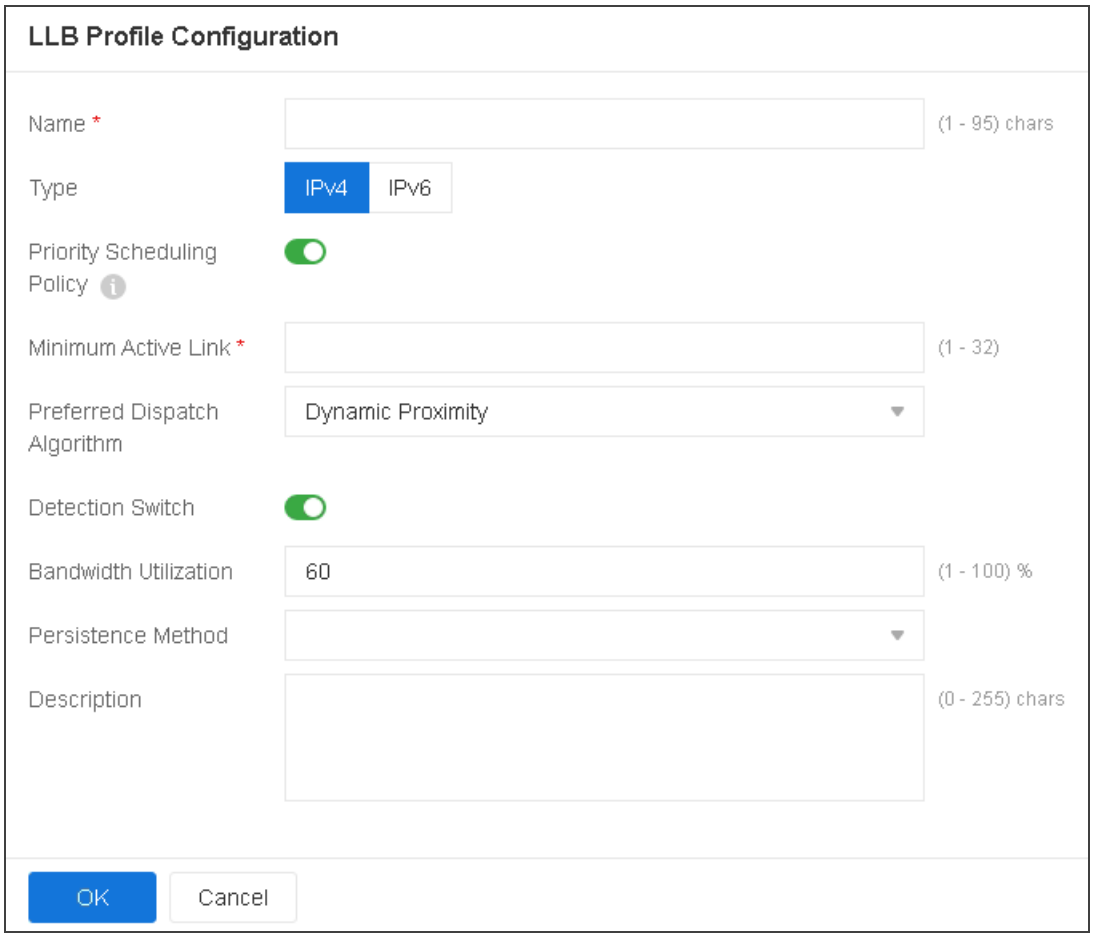
    - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
    - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
    - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
    - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.

Configuring LLB Profile

To configure an LLB profile, take the following steps:

1. Select **Network > Outbound LLB > LLB Profile**.

2. Click **New**.





3. In the LLB Profile Configuration page, configure as follows:

Option	Description
Name	Specifies the LLB Profile name whose length range is 1-95 characters.
Type	Specifies the IP type of the LLB Profile as IPv4 or IPv6. The default type is IPv4.
Priority Scheduling Policy	Click Enable to enable the priority scheduling policy for link load balancing and specify the minimum number of active links. The minimum number of active links is the minimum number of links participating in the link load balancing scheduling, with a value range of 1 to 32. The priority of the device's outbound links is determined by the link load balancing priority of their corresponding interfaces. For example, if there are 10 outbound links on the device and the minimum number of active links is 6, then based on the pri-

Option	Description
	ority ranking of the outbound links corresponding to the interfaces, all available links with the highest priority will be prioritized to join the scheduling; if the number of links with the highest priority is less than 6, all available links with the next priority will be added to the scheduling. This process continues until the number of available links participating in the scheduling is greater than or equal to 6 or all available links have participated in the scheduling. When a link that participates in the scheduling becomes unavailable, causing the actual number of links participating in the scheduling to be less than 6, the device will continue to select all available links with the highest priority from the links not yet participating in the scheduling until the condition is met; when high-priority links become available again, they will rejoin the scheduling. For example, the link load balancing priorities of interfaces eth0/1, eth0/2, eth0/3, and eth0/4 are 10, 20, 30, and 20, respectively; the ISPs of interfaces eth0/1, eth0/2, eth0/3, and eth0/4 are China-telecom, China-telecom, China-telecom, and China-mobile, respectively. The preferred balancing algorithm of the LLB profile is "ISP", and the secondary algorithm is "Round Robin". The priority scheduling policy is enabled, and the minimum number of active links is 2. Other options remain at default settings, and associate LLB rules with the LLB profile. After customers using the telecom operator send requests to the device, because the LLB balancing algorithm is ISP, the out-

Option	Description
	bound links corresponding to interfaces eth0/1, eth0/2, and eth0/3 will participate in the scheduling; since interfaces eth0/1 and eth0/2 have higher priority, the device will ultimately round-robin distribute the telecom client request to interfaces eth0/1 and eth0/2. By default, it is disabled.
Preferred Dispatch Algorithm	Specifies the preferred algorithm for balancing. After configuring this option, the system will route the outbound traffic based on the specified algorithm. The default system algorithm is "Dynamic Proximity". For more information, see Link Load Balancing Algorithm. **Notes:** When the load balancing algorithm for outbound traffic is set to "Minimum Bandwidth" or "Weighted Minimum Bandwidth", you can specify the statistical period of traffic bandwidth as needed.
Balance Direction	When the preferred balancing algorithm is "Minimum Bandwidth" or "Weighted Minimum Bandwidth", you need to specify the direction of traffic load balancing, i.e., calculate the actual bandwidth of the link based on the specified data flow direction. • Upstream - The system will calculate the bandwidth in the outgoing direction of the data flow and adjust the routing method accordingly. • Downstream - The system will calculate the bandwidth in the incoming direction of the data flow and adjust the rout-

Option	Description
	ing method accordingly. • Bidirectional - The system will calculate the sum of the bandwidths in both the incoming and outgoing directions of the data flow and adjust the routing method accordingly. This parameter is the default direction.
Secondary Algorithm	When the preferred balancing algorithm is "ISP", you need to specify the secondary algorithm for balancing. If multiple links match the ISP of the destination IP of the traffic, the secondary algorithm will be used to reroute the traffic among these links.
Alternative Dispatch Algorithm	When the preferred dispatch algorithm is "ISP", you need to specify the alternative dispatch algorithm. If the system cannot match suitable links for the traffic through the preferred dispatch algorithm, the alternative dispatch algorithm will be used to reroute the traffic.
Detection Switch	When the preferred balancing algorithm is "Dynamic Proximity", the link detection function can be enabled. By default, this function is enabled. When the link detection function is enabled, the device will use a combination of active and passive detection methods to detect the network link status based on various configured parameters for link status detection, and then select the optimal route. For more information about the priority of optimal route selection, see the introduction of the dynamic proximity algorithm in the Link Load Balancing Algorithm. When disabled, the system will only select routes based on the bandwidth

Option	Description
	utilization of each outbound link, giving priority to links with lower bandwidth utilization. For the various configured parameters of link status detection, refer to the "Configure Outbound Load Balancing > Configure LLB Profile > Configuring Link Detection Function > Configure Weights for Calculating Link Status" section in the *StoneOS CLI User Guide*.
Comprehensive	Click Enable to enable the comprehensive dispatch function for link load balancing. When the balancing algorithm is set to "Round Robin" or "Weighted Round Robin", the system will integrate the session persistence algorithm results for link scheduling and perform intelligent routing. When new outbound traffic arrives, the system will prioritize selecting the link carrying less traffic based on the current traffic load of each link. By default, it is disabled.
Persistence Method	Specifies the session persistence method for link load balancing, and the system will select the same outbound link for traffic that meets certain conditions. It can be: • Source IP and Destination IP: For traffic from the same client with the same destination address, select the same link for forwarding. • Source IP: For traffic from the same client, select the same link for forwarding. • Destination IP: For traffic with the same destination

Option	Description
	address, select the same link for forwarding. **Note:** You can configure busy protection for outbound links. When the outbound traffic of a link reaches the bandwidth threshold specified by the interface, if the system selects an outbound link for the traffic through the load balancing algorithm, it will prioritize other non-busy links; if the system selects an outbound link for the traffic through the session persistence algorithm and matches the corresponding session persistence table item, it will ignore the busy protection function and select the matched link to forward the traffic. For more information about the bandwidth threshold configuration, see Configuring the Bandwidth Threshold of Interface.
Timeout	Specifies the timeout time for session persistence. After exceeding the specified time value, the device will clear the corresponding data traffic information. The value range is 60 to 65535 seconds, with a default value of 300 seconds.
Balance Mode	There are two equalization modes: High Performance and High Compatibility. • High Performance - In this mode, system adjusts link to keep the link balance as fast as possible • High Compatibility - 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

Option	Description
	mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.
Bandwidth Utilization	When the preferred dispatch algorithm is "Dynamic Proximity", you can specify Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth, system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.
Weight Factors	The system selects routes based on the Cost value of each link, where a smaller Cost value indicates a more favorable link. "Weight Factors" is used to calculate the Cost value of a link, including parameters such as latency, jitter, packet loss rate, and bandwidth weight. These factors indicate the proportion of weight that latency, jitter, packet loss rate, and bandwidth have on the Cost value of the link. The weight factors of the Cost value of a link include the following options: • User-defined: You can customize the weight of latency, jitter, packet loss rate, and bandwidth of link. When you select this option, you need to specify the weight of latency, jitter, packet loss rate, and bandwidth for the Cost value of the link in subsequent configuration items.

Option	Description
	• Delay First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 10, 2, 4, and 1, respectively, indicating that latency has the greatest impact on the Cost value of the link. • Jitter First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 10, 4, and 1, respectively, indicating that jitter has the greatest impact on the Cost value of the link. • Loss First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 2, 10, and 1, respectively, indicating that packet loss rate has the greatest impact on the Cost value of the link.
Delay Weight	Specifies the proportion of weight that latency has on the Cost value of the link. Valid values: 0 to 15. Default value: 1.
Jitter Weight	Specifies the proportion of weight that jitter has on the Cost value of the link. Valid values: 0 to 15. Default value: 2.
Loss Weight	Specifies the proportion of weight that packet loss rate has on the Cost value of the link. Valid values: 0 to 15. Default value: 4.
Bandwidth Weight	Specifies the proportion of weight that bandwidth has on the Cost value of the link. Valid values: 0 to 15. Default value: 1.
Description	Configure Additional details for the LLB profile.

4. Click **OK**.

5. On the **LLB Profile** page, you can also perform the following operations:

    - Edit LLB profile: Select an LLB profile and click **Edit** to edit the profile.
    - Delete LLB profile: Select one or more LLB profiles and click **Delete** to delete them.

Notes:

- Changing the IP type is not allowed when editing the LLB Profile.
- Non-root VSYS does not support to configure functions related to load balancing algorithms, such as bandwidth statistics period, priority scheduling policies for link load balancing, comprehensive consideration of other scheduling results, load balancing algorithms, and session persistence methods.

Specifying the Statistical Period of Bandwidth

When the load balancing algorithm of outbound traffic is configured as "Minimum Bandwidth" or "Weighted Minimum Bandwidth," you can specify the statistical period for traffic bandwidth as required. To do this, take the following steps:

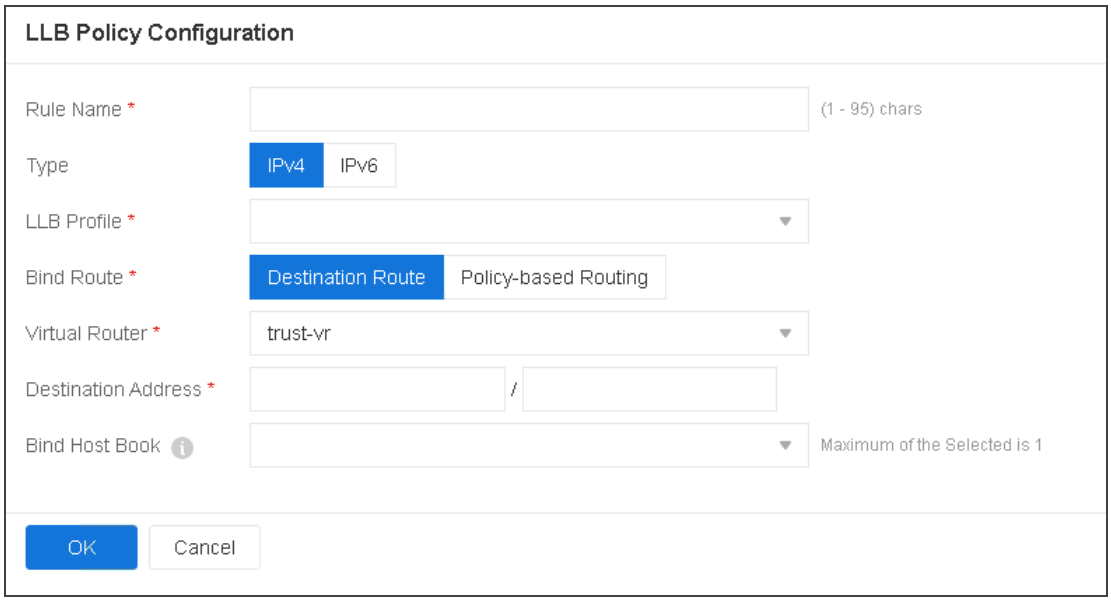
1. Select **Network > Outbound LLB > LLB Profile**.
2. Click **Bandwidth Statistics Period Dispose** above the list. In the **Bandwidth Statistics Period Dispose** panel, specify the statistical period for traffic bandwidth. The value range is 1 to 300 seconds, with a default value of 120 seconds.

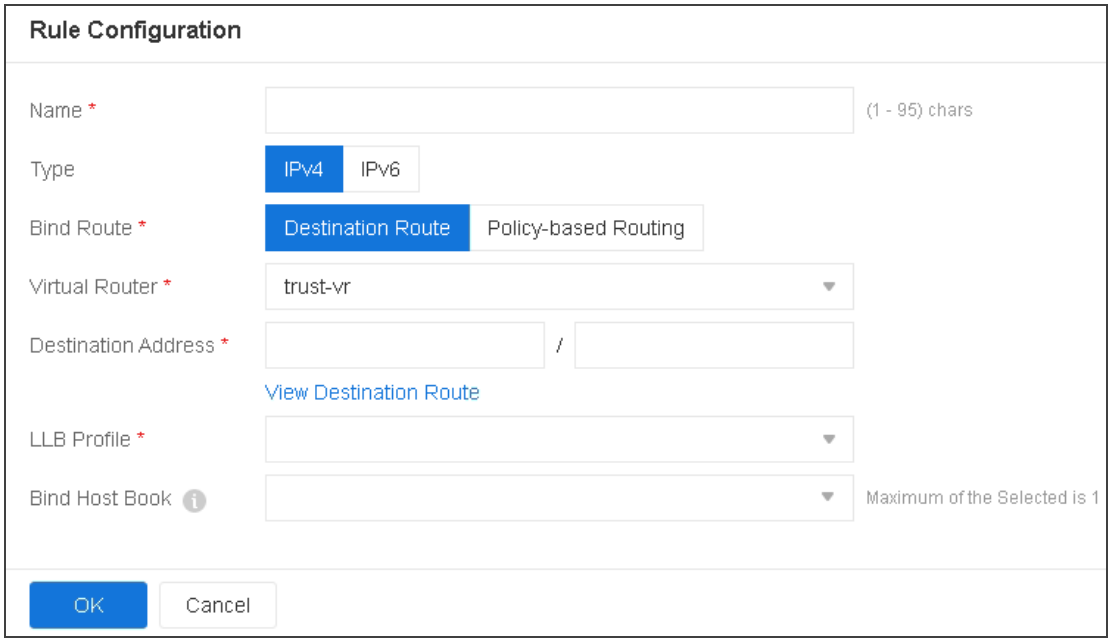
Configuring LLB Rule

To bind SLA profile (optional) and LLB profile to the route to form an LLB rule, which can control and load balance outbound link traffic, take the following steps:

1. Select **Network > Outbound LLB > Rule**.

2. Click **New**.





3. In the LLB Policy Configuration page, configure the following:

Option	Description
Name	Specifies the Rule name, length of 1-96 characters
Type	Specifies the type of the LLB Rule as IPv4 or IPv6. The default type is IPv4.
Bind Route	Specify the route to be bound in the rule: Destination Route or Policy Based Route. • Destination Route - When this option is selected, specify the virtual router and destination address of the destination route. • Policy Based Routing - Select this option to specify the name and id of the policy route. The IP type of PBR rule should be the same as the LLB Rule. If the IP tyoe of LLB Rule is IPv6, the IP type of PBR rule should be IPv6 as well.
Virtual Router	Specifies the name of the virtual router in the drop-down menu. The default vrouter is trust-vr.
Destination Address	Specifies the Vrouter destination address. When the type of the LLB Rule is specifies as IPv6, use *X:X:X:X::X/M* to configure the destination address of Vrouter. When the type of the LLB Rule is specifies as IPv4, the device supports two modes, A.B.C.D / M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
SLA Profile	Select SLA Profile to bind. When the type of the LLB rule is specifies as IPv4, only the SLA Profile of IPv4 can be bound. When

Option	Description
	the type of the LLB Rule is specified as IPv6, only the SLA Profile of IPv6 can be bound. **Notes:** The SLA profile only takes effect when any of the options in the LLB profile's primary scheduling algorithm, secondary scheduling algorithm, or alternative scheduling algorithm is set to the "Dynamic Proximity" algorithm.
LLB Profile	Select LLB Profile to bind. When the type of the LLB Rule is specified as IPv4, only the LLB Profile of IPv4 can be bound. When the type of the LLB Rule is specified as IPv6, only the LLB Profile of IPv6 can be bound. This item is required.
Bind Host Book	Select the host book when destination route is specified.

4. Click **OK**.
5. On the **Rule** page, you can also perform the following operations:
    - Delete LLB rule: Select one or more LLB rules and click **Delete** to delete them.
    - Filter LLB rule: Click **Filter**. Select a filter condition from the drop-down list and enter a value. This way, rules that meet the filter condition are displayed in the list. Repeat the steps above to add more filter conditions. The logical operator among these filter conditions is AND.

For more information, refer to the **Network** > **Load Balancing** > **Link Load Balancing** > **Outbound Load Balancing** topic in *StoneOS WebUI User Guide*. FR 41325

Configuring an Interface

The configuration options for different types of interfaces may vary. For more information, see the following instructions.

Both IPv4 and IPv6 address can be configured for the interface.

Creating a PPPoE Interface

> **Notes:** Non-root VSYS does not support to create the PPPoE interface.

To create a PPPoE interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > PPPoE Interface**.

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the PPPoE interface.
Description	Enter descriptions for the PPPoE interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not click-

Option	Description
	ing this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	
User	Specifies a user name for PPPoE.
Password	Specifies PPPoE user's password.
Confirm Password	Enter the password again to confirm.
Idle interval	If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connections; if the interface requires Internet access, the system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 0.
Re-connect interval	Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 10, which means the function is disabled.
Set gateway information from PPPoE server as the default gateway route	With this selected check box, system will set the gateway information provided by PPPoE server as the default gateway route.

Option	Description
Advanced	In the Advanced page, configure advanced options for PPPoE, including: • Access Concentrator - Specifies a name for the concentrator. • Authentication - The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). • Netmask - Specifies a netmask for the IP address obtained via PPPoE. • Static IP - You can specify a static IP address and negotiate about using this address to avoid IP change. To specify a static IP address, type it into the box. • Distance - Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight - Specifies a route weight. The value range is 1 to 255. The default value is 1. • Service - Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.

Option	Description
DDNS	In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF**, and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable**， **Close** or **Global Default** radio button as needed. • Enable：Enable the WebAuth function of the specified interface. • Close：Disable the WebAuth function of the specified interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login

Option	Description
	page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

Expand Interface Properties, configure properties for the interface.

Option	Description
Parameters	
ARP Learning	Click the **Enable** button to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other

Option	Description
	interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	System clones a MAC address in the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with

Option	Description
	the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. Note: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Mirror	Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.

Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight.

Option	Description
ISP Profile	Select an existing IPv4 ISP from the drop-down list. After binding the interface to the specified ISP, it indicates that the link corresponding to the interface is bound to the ISP.

Option	Description
	Click ⊕ in the drop-down list. In the **ISP Configuration** panel, you can add the required ISP information. For more information, see Configuring ISP Information.
ISP IPv6 Profile	Select an existing IPv6 ISP from the drop-down list. After binding the interface to the specified ISP, it indicates that the link corresponding to the interface is bound to the ISP. Click ⊕ in the drop-down list. In the **ISP Configuration** panel, you can add the required ISP information. For more information, see Configuring ISP Information.
LLB Priority	Specifies the priority of the interface. When the system performs outbound load balancing and uses a priority-based scheduling policy, this value determines the priority of the link corresponding to the interface. The value range is 1 to 100, with a default value of 50. The smaller the number, the higher the priority of the outbound link.
LLB Weight	Specifies the weight of the interface. When the system performs outbound load balancing, different load balancing algorithms use this weight to calculate and select routes differently. The value range is 1 to 255, with a default value of 50. The larger the number, the greater the interface weight, and the more traffic the corresponding outbound link will forward.
Upstream Threshold	Specifies the upstream bandwidth threshold for the interface as needed. When the upstream bandwidth utilization of the interface

Option	Description
	reaches the specified threshold, the system will no longer distribute traffic to the interface. The value range is 0 to 100 (0% to 100%), with a default value of 0 (indicating no limit). **Notes:** When selecting an outbound link for outbound traffic, if a link in the session persistence table matches, the device will still use that link to forward traffic even if it is busy.
Downstream Threshold	Specifies the downstream bandwidth threshold for the interface as needed. When the upstream bandwidth utilization of the interface reaches the specified threshold, the system will no longer distribute traffic to the interface. The value range is 0 to 100 (0% to 100%), with a default value of 0 (indicating no limit). **Notes:** When selecting an outbound link for outbound traffic, if a link in the session persistence table matches, the device will still use that link to forward traffic even if it is busy.

Expand Advanced Configuration, configure advanced options for the interface.

Option	Description
NetFlow Configuration	Select a configured NetFlow profile from the drop-down list below.
Reverse Route	Enable or Disable reverse route as needed:

Option	Description
	• Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is to say, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Shutdown	System supports interface shutdown. You can not only force a specific interface to shut down, but also control the time it shuts down by schedule or according to the link status of tracked objects. Configure the options as below: 1. Select the **Shut down** check box to enable interface shutdown. 2. To control the shutdown by schedule or tracked objects, select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list or click ⊕ button to create a new schedule or a new track object.

Option	Description
Monitor and Backup	Configure the options as below: 1. Select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list or click ⊕ button to create a new schedule or a new track object. 2. Select an action: • Shut down the interface: During the time specified in the schedule, or when the tracked object fails, the interface will be shut down and its related route will fail; • Migrate traffic to backup interface: During the time specified in the schedule, or when the tracked object fails, traffic flowing to the interface will be migrated to the backup interface. In such a case you need to select a backup interface from the Backup interface drop-down list and type the time into the Migrating time box. (Migrating time, 0 to 60 minutes, is the period during which traffic is migrated to the backup interface before the primary interface is switched to the backup interface. During the migrating time, traffic is migrated from the primary interface to the backup interface smoothly. By default the migrating time is set to 0,

Option	Description
	i.e., all the traffic will be migrated to the backup interface immediately.)

Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface.

Option	Description
Authentication mode	Specifies a packet authentication mode for the system, including plain text (the default) and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that require high security.
Authentication string	Specifies a RIP authentication string for the interface.
Transmit version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Receive version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Split horizon	Select the **Enable** checkbox to enable split horizon. With this function enabled, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent.
Passive mode	The interface which receives data only but not send is known as a passive interface. Click the button to enable the interface as passive interface.

Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface.

Option	Description
Interface Timer	There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. • Dead Time: Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.
Priority	Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selec-

Option	Description
	ted as the designated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.
Network Type	Specifies the network type of an interface. The network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast.
Link Cost	Click the **Enable** button to enable the link cost function. The value range is 1 to 65535. By default, the HA synchronization function is enabled, and the link cost will be synchronized to the backup device. Clear the check box to disable the synchronization function, and the system will stop synchronizing.

Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface.

Option	Description
Area ID	Specifies the area ID to which the interface belongs. The area ID is represented by 32 bits, which can be a number or an IP address.
Instance ID	Specifies the instance ID to which the interface belongs. The value range is 0 to 255. The default value is 0.
Interface	There are four interface timers: the interval for sending Hello

Option	Description
Timer	packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. • Dead Time: Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1
Priority	Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a net-

Option	Description
	work can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.
Link Cost	Specifies the link cost. The value range is 1 to 65535.
Passive	Some interfaces can be configured to receive updates but not send them. Such interfaces are passive interfaces. Click **Enable** to enable the passive interface.
MTU-Ignore	OSPFv3 uses DBD packets to check whether the MTU of interfaces between neighbors match. If mtus of adjacent OSPFv3 router interfaces do not match each other, they cannot establish an adjacency relationship. You can modify the MTU of the interface to solve this problem. MTU cannot be modified on some interfaces. In this case, you can click the **Enable** button to make OSPFv3 ignore the MTU matching check.

Expand IPv6 Configuration, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address.

Option	Description
	• Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
Enable DNS Proxy	Select this check box to enable DNS proxy for the interface.
DHCP	System supports DHCPv6 client, DHCPv6 server and DHCPv6 relay proxy. • Select **DHCP** check box to enable DHCP client for the interface. After enabling, system will act as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Selecting **Rapid-commit** option can help fast get IPv6 addresses from the server. You need to enable both of the DHCP client and the server's Rapid-commit function. • Select **DHCPv6 Server** from DHCP drop-down list and configure options as Configuring DHCPv6 Server, system will act as a DHCPv6 server to appropriate IPv6 addresses for DHCP client. • Select **DHCPv6 Relay Proxy** from DHCP drop-down list and configure options as Configuring DHCPv6 Relay Proxy, system will act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server
IPv6 Advanced	

Option	Description
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses.. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specifies an IPv6 MTU for an interface. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an

Option	Description
	unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.
ND Learning	Click the button to enable ND learning for the interface. The interface obtains IP-MAC binding information in the internal network from ND learning and adds the binding information to the ND table. By default, ND learning is enabled. The interface continuously performs ND learning and adds the learned IP-MAC binding information to the ND table of the system. After the function is disabled, only IP addresses that are in the ND table can forward packets by using the interface.
ND Learning Limit	When a user host that connects to the interface initiates ND attacks, ND entry resources may be exhausted, making other interfaces unable to perform ND learning. To avoid this issue, the system allows you to enable ND learning limit and specify the maximum number of ND entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ND learning when the maximum number of ND entries is

Option	Description
	reached. Click the button to enable ND learning limit for the interface and enter the maximum number of ND entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

3. Click **OK**.

Creating a Tunnel Interface

Notes: Non-root VSYS does not support to create the tunnel interface.

To create a tunnel interface:

1. Select **Network > Interface**.

2. Select **New > Tunnel Interface**.

   In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the tunnel interface. The length varies from hardware platforms.
Description	Enter descriptions for the tunnel interface.
Binding Zone	If Layer 2 zone or Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone or Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
NetFlow configuration	Select a configured NetFlow profile from the drop-down list below.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.

Option	Description
	Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends

Option	Description
	option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. Notes: • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
Tunnel Binding	Bind the interface to a VPN tunnel or ZTNA instance. One tunnel interface can be bound to multiple IPSec VPN tunnels, while only to one SSL VPN tunnel.

Option	Description
	• IPSec VPN: Select IPSec VPN radio button. Specifies a name for the IPSec VPN tunnel that is bound to the interface. Then select a next-hop address for the tunnel, which can either be the IP address or the egress IP address of the peering tunnel interface. This parameter, which is 0.0.0.0 by default, will only be valid when multiple IPSec VPN tunnels is bound to the tunnel interface. • SSL VPN: Select SSL VPN radio button. Specifies a name for the SSL VPN tunnel that is bound to the interface.
TAP Configuration	• Control Interface: A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections. By default, the bypass control interface is the bypass interface itself. For tunnel interfaces, if the interface itself is used as the control interface, the control message sent by the tunnel interface may not be processed correctly. It is recommended that bypass tunnel interfaces be configured with other interfaces as control interfaces. When configuring, ensure that the control interface can send messages to the switch normally. • LAN Address: Specify a LAN address. Packets whose

Option	Description
	source IP is in the specified range will be counted.
Firewall Linkage Configuration	Specify the firewall information (firewall's IP, SSH port, login name, and password) in Firewall Linkage Configuration to combine the current device with a Hillstone firewall. If the device detects the attack traffic, it will send the IP of the attack source to the linkage firewall in the form of blacklist, and the linkage firewall will block the traffic of the attack source IP.
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.
Tunnel Binding: Bind VPN tunnel, IPv6 over IPv4 tunnel, or ZTNA instance to a tunnel interface. One tunnel interface can be bound to multiple IPSec VPN tunnels or GRE VPN tunnels, while only to one SSL VPN tunnel, one L2TP tunnel, one IPv6 over IPv4 tunnel, or one ZTNA instance.	
New	Click **New** to add an entry.
Type	Specifies the type of the tunnel or instance bound to a tunnel interface.
Name	Specifies the name of VPN tunnel, IPv6 over IPv4 tunnel, or ZTNA instance bound to a interface. Note: If you specify the instance type bound to the tunnel interface is ZTNA, only "remote access ZTNA instance" can be selected.
Domain	Bind the domain name to the L2TP tunnel. If you bind the

Option	Description
	domain name, usernames without the domain name cannot dial up successfully. If you do not bind the domain name, LNS will omit the domain name of usernames when authenticating users.
IPv4/IPv6 Gateway	The next hop IP addresses can be specified to either IPv4 or IPv6 addresses. Only when GRE VPN is bound can next hop IP addresses.

3. Expand Interface Properties, configure properties for the interface.

Option	Description
Parameters	
MTU	Specifies a MTU for the interface. The value range is 1280 to 1500/1800 bytes (The max MTU may vary on different platforms). The default value is 1500. Specifies the MTU value. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.

Option	Description
MAC clone	System clones a MAC address in the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. **Note**: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Mirror	Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.

Option	Description
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.

4. Expand IPv6 Configuration, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. • Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
Enable DNS Proxy	Select this check box to enable DNS proxy for the interface.
DHCP	System supports DHCPv6 client, DHCPv6 server and DHCPv6 relay proxy. • Select **DHCP** check box to enable DHCP client for the interface. After enabling, system will act as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Selecting **Rapid-commit** option can help fast get IPv6 addresses from the server. You need to enable both of the

Option	Description
	DHCP client and the server's Rapid-commit function. • Select **DHCPv6 Server** from DHCP drop-down list and configure options as Configuring DHCPv6 Server, system will act as a DHCPv6 server to appropriate IPv6 addresses for DHCP client. • Select **DHCPv6 Relay Proxy** from DHCP drop-down list and configure options as Configuring DHCPv6 Relay Proxy, system will act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server.
IPv6 Advanced	
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses.. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.

Option	Description
MTU	Specifies an IPv6 MTU for an interface. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is

Option	Description
	known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

5. "Expand Interface Properties, configure properties for the interface." on Page 692
6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
10. Click **OK**.

Creating a Virtual Forward Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To create a virtual forward interface, take the following steps:

1. Select **Network > Interface**.

2. Select **New > Virtual Forward Interface**.

   In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If Layer 2 zone or Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone or Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.

Option	Description
	Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends

Option	Description
	option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable** , **Close** or **Global Default** radio button as needed.

Option	Description
	• Enable：Enable the WebAuth function of the specified interface. • Close：Disable the WebAuth function of the specified interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you

Option	Description
	visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

3. "Expand IPv6 Configuration, configure the following." on Page 681
4. "Expand Interface Properties, configure properties for the interface." on Page 692
5. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
10. Click **OK**.

Creating a Loopback Interface

To create a loopback interface, take the following steps:

1. Select **Network > Interface**.

2. Click **New > Loopback Interface**.

   In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the loopback interface.
Description	Enter descriptions for the loopback interface.
Binding Zone	If Layer 2 zone or Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone or Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP:In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.

Option	Description
	Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends

Option	Description
	option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.

3. "Expand IPv6 Configuration, configure the following." on Page 681

4. "Expand Interface Properties, configure properties for the interface." on Page 692

5. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
10. Click **OK**.

Creating an Aggregate Interface

To create an aggregate interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Aggregate Interface**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the aggregate interface.
Description	Enter descriptions for the aggregate interface.

Option	Description
Binding Zone	Specifies the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. And you can also specify the firewall information (firewall's Pv4 or IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP mode and this interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block;

Option	Description
	• The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.

Aggregate mode	• Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally.
	• Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are:
	  • System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be.
	  • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum

Option	Description
	number, the status of other legal interfaces will change to Standby. • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
HA sync	Click this button to enable HA sync function. The primary device will synchronize its information with the backup device.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box being selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced:

Option	Description
	• Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.

DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.

Password: Specifies PPPoE user's password.

Confirm Password: Enter the password again to confirm.

Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td colspan="2">value range is 0 to 10000 minutes. The default value is 30.</td></tr>
<tr><td colspan="2">Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</td></tr>
<tr><td colspan="2">Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</td></tr>
<tr><td>Advanced</td><td>Access concentrator: Specifies a name for the concentrator.</td></tr>
<tr><td></td><td>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</td></tr>
<tr><td></td><td>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</td></tr>
<tr><td></td><td>Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.</td></tr>
<tr><td></td><td>Service: Specifies allowed service. The specified ser-</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>vice must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td>TAP Configuration</td><td>• Control Interface: A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections. By default, the bypass control interface is the bypass interface itself. For tunnel interfaces, if</td></tr>
</table>

Option	Description
	the interface itself is used as the control interface, the control message sent by the tunnel interface may not be processed correctly. It is recommended that bypass tunnel interfaces be configured with other interfaces as control interfaces. When configuring, ensure that the control interface can send messages to the switch normally. • LAN Address: Specify a LAN address. Packets whose source IP is in the specified range will be counted.
Firewall Linkage Configuration	Specify the firewall information (firewall's IP, SSH port, login name, and password) in Firewall Linkage Configuration to combine the current device with a Hillstone firewall. If the device detects the attack traffic, it will send the IP of the attack source to the linkage firewall in the form of blacklist, and the linkage firewall will block the traffic of the attack source IP.
WebAuth	
Auth Service	Click the **Enable**， **Close** or **Global Default** radio button as needed. • Enable：Enable the WebAuth function of the specified interface. • Close：Disable the WebAuth function of the specified interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default

Option	Description
	configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 681

5. "Expand Interface Properties, configure properties for the interface." on Page 692
6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

7. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
8. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
9. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
10. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
11. Expand Load Balance, configure a load balance mode for the interface. "Flow-based" means enabling automatic load balance based on the flow. This is the default mode. "Tuple" means enabling load based on the source/destination IP, source/destination MAC, source/destination interface or protocol type of packet, or the combination of the selected items.
12. Click **OK**.

Creating a Redundant Interface

To create a redundant interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Redundant Interface**.
3. "In this page, configure the following." on Page 708

4. "Expand IPv6 Configuration, configure the following." on Page 681
5. "Expand Interface Properties, configure properties for the interface." on Page 692
6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

7. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
8. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
9. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
10. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
11. Click **OK**.

Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface

To create an ethernet sub-interface/an aggregate sub-interface/a redundant sub-interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Ethernet Sub-interface/Aggregate Sub-interface/Redundant Sub-interface**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If Layer 2 zone or Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone or a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced:

Option	Description
	• Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that the system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.

DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.

Password: Specifies PPPoE user's password.

Confirm Password: Enter the password again to confirm.

Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td colspan="2">value range is 0 to 10000 minutes. The default value is 30.</td></tr>
<tr><td colspan="2">Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</td></tr>
<tr><td colspan="2">Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</td></tr>
<tr><td>Advanced</td><td>Access concentrator: Specifies a name for the concentrator.</td></tr>
<tr><td></td><td>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</td></tr>
<tr><td></td><td>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</td></tr>
<tr><td></td><td>Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.</td></tr>
<tr><td></td><td>Service: Specifies allowed service. The specified ser-</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>vice must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td colspan="2">WebAuth</td></tr>
<tr><td>Auth Service</td><td>Click the Enable， Close or Global Default radio button as needed.
Enable： Enable the WebAuth function of the specified interface.
Close： Disable the WebAuth function of the specified interface.</td></tr>
</table>

Option	Description
	• Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the

Option	Description
	WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 681
5. "Expand Interface Properties, configure properties for the interface." on Page 692
6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

> **Notes:** Non-root VSYS does not support this configuration.

7. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
8. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
9. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
10. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
11. Click **OK**.

Creating a VSwitch Interface

To create a VSwitch interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > VSwitch Interface**.
3. "In this page, configure the following." on Page 698

4. "Expand IPv6 Configuration, configure the following." on Page 681
5. "Expand Interface Properties, configure properties for the interface." on Page 692
6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

7. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
8. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677
9. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678
10. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679
11. Click **OK**.

Creating a Vif Interface

The Vif interface is a logical interface, which is used for the Multicast Service Reflection (MSR) function. On the Vif interface, you can configure the IGMP Join-group function to direct multicast traffic to the MSR device, and then convert the original multicast streams (S1, G1) into new multicast streams (S2, G2) based on the address mapping configured on the MSR device.

To create a Vif interface, take the following steps:

1. Select **Network > Interface**.

2. Click **New** > **Vif Interface**.

   In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the Vif interface, which can only be vif1. You can configure only one vif interface.
Description	Enter descriptions for the Vif interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuraton	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface, which cannot be 32 or 255.255.255.255, otherwise, the MSR function does not take effect.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to

Option	Description
	255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the cli-

Option	Description
	ent uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including SSH, Ping, HTTPS , SNMP, NETCONF, TRACEROUTE, HTTP, and Telnet.

3. "Expand Interface Properties, configure properties for the interface." on Page 692
4. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

Notes: Non-root VSYS does not support this configuration.

5. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674
6. "Expand IPv6 Configuration, configure the following." on Page 681
7. Select Network > Routing > PIM, click Interface Configuration to open the Interface page and configure the MSR function for the selected interface.
8. Click **OK**.

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network > Interface**.
2. Select the interface you want to edit from the interface list and click **Edit**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the interface.
Description	Enter descriptions for the interface.
Binding Zone	Specifies the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. You can also specify the firewall information (firewall's IPv4 or

Option	Description
	IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP mode and this interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block; • The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, you should also select an aggregate interface/redundant interface: • Aggregate Interface: The interface you specified belongs to a aggregate interface. • Interface: Choose an aggregate interface which the aggregate interface belongs to from Interface drop-

Option	Description
	down list. • Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority. • Port timeout mode: The LACP timeout refers to the time interval for the members The system supports **Fast** (1 second) and **Slow** (30 seconds, the default value) waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. • Redundant Interface: This interface belongs to a redundant interface. Select that redundant interface from the Interface drop-down list. • None: This interface does not belong to any object.
Aggregate mode	• Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the

Option	Description

	traffic passing through the aggregate interface equally.
	• Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are:
	  • System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be.
	  • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby.
	  • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will

Option	Description
	not forward any traffic.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gate-

Option	Description
	way route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>static routing information to the routing table.
• MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.
Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.
Password: Specifies PPPoE user's password.
Confirm Password: Enter the password again to confirm.</td></tr>
</table>

<table>
<tr><th>Option</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.</td></tr>
<tr><td></td><td colspan="2">Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</td></tr>
<tr><td></td><td colspan="2">Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</td></tr>
<tr><td></td><td>Advanced</td><td>Access concentrator: Specifies a name for the concentrator.</td></tr>
<tr><td></td><td></td><td>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</td></tr>
<tr><td></td><td></td><td>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</td></tr>
</table>

Option	Description
	Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box. Service: Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically. Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable**, **Close** or **Global Default** radio button as needed. • Enable: Enable the WebAuth function of the specified

Option	Description
	interface. • Close：Disable the WebAuth function of the specified interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be

Option	Description
	prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 681

5. Expand Interface Properties, configure properties for the interface.

Property	Description
Duplex	Specifies a duplex working mode for the interface. Options include auto, full duplex and half duplex. Auto is the default working mode, in which system will select the most appropriate duplex working mode automatically. 1000M half duplex is not supported.
Rate	Specifies a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported. For 1GE(SFP) optical port of certain A-series devices, you can set the data rate to 100 Mbps or 1,000 Mbps. The default data rate is 1000 Mbps. When you set the data rate to 100 Mbps, the optical port can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers. **Note**: Only the following devices allow you to backward switch the data rate of 1GE(SFP) optical port: SG-6000-A5500, A5200,

Property	Description
	A5100, A3800, A3700, A3600, A3000, A2800, and A2700.
Channel-Speed	Converts the data rate of 10GE (SFP+) optical interfaces. • 1G: Convert the data rate of 10GE (SFP+) optical interfaces from 10Gbps to 1Gbps. • Close: Do not convert the data rate of the 10GE (SFP+) optical interface, which is 10Gbps by default.
Optical Interface to Electrical Interface	This option applies to the X8180 devices' 10GE (SFP+) optical port, and by default, Optical Interface to Electrical Interface function is disabled. To enable this function, take the following steps: 1. Insert a copper SFP module. 2. Channel-Speed option is configured to "1G". 3. Click the **Enable** button, convert optical port to electrical port.
Combo type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, and the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: • Auto: The above default scenario.

Property	Description
	• Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this option configured, the device will migrate the traffic on the copper port to the fiber port automatically without reboot.
MTU	The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the inter-

Property	Description
	face. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	System clones a MAC address to the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will retore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. **Note**: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local

Property	Description
	interface.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.

6. "Click Link to expand the link configuration items and configure the link load balancing information about the interface, including the priority and weight." on Page 672

   Notes: Non-root VSYS does not support this configuration.

7. "Expand Advanced Configuration, configure advanced options for the interface." on Page 674

8. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 677

9. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 678

10. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 679

11. Click **OK**.

Notes:

- Before deleting an aggregate/redundant interface, you must cancel other interfaces' bindings to it, aggregate/redundant sub-interface's configuration, its IP address configuration and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.
- When a VSwitch interface is deleted, the corresponding VSwitch will be deleted as well.
- The HA interface can not bind the track object.

For more information, refer to the **Network** > **Interface** > **Configuring an Interface** topic in *StoneOS WebUI User Guide*. FR 41325

CLI

Outbound Load Balancing

.....

Limits



Device Supported: : Only SG-6000 A series, K series (except K9180/K6580), and CloudEdge platforms support to configure functions related to load balancing algorithms, such as bandwidth statistics period, priority scheduling policy for link load balancing, comprehensive consideration of other scheduling results, load balancing algorithm, session persistence method, etc.

When configuring outbound load balancing, please carefully read the following restrictions.

Notes:

- When configuring the LLB profile, functions related to load balancing algorithms, such as bandwidth statistics period, priority scheduling policy for link load balancing, comprehensive consideration of other scheduling results, load balancing algorithm, session persistence method, etc., are not supported in non-root VSYS.
- When configuring the LLB profile, the configuration of various parameters for link status detection, load balancing mode configuration, and data traffic direction configuration varies across different platforms; please refer to the actual platform.
    - For A series, K series (except K9180/K6580), and CloudEdge: when configuring the above functions, you need to use commands in the form of **dynamic-extra-conf** xxxx, for example, to enable link detection, use the **dynamic-extra-conf detect enable** command. For more information, see the corresponding function descriptions in the "Configure LLB Profile" section.
    - For X series, K9180, and K6580: when configuring the above functions, you cannot use commands in the form of **dynamic-extra-conf** xxxx, for example, to enable link detection, use the **detect enable** command. For more information, see the corresponding function descriptions in the "Configure LLB Profile" section.
- If an LLB rule is bound to both an LLB profile and an SLA profile, the SLA profile will only take effect if any of the preferred scheduling algorithm, secondary scheduling algorithm, or backup scheduling algorithm options in the LLB profile use the "Dynamic Proximity" algorithm.

Configuring SLA Profile

To create or configure an SLA profile, use the following command in the global configuration mode:

sla-profile*profile-name*

- *profile-name* – Specifies the name of the SLA profile. After you execute this command, the system creates an SLA profile with the specified name and enters the SLA profile configuration mode. If the specified name already exists, the system will directly enter the SLA profile configuration mode.

To delete the specified SLA profile, in the global configuration mode, use the command: **no sla-profile***profile-name*.

Enabling or Disabling SLA Function

In SLA profile configuration mode, the SLA function is enabled by default. To enable or disable it, use the following command:

sla-status {**disable** | **enable**}

- **disable** – Disable the SLA function.
- **enable** – Enable the SLA function.

Configuring Detection Mode

SLA detection modes include passive detection mode and active detection mode:

- Passive detection mode: The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.
- Active detection mode: In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.

To set the detection mode to passive detection mode, in SLA Profile configuration mode, use the following command:

detect-mode passive type {**ipv4** | **ipv6**}

- **ipv4** | **ipv6** - Specifies the IP type of passive detection, which can be IPv4 or IPv6. The default type is IPv4.

To set the detection mode to active detection mode, in SLA Profile configuration mode, use the following command:

detect-mode active type {**ipv4** {**domain-name***domain-name* | **ipv4-addr***A.B.C.D*} **protocol** {**icmp** | **tcp port***port-number*} | **ipv6** {**domain-name***domain-name* | **ipv6-addr***X:X:X:X::X*} **protocol** {**icmp6** | **tcp port***port-number*} [**interval***num* [**number***num*]]

- **ipv4** {**domain-name***domain-name* | **ipv4-addr***A.B.C.D*} **protocol** {**icmp** | **tcp port***port-number*} - Sets the type of active detection mode to IPv4 and configure the following parameters:
  - **domain-name***domain-name* | **ipv4-addr***A.B.C.D* - Specifies the destination address for detection packets in active detection mode, which can be an IPv4 address or a domain name.
  - **protocol** {**icmp** | **tcp port***port-number*} - Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP or TCP, with ICMP being the default. When you select TCP, you need to enter a TCP port number.
- **ipv6** {**domain-name***domain-name* | **ipv6-addr***X:X:X:X::X*} **protocol** {**icmp6** | **tcp port***port-number* - Sets the type of active detection mode to IPv6 and configure the following parameters:
  - **domain-name***domain-name* | **ipv6-addr***X:X:X:X::X* - Specifies the destination address for detection packets in active detection mode, which can be an IPv6 address or a domain name.
  - **protocol** {**icmp6** | **tcp port***port-number*} - Specifies the protocol type for sending detection packets in active detection mode, which can be ICMPv6 or TCP, with ICMPv6 being the default. When you select TCP, you need to enter a TCP port number.

- **interval***num* - Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
- **number***num* - Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.

Configuring SLA Threshold

To configure SLA threshold, in SLA Profile configuration mode, use the following command:

threshold {**delay-thres***num*| **jitter-thres***num* | **lossrate-thres***num*}

- **delay-thres***num* - Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
- **jitter-thres***num* - Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
- **lossrate-thres***num* - Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.

To restore the SLA threshold to default values, in SLA Profile configuration mode, use the command: **no threshold** {**delay-thres**| **jitter-thres** | **lossrate-thres**}.

Configuring Success Times Required For Activation

The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. To configure the success times required for activation, in SLA Profile configuration mode, use the following command:

activation*num*

- *num* - Specifies the number of success times required for activation. Valid values: 1 to 100. Default value: 5.

To restore the number of success times required for activation to the default value, in SLA Profile configuration mode, use the command: **no activation**.

Configuring Failed Times Required For Deactivation

The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. To configure the failed times required for deactivation, in SLA Profile configuration mode, use the following command:

inactivation*num*

- *num* - Specifies the number of failed times required for deactivation. Valid values: 1 to 100. Default value: 5.

To restore the number of failed times required for deactivation to the default value, in SLA Profile configuration mode, use the command: **no inactivation**.

Configuring LLB Profile

The LLB profile contains the parameters of the load balancing algorithm, such as bandwidth utilization threshold, probe switch, probe mode, and equalization direction.

To create or configure an LLB profile, use the following command in the global configuration mode:

llb profile *llb-profile-name*[**ipv6**]

- *llb-profile-name* – Specifies the name of the LLB profile. After you execute this command, the system creates an LLB profile with the specified name and enters the LLB profile configuration mode. If the specified name already exists, the system will directly enter the LLB profile configuration mode.

- **ipv6** – Specifies the type of the LLB Profile as IPv6. If not specified, the type of the LLB Profile is IPv4.

To delete the specified LLB profile, in the global configuration mode, use the command: **no llb profile** *llb-profile-name*.

> **Notes:** The LLB Profile name in the IPv4 should be different from that in IPv6.

Configuring a Load Balancing Algorithm

After configuring the load balancing algorithm, when new outbound traffic arrives, the system will select the egress link based on the specified algorithm.

The system supports multiple load balancing algorithms for outbound traffic. For more information, see Link Load Balancing Algorithm.

In LLB Profile configuration mode, use the following command to configure the load balancing algorithm:

balance {**prefer** {**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** |**hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port**| **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection**| **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin** |**isp** [**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** |**hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port**| **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection**| **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**] } | **alternative** {**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** |**hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port**| **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection**| **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**}}

- **prefer** - Specifies the preferred load balancing algorithm.
    - **dynamic-proximity** - Specifies the preferred balancing algorithm as dynamic proximity. This parameter is the default algorithm. After specifying this algorithm, the system

intelligently selects routes for outbound traffic based on the configuration of link detection parameters. For more information about link detection configuration, see Configuring Link Detection.

- **hash-dst-ip** - Specifies the preferred balancing algorithm as destination IP hash algorithm.
- **weighted-hash-dst-ip** - Specifies the preferred balancing algorithm as weighted destination IP hash algorithm.
- **hash-src-ip** - Specifies the preferred balancing algorithm as source IP hash algorithm.
- **weighted-hash-src-ip** - Specifies the preferred balancing algorithm as weighted source IP hash algorithm.
- **hash-src-ip-port** - Specifies the preferred balancing algorithm as source IP port hash algorithm.
- **weighted-hash-src-ip-port** - Specifies the preferred balancing algorithm as weighted source IP port hash algorithm.
- **least-bandwidth** - Specifies the preferred balancing algorithm as minimum bandwidth algorithm.
- **least-connection** - Specifies the preferred balancing algorithm as minimum connection algorithm.
- **weighted-least-connection** - Specifies the preferred balancing algorithm as weighted minimum connection algorithm.
- **round-robin** - Specifies the preferred balancing algorithm as round-robin algorithm. This parameter is the default algorithm.

- **weighted-least-bandwidth** - Specifies the preferred balancing algorithm as weighted minimum bandwidth algorithm.
- **weighted-round-robin** - Specifies the preferred balancing algorithm as weighted round-robin algorithm.

  Note: When the load balancing algorithm is set to **weighted-hash-src-ip**, **weighted-hash-dst-ip**, **weighted-hash-src-ip-port**, **weighted-least-connection**, **weighted-least-bandwidth**, or **weighted-round-robin**, the system will select routes in proportion to the interface weights. For more information, see Configuring Link Load Balancing Weights of Interface.
- **isp** [**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** |**hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port**| **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection**| **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**] - Specifies the preferred balancing algorithm as ISP algorithm and requires specifying a secondary balancing algorithm. If there are multiple links that match the ISP of the traffic's destination IP, the system needs to re-select routes among these links based on the secondary algorithm. The default secondary balancing algorithm is **round-robin**.

  Note: When the load balancing algorithm is set to **isp**, the system uses the ISP information configured for the interface as the ISP information corresponding to the link, thus performing route selection. For more information on interface ISPs, see Configuring ISP of Interface.

- **alternative** {**dynamic-proximity** | **hash-dst-ip** | **weighted-hash-dst-ip** |**hash-src-ip** | **weighted-hash-src-ip** | **hash-src-ip-port**| **weighted-hash-src-ip-port** | **least-bandwidth** | **least-connection** | **weighted-least-connection**| **round-robin** | **weighted-least-bandwidth** | **weighted-round-robin**} - Specifies the alternate balancing algorithm when the preferred balancing algorithm is **isp** or **host-any-dynamic-proximity**. If the system fails to match appropriate links

for the traffic using the preferred balancing algorithm, it will re-select routes for the traffic based on the alternate balancing algorithm.

In LLB Profile configuration mode, use the **nobalance** {**prefer** | **alternative**} command to restore the default load balancing algorithm.

Notes:

- When the load balancing algorithm for outbound traffic is configured as "minimum bandwidth" or "weighted minimum bandwidth," you can specify the statistical period for traffic bandwidth as needed.
- If all selected links are busy based on the load balancing algorithm, the system will forward the traffic using the default route.

Configuring Statistical Period for Bandwidth

When the load balancing algorithm for outbound traffic is configured as "minimum bandwidth" or "weighted minimum bandwidth," you can specify the statistical period for traffic bandwidth as needed. To configure the bandwidth statistics period for outbound traffic load balancing, use the following command in global configuration mode:

llbbandwidth-statistics-period*value*

- *value* - Specifies the statistical period for bandwidth. The value range is 1 to 300 seconds, with a default value of 120 seconds.

In global configuration mode, use the **nollbbandwidth-statistics-period** command to restore the default value.

Enabling Comprehensive Scheduling Function

When the balancing algorithm is set to "round-robin" or "weighted round-robin," the system supports to enable the comprehensive scheduling function for link load balancing. After enabling this function, the system will perform intelligent route selection by considering the results of session persistence algorithms on links. When new outbound traffic arrives, the system will prioritize selecting

links with less traffic for forwarding based on the current traffic load on each link.

In LLB Profile configuration mode, use the following command to enable the comprehensive scheduling function:

balancecomprehensive

- **comprehensive** - Enable the comprehensive scheduling function of link load balancing. By default, this function is disabled.

In LLB Profile configuration mode, use the **nobalancecomprehensive** command to disable the comprehensive scheduling function.

Configuring Priority Scheduling Policy for Link Load Balancing

To enable the priority scheduling policy for links, you need to specify the minimum number of active links, which is the minimum number of links participating in link load balancing scheduling. The value range is 1 to 32.

In LLB Profile configuration mode, use the following command to enable the priority scheduling policy for link load balancing:

min-active-link*value*

- *value* - Specifies the minimum number of active links. The value range is 0 to 32, with a default value of 0, indicating that the priority scheduling function for link load balancing is disabled.

In LLB Profile configuration mode, use the **nomin-active-link** command to restore the default value of the minimum number of active links.

The priority of device egress links is determined by the link load balancing priority of their corresponding interfaces. For example, if there are 10 egress links on the device and the minimum number of active links is 6, then based on the priority ranking of the egress links' corresponding interfaces, all available links with the highest priority will be prioritized for scheduling; if the number of links with the highest priority is less than 6, all available links with the next highest priority will be added to the scheduling. This process continues until the number of available links participating in the scheduling is greater than or equal to 6, or all available links have been scheduled. If one of the scheduled links becomes unavailable, causing the actual number of scheduled links to be

less than 6, the device will continue to select all available links with the highest priority from the unscheduled links until the condition is met; when a high-priority link becomes available again, it will be rescheduled.

For example, the link load balancing priorities of interfaces eth0/1, eth0/2, eth0/3, and eth0/4 are 10, 20, 30, and 20, respectively; the ISPs of interfaces eth0/1, eth0/2, eth0/3, and eth0/4 are China-telecom, China-telecom, China-telecom, and China-mobile, respectively. The preferred balancing algorithm for the LLB profile is "ISP," the alternative balancing algorithm is "round-robin," the priority scheduling policy is enabled, and the minimum number of active links is 2. Other options remain at their default settings, and the LLB profile is associated with an LLB rule. When a client using the telecom operator sends a request to the device, because the LLB balancing algorithm is ISP, the egress links corresponding to interfaces eth0/1, eth0/2, and eth0/3 will participate in the scheduling; since interfaces eth0/1 and eth0/2 have higher priority, the device will ultimately round-robin assign the telecom client's request to interfaces eth0/1 and eth0/2.

Configuring the Link Detection Function

You can configure various parameters for link status detection as needed. The system will intelligently select routes for outbound traffic based on the configuration of link detection. For the SG-6000 A series, K series (excluding K9180/K6580 models), and CloudEdge platforms, this configuration only takes effect when the load balancing algorithm for traffic is "dynamic proximity (**dynamic-proximity**)."

- Enabling and Disabling Link Detection
- Configuring Link Detection Mask/Prefix
- Configuring Bandwidth Utilization Threshold
- Configuring Weights for Calculating Link Status
- Configuring Link Weight Refresh Time
- Configuring Maximum Number of Subnet Entries

Enabling and Disabling Link Detection

In LLB profile configuration mode, the detect function is enabled by default. To enable or disable it, use the following command:

dynamic-extra-conf detect {disable | enable}

- **disable** − Disables the detect function, the system adjusts the routing link according to the bandwidth occupancy of each egress link, and the link with low bandwidth occupation rate is preferred.
- **enable** − Enable the detection function. Once the detection function is enabled, the device will use a combination of active and passive detection methods to detect the network link status based on various configured parameters for link status detection, and then select the optimal route. The priority for selection is as follows:

    1. When the LLB rule binds to a domain name book and the client's access request matches the bound domain name book, the system will initiate active detection for the corresponding outbound link quality, and the results of the active detection will be used as the basis for routing.
    2. When the LLB rule does not bind to a domain name book, or binds to a domain name book but the client's access request does not match the bound domain name book, if the link bandwidth utilization is below the configured bandwidth threshold, the system will only calculate the link quality based on latency, packet loss, and jitter, prioritizing higher-quality links; if the link bandwidth utilization exceeds the configured bandwidth threshold, the system will comprehensively calculate the link quality based on latency, packet loss, jitter, and bandwidth utilization, prioritizing higher-quality links.

For the SG-6000 K9180/K6580 and X series platforms, use the **detect {disable | enable}** command to configure.

Notes: For more information about parameters that you need to configure, see Configuring Weights for Calculating Link Status.

Configuring Link Detection Mask/Prefix

In LLB Profile configuration mode, use the following command to configure the mask during link detection:

dynamic-extra-conf detect {**netmask** {*A.B.C.D* | *num*} | **prefix***prefix-len*}

- **netmask** {*A.B.C.D* | *num*} - Specifies the detection subnet. The system will monitor the traffic in real time based on the subnet. The traffic of the same subnet will choose the same link. The system supports two formats, A.B.C.D or num. The value of A.B.C.D ranges from 255.255.240.0 to 255.255.255.255, and the default value is 255.255.240.0; num ranges from 20 to 32 and defaults to 28.
- **prefix***prefix-len* - **prefix***prefix-len* – Specifies prefix length. The system will monitor the traffic in real time based on the prefix length. The traffic with the same prefix length will choose the same link. The value range of prefix len is 64 to 96, and the default value is 64.

Configuring Bandwidth Utilization Threshold

To specify the interface bandwidth utilization threshold, in LLB Profile configuration mode, use the following command:

dynamic-extra-conf detect threshold *value*

- *value* – Specifies the interface bandwidth utilization threshold. When the interface's bandwidth utilization does not exceed the threshold, the system will only analyze the link's latency, jitter, and packet loss to dynamically adjust the routing method; when the interface's bandwidth utilization exceeds the threshold, the system will also analyze the "bandwidth utilization" parameter on each link to adjust the routing method. The value range of value is 1 to 100 (1%-100%), with a default of 60%.

In LLB Profile configuration mode, use the **no dynamic-extra-conf detect threshold** command to restore the parameter to its default value.

For SG-6000 K9180/K6580 and X series platforms, use the **detect threshold** *value* command to configure.

Configuring Weights for Calculating Link Status



Device Supported: : SG-6000 A series, K series (all models except K9180/K6580), and CloudEdge platforms support configuration only through CLI commands.

Specify the factors affecting the link Cost value. These factors are parameters used to calculate the link Cost value, including the link's delay, jitter, packet loss rate, and bandwidth weight, i.e., the impact ratio of the link's delay, jitter, packet loss rate, and bandwidth on the link Cost value. You can choose predefined factors or configure custom factors.

dynamic-extra-conf detect weight-factors {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factor jitter-factor loss-rate-factor BW-rate-threshold-factor* [*BW-rate-factor*]}

- **delay-template** - In this item, the delay, jitter, packet loss rate, and bandwidth weight are 10, 2, 4, 1, respectively, indicating that the link delay has the greatest impact on the link Cost value.
- **jitter-template** - In this item, the delay, jitter, packet loss rate, and bandwidth weight are 1, 10, 4, 1, respectively, indicating that the link jitter has the greatest impact on the link Cost value.
- **loss-template** - In this item, the delay, jitter, packet loss rate, and bandwidth weight are 1, 2, 10, 1, respectively, indicating that the link packet loss rate has the greatest impact on the link Cost value.
- *delay-factor* - Specifies the ratio of link delay. The value range is 0 to 15, with a default of 1.
- *jitter-factor* - Specifies the ratio of link jitter. The value range is 0 to 15, with a default of 2.

- *loss-rate-factor* - Specifies the ratio of link packet loss rate. The value range is 0 to 15, with a default of 4.
- *BW-rate-threshold-factor* - Specifies the ratio of bandwidth utilization when the link bandwidth utilization exceeds the threshold. The value range is 0 to 15, with a default of 1.
- *BW-rate-factor* - Specifies the ratio of current link bandwidth utilization. The value range is 0 to 15, with a default of 1.

In LLB Profile configuration mode, use the **no dynamic-extra-conf detect weight-factors** command to restore the parameter to its default value.

For SG-6000 K9180/K6580 and X series platforms, use the **detect weight-factors** {**predefine** {**delay-template** | **jitter-template** | **loss-template**} | *delay-factor jitter-factor loss-rate-factor BW-rate-threshold-factor* [*BW-rate-factor*]} command to configure.

Configuring Link Weight Update Interval

To specify the interval time for updating the weights of various link factors, in LLB Profile configuration mode, using the following command:

dynamic-extra-conf detect weight-update-interval *value*

- *value* - Specifies the interval for updating the system link status weights. The value range is 1 to 300 seconds, with a default of 1 second.

In LLB Profile configuration mode, use the **no dynamic-extra-conf detect weight-update-interval** command to restore the parameter to its default value.

For SG-6000 K9180/K6580 and X series platforms, use the **detect weight-update-interval** *value* command to configure.

Configuring Maximum Number of Subnet Entries

To configure the maximum number of LLB Profile subnet entries, in LLB Profile configuration mode, use the following command:

dynamic-extra-conf detect max-entry-number *value*

- *value* – Specifies the maximum number of LLB profile subnet entries that the system can configure. The default value varies depending on the platform, please refer to the actual configuration.

In LLB Profile configuration mode, use the **no dynamic-extra-conf detect max-entry-number** command to restore the parameter to its default value.

For SG-6000 K9180/K6580 and X series platforms, use the **detect max-entry-number** *value* command to configure.

Configuring Session Persistence Method

Specify the session persistence method for load balancing. By configuring the session persistence method, the system will forward traffic that meets the session persistence conditions to the same link. In LLB Profile configuration mode, use the following command to configure the session persistence method:

persistencemethod {**dst-ip** | **src-dst-ip** | **src-ip**}

- **src-ip** - For traffic from the same client, select the same link for forwarding.
- **src-dst-ip** - For traffic from the same client and with the same destination address, select the same link for forwarding.
- **dst-ip** - For traffic with the same destination address, select the same link for forwarding.

In LLB Profile configuration mode, use the **nopersistence method** command to delte the session persistence method.

Notes: When selecting an egress link for outbound traffic, session persistence is matched first. If a link in the session persistence table is matched, even if the link is busy, the device will still use that link to forward traffic.

Configuring Session Persistence Timeout

Specify the timeout for session persistence. After exceeding the specified time value, the device will clear the corresponding session persistence table information. In LLB Profile configuration mode, use the following command to configure the session persistence timeout:

persistence timeout*value*

- *value* - Specifies the timeout for session persistence. The value range is 60 to 65535 seconds, with a default of 300 seconds.

In LLB Profile configuration mode, use the **nopersistence timeout** command to restore the default session timeout value.

Configuring Busy Protection for Link



Device Supported: : Only the SG-6000 A series, K series (excluding K9180/K6580), and CloudEdge platforms support this function.

You can configure busy protection for the egress links, i.e., configure the actual bandwidth value and bandwidth threshold of the interface. When the outbound traffic of a link reaches the bandwidth threshold specified for the interface, if the system selects an egress link through a load balancing algorithm, it will prioritize other non-busy links; when the system selects an egress link through a session persistence algorithm, if a matching session persistence table entry is found, the link busy protection function will be ignored, and the matched link will be selected to forward the traffic.

In interface configuration mode, use the following command:

bandwidth {**downstream** | **upstream**} {**threshold***value*| *bandwidth*}

- **downstream** - Configures the maximum bandwidth value and bandwidth threshold in the downstream direction of the interface.

- **upstream** - Configures the maximum bandwidth value and bandwidth threshold in the upstream direction of the interface.
- **threshold***value* - Specifies the bandwidth threshold of the interface. The value range is 0 to 100 (0% to 100%), with a default value of 0, indicating no limit.
- *bandwidth* - Specifies the maximum bandwidth value of the interface. The range is 512,000 to 1000,000,000,000 bps. The default value is 1000,000,000 bps.

In interface configuration mode, use the **nobandwidth** {**downstream** | **upstream**} [**threshold**] command to restore the default values of the interface's maximum bandwidth and bandwidth threshold.

Notes: Non-root VSYS does not support this configuration.

Specifying to Record Log Information

When the bandwidth utilization of the link exceeds the specified limit, the system will record the logs. To record the logs, use the following command:

log enable [**utilization-limit***utilization-limit*]

- **utilization-limit***utilization-limit* - Specifies the limit value of link bandwidth utilization, the range is 1 to 100. The default value is 90.

Use the command **no log enable** to cancel recording logs.

Configuring the Load Balancing Direction

When the system calculates the bandwidth utilization of load balancing, the direction of data traffic needs to be configured. For the SG-6000 A series, K series (all models except K9180/K6580), and CloudEdge platform, this configuration only takes effect when the load balancing algorithm is "least-bandwidth" or "weighted-least-bandwidth".

To configure the load balancing direction, use the following command in LLB Profile configuration mode:

dynamic-extra-conf bandwidth-balance-direction {**bidirection** | **downstream** | **upstream**}

- **bidirection** – The system will compare the maximum bandwidth utilization ratio with the bandwidth utilization threshold in the two directions of data flow into and out, and then adjust the routing method.
- **downstream** – The system will compare the bandwidth utilization of the data stream into the bandwidth utilization threshold, and then adjust the routing method.
- **upstream** - The system will compare the bandwidth utilization of the data stream out the bandwidth utilization threshold, and then adjust the routing method.

To restore the default mode of the load balancing direction, use the command **no dynamic-extra-conf bandwidth-balance-direction**.

For SG-6000 K9180/K6580 and X series platforms, use the **bandwidth-balance-direction** {**bidirection** | **downstream** | **upstream**} command to configure.

Configuring the Load Balancing Mode

To configure the load balancing mode, use the following command:

dynamic-extra-conf mode {**compatibility** [**upper-limit** *value* **lower-limit** *value*] | **performance**}

- **compatibility** – Configure the load balancing mode to work in high compatibility mode. When the link load changes, the system does not switch the link frequently, but ensures that the service is as far as possible on the previous link, such as banking services.
    - **upper-limit***upper-limit-value***lower-limit***lower-limit-value*- In the high compatibility mode, the system records the source, destination, output interface and other information into the cache. If the bandwidth of the link exceeds *upper-limit-value*and the other links are lower than *lower-limit-value*, the system will delete all caches of the link. The default value of **upper-limit**is 95, and the default value of **lower-limit**is 90.
- **performance** – Configure the load balancing mode for high-performance. In this mode, the system adjusts link to keep the link balance as fast as possible.

To restore the default mode of the load balancing mode, use the command **no dynamic-extra-conf mode**.

For SG-6000 K9180/K6580 and X series platforms, use the **mode** {**compatibility** [**upper-limit** *value* **lower-limit** *value*] | **performance**} command to configure.

For more information about configuring load balancing, use the following command:

description*description*

- *description* – Configure Additional details of llb profile.

To cancel the configuration description, use the command: **no description**.

The active link detection interval is the interval at which the system sends detection packets to the specified host. To configure the link detection interval, use the following command:

host-detect interval*interval*

- *interval*- Specifies the link detection interval. The range is 60 to 86400s. The default value is 600s.

To restore the default value of the link detection interval, use the following command:

no host-detect interval

Viewing the Link Detection Result for a Specified Domain Name

To view the link detection result for a specified domain name, in any mode, use the following command:

show llb rule [*rule-name*] **spec-host task** { **all** | *host-name*} [**slot***slot-number*]

- **rule** [*rule-name*] – Specifies the LLB rule name.
- **spec-host task** { **all** | *host-name*} - View the link detection result for a specified domain name
    - **all**- View link detection results of all domain names in the LLB rule.
    - *host-name*- Specify the domain name and view the link detection result of this domain name.

- **slot***slot-number* - Specify the slot number of the module card. View the link detection result of all domain names (*all*) or the specified domain name (*host-name*) on the module card. This parameter is only supported on X-Series devices.

Configuring LLB Rule

After you bind SLA profile (optional) and LLB profile to the route to form an LLB rule, you can control and load balance outbound link traffic. Currently the system support binding destination routing (DBR) and policy-based routing (PBR). To configure LLB rules, use the following command in global mode:

llb rule*rule-name* [**ipv6**] {**pbr***pbr-name***id***match-id* | **dbr** [**vrouter***vr-name*] {{*X:X:X:X::X/M*} | {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}} {**profile***profile-name*} [**sla-profile***profile-name*] [**host** *host-book-name*]

- *rule-name* – Specify the name of llb rule.
- **ipv6** – Specifies the type of the LLB Rule as IPv6. If not specified, the type of the LLB Rule is IPv4.
- **pbr** *pbr-name* – Specify the name of PBR.
- **id***match-id* – Specify the match id of PBR. The IP type of PBR rule should be the same as the LLB Rule. If the IP tyoe of LLB Rule is IPv6, the IP type of PBR rule should be IPv6 as well.
- **dbrvrouter***vr-name* – Specify the vroute's name of DBR.
- {*X:X:X:X::X/M*} | {*A.B.C.D/M* | *A.B.C.D A.B.C.D* } – Specifies the Vrouter destination address. When the type of the LLB Rule is specified as IPv6, use *X:X:X:X::X/M* to configure the destination address of Vrouter. When the type of the LLB Rule is specified as IPv4, the device supports two modes, A.B.C.D / M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
- **profile***profile-name* – Specifies the bound LLB profile. The IP type of the LLB Profile should be the same as the LLB Rule.

- **sla-profile***profile-name* - Specifies the bound SLA profile. You need to select an SLA profile of the same type based on the IP type configured for the LLB rule. For the SG-6000 A series, K series (all models except K9180/K6580), and CloudEdge platforms, the SLA profile will only take effect when any of the options in the LLB profile's preferred scheduling algorithm, secondary scheduling algorithm, or alternative scheduling algorithm is set to "Dynamic Proximity" algorithm.
- **host** *host-book-name* - Specifies the bound host book.

To delete the specified LLB rule,in the global configuration mode, use the command: **no llb rule***llb-rule-name*.

Notes: The LLB Rule name in the IPv4 should be different from that in IPv6.

Viewing LLB Rule Configuration Information

To view information about LLB rule configurations, in any mode, use the following command:

show llb rule [*rule-name*]

- *rule-name* – Displays the LLB rule configuration information of the specified name. If not specified, configuration information of all LLB rules is displayed.

Viewing Link Detection Results of Specified Domain

To view link detection results of the specified domain name, in any mode, use the following command:

show llb rule*rule-name***spec-host task** {**all** | *host-name*} [**slot***slot-number*]

- *rule-name* – Specifies the LLB rule name.
- **spec-host task** { **all** | *host-name*} - Displays the link detection results based on the specified domain name.

- **all**- Displays link detection results of all domain names in the LLB rule.
- *host-name*- Specifies the domain name to view its link detection results.

- **slot***slot-number* - Specifies the slot number of the module card to view link detection results of the module card based on all domain names (*all*) or specified domain name (*host-name*). This parameter is available only for X-series devices.

Viewing LLB Profile Configuration Information

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

show llb profile [*profile-name*]

- *profile-name* – Displays the LLB profile configuration information of the specified name. If not specified, configuration information of all LLB profiles is displayed.

Viewing Statistical Period for Bandwidth

To view the current statistical period for bandwidth of the system, in any configuration mode, use the following command:

showllbbandwidth-statistics-period

Viewing SLA Profile Configuration Information

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

show sla-profile [*profile-name*]

- *profile-name* – Displays the SLA profile configuration information of the specified name. If not specified, configuration information of all SLA profiles is displayed.

For more information, refer to the **Traffic Management** > **Load Balancing** > **Link Load Balancing** > **Outbound Load Balancing** topic in *StoneOS CLI User Guide*. FR 41325

Configuring an Interface

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

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

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

- Binding an interface to a zone
- Configuring an interface IP address
- Configuring an interface MTU value
- Configuring interface force shutdown
- Specifying the Track Object

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

- Configuring 10 G Interface Auto Tuning
- Configuring ISP of the Interface
- Configuring Link Load Balancing Priority of the Interface
- Configuring Link Load Balancing Weight of the Interface
- Configuring Busy Protection for Link

.....

Configuring ISP of the Interface

Device Supported: : Only the SG-6000 A series, K series (excluding K9180/K6580), and CloudEdge platforms support this function.

Configure the IPv4 ISP or IPv6 ISP of the interface, and the corresponding link will also be bound to the specified ISP. In interface configuration mode, use the following command to configure the ISP of the interface:

{**isp** | **isp-v6**} *isp-name*

- **isp***isp-name*- Specifies the existing IPv4 ISP information to be bound with the interface.
- **isp-v6***isp-name*- Specifies the existing IPv6 ISP information to be bound with the interface.

isp-v6*isp-name*- Specifies the existing IPv6 ISP information to be bound with the interface.

Notes: Non-root VSYS does not support this configuration.

Configuring Link Load Balancing Priority of the Interface

Device Supported: : Only the SG-6000 A series, K series (excluding K9180/K6580), and CloudEdge platforms support this function.

Specify the link load balancing priority of the interface. When the system performs outbound load balancing and uses a priority scheduling policy, this value determines the priority of the link associated with the interface. To configure the link load balancing priority of the interface, in interface configuration mode, use the following command:

llb priority*value*

- *value* - Specifies the link load balancing priority of the interface. The value range is 1 to 100, with a default value of 50. The smaller the number, the higher the priority of the egress link.

In interface configuration mode, use the **nollb priority** command to restore the default value of the interface's link load balancing priority.

Notes: Non-root VSYS does not support this configuration.

Configuring Link Load Balancing Weight of the Interface

Device Supported: : Only the SG-6000 A series, K series (excluding K9180/K6580), and CloudEdge platforms support this function.

Specify the link load balancing weight of the interface. When the system performs outbound load balancing, different load balancing algorithms calculate and select routes based on this weight. To configure the link load balancing weight of the interface, in interface configuration mode, use the following command:

llb weight*value*

- *value* - Specifies the link load balancing weight of the interface. The value range is 1 to 255, with a default value of 50. The larger the number, the greater the weight of the interface, and the more traffic the corresponding egress link forwards.

In interface configuration mode, use the **nollb weight** command to restore the default value of the interface's link load balancing weight.

Notes: Non-root VSYS does not support this configuration.

Configuring Busy Protection for Link

Device Supported: : Only the SG-6000 A series, K series (excluding K9180/K6580), and CloudEdge platforms support this function.

You can configure busy protection for the egress links, i.e., configure the actual bandwidth value and bandwidth threshold of the interface. When the outbound traffic of a link reaches the bandwidth threshold specified for the interface, if the system selects an egress link through a load balancing algorithm, it will prioritize other non-busy links; when the system selects an egress link through a session persistence algorithm, if a matching session persistence table entry is found, the link busy protection function will be ignored, and the matched link will be selected to forward the traffic.

In interface configuration mode, use the following command:

bandwidth {**downstream** | **upstream**} {**threshold***value*| *bandwidth*}

- **downstream** - Configures the maximum bandwidth value and bandwidth threshold in the downstream direction of the interface.
- **upstream** - Configures the maximum bandwidth value and bandwidth threshold in the upstream direction of the interface.

- **threshold***value* - Specifies the bandwidth threshold of the interface. The value range is 0 to 100 (0% to 100%), with a default value of 0, indicating no limit.
- *bandwidth* - Specifies the maximum bandwidth value of the interface. The range is 512,000 to 1000,000,000,000 bps. The default value is 1000,000,000 bps.

In interface configuration mode, use the **nobandwidth** {**downstream** | **upstream**} [**threshold**] command to restore the default values of the interface's maximum bandwidth and bandwidth threshold.

Notes: Non-root VSYS does not support this configuration.

Supporting to Specify the Source Interface When Upgrading Signature Database and Trusted Root Certificate

WebUI

Updating Signature Database

Device Supported: :

The following devices support to upgrade antivirus intelligence file engine database.

- A-series: Except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200.
- K-series: SG-6000-K2680, SG-6000-K2380, and SG-6000-K6280-GS.SG-6000-K6580, and SG-6000-K9180.
- X-series: SG-6000-X25803, SG-6000-X25812, SG-6000-X9180-GS, and SG-6000-X8180.
- CloudEdge: Only CloudEdge that is deployed on X86-based or ARM-based server.

The signature databases that can be installed include Encrypted traffic detection database,Share Access signature database,Application signature database, URL signature database, Antivirus signature database, antivirus intelligence file engine database, Sandbox Whitelist Database, IPS signature database, IP reputation database, SSL proxy domain whitelist signature database, Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database. Except Encrypted traffic detection database,SSL proxy domain whitelist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, you can only view other signature databases when the system is installed with the corresponding licenses. The system support the following two methods to upgrade signature databases: remote update via HTTP and HTTPS; local update via downloading update package through the default signature database update server.Except the SSL proxy domain whitelist signature database or ISP Information Database, you can only view signature databases installed with licenses.

The system supports to download each signature database over IPv6.

To update signature database, take the following steps:

1. Select **System** > **Upgrade Management** > **Signature Database Update**.
2. In the **Signature Database Update** page, configure the following.

Option	Description
Current Version	Show the current version number.
Latest Version	Show the latest version number. **Note:** The latest version of the ISP information database can be displayed only when the current version exists. The latest version of other signature databases can be displayed only when the corresponding signature database licenses are activated and the current version exists.
Update Entire Signature	In the IPS signature database module, you can update the current IPS signature database to the IPS entire signature database. By default, this

Option	Description
	option is disabled. Click  to update the IPS entire signature database. This operation may cause the throughput performance of the device to drop by up to 20%. It is recommended that you configure it based on the actual load of the device. Click  to cancel updating the IPS entire signature database. This operation reduces the current number of signatures in the IPS signature database and may affect the details of threat events that have been generated. **Notes:** The following devices support this option: • A-series: SG-6000-A200/A200G4B /A200W/A1000/A1100 • E-series: E1606/E1700/E2300 /E2800/E2860/E2868/E3662/E3668/E3960/E3968 /E3965/E5168/E5260/E5268/E5560/E5568/E5660 /E5760/E5960
Remote Update	Encrypted traffic detection database, Application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database. • Protocol: Select the update method of the signature database,

Option	Description
	including HTTP and HTTPS. Click **Restore Default** to restore the default HTTPS transmission method. • Update Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. The IPv4 and IPv6 address are supported for configuring the update server address. Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers according to your need. In **Update Server**, specify the server IP or domain name, and select a Virtual Router and source interface from the drop-down list. The source interface needs to be within the virtual router. When updating the trusted root certificate database, the system will access the update server via this source interface. • Update Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally. In **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button of **Auto Update** and specify the auto update time. Click **Ok** to save your changes. • Update Now: Click **Ok And Online Update** to update the sig-

Option	Description
	nature database right now.
Local Update	Download the update package from the default feature update server for local update. • Download the upgrade packages of the encrypted traffic detection database, application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database, SSL proxy domain whitelist signature database, , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database from https://update1.hillstonenet.com and https://update2.hillstonenet.com. • Click **Browse** and select the signature file in your local PC, and then click **Upload**. **Notes:** 1. Before StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Botnet C&C Detection Package" link of the default update server. From StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Encrypt Botnet C&C Detection Package" link of the default update server. 2. If a large number of devices (with the same version and model) need local update, contact Hillstone's support team to acquire bulk update solutions.

Updating Trusted Root Certificate Database

To ensure that the root certificates stored on your device are sufficient and up-to-date, and to reduce errors occurred during server certificate verification, you need to update the trusted root certificate database timely. System supports both remote upgrade and local upgrade. When updating the trusted root certificate database, system will delete revoked certificates and expired certificates, and add new certificates.

To update the trusted root certificate database, take the following steps:

1. Select **System** > **Upgrade Management** > **Trusted Root Certificate Update**.
2. In the **Trusted Root Certificate Update** page, configure the following.

Option	Description
Current Version	Show the current version number.
Remote Update	Click **Remote Update** and configure the following update parameters. • Update Server: By default, system updates the trusted root certificate database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers as needed. Under **Update Server**, specify the server IP or domain name, and select a Virtual Router and source interface from the drop-down list. The source interface needs to be within the virtual router. When updating the trusted root certificate database, the system will access the update server

Option	Description
	via this source interface. • Update Proxy Server: When the device accesses the Internet through an HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server to ensure the trusted root certificate database can be updated normally. Under **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button and specify the auto update time. Click **OK** to save your changes. • OK And Online Update: Click the button to update the trusted root certificate database immediately.
Local Update	Click **Local Update**, and click **Browse** to select a trusted root certificate database file in your local PC, and then click Upload.

For more information, refer to the **System Management** > **Upgrading System** topic in *StoneOS WebUI User Guide*. FR 44095

CLI

Configuring the ISP Information Database

By default, the system automatically updates the ISP information database on a daily basis. You can modify the update configuration as needed.

.....

Configuring the Update Server

The system provides the default update server of the ISP information database update1.hillstonenet.com and update2.hillstonenet.com. You can also configure other update servers to download the latest predefined ISP profile as needed. At most 3 update servers can be configured. To configure an update server, in global configuration mode, use the following command:

isp-information update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the server to be configured. The server supports both IPv4 and IPv6. The default value of **server1** is update1.hillstonenet.com and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server, which can be an IP address or domain name, such as update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router bound to the update server. By default, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the ISP information database. If not specified, the management port will be used as the default source interface.

To restore the default configuration of server1 or server2 or delete the configuration of server3, in global configuration mode, use the following command:

no isp-information update {**server1** | **server2** | **server3**}

For more information, refer to the **Routing** > **ISP Route** topic in *StoneOS CLI User Guide*. FR 44095

Updating the Signature Database

Applications are updated frequently. Hillstone devices allow you to update the application signature database to assure the devices can adapt to these changes in time and identify the latest software version. You can download the latest signature file and upload to the device. Hillstone regularly uploads new signature files on the Hillstone website. You need to download the files, and then upload them to the device.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest application signature database as needed. To configure the update the server, in the global configuration mode, use the following command:

app update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the application signature information database. If not specified, the management port will be used as the default source interface.

In the global configuration mode, use the following command to restore the default settings of the update server.

no app update {**server1** | **server2** | **server3**}

For more information, refer to the **Firewall** > **Service and Application** > **Application Overview** > **Application Identification** topic in *StoneOS CLI User Guide*. FR 44095

Updating AV Signature Database

By default system updates the AV signature database everyday automatically. You can change the update configuration as needed.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest AV signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

av signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this

source interface when updating the virus signature information database. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no av signature update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Anti-Virus** topic in *StoneOS CLI User Guide*. FR 44095

Updating AV Intelligence File Engine Database

By default, the system will automatically update the AV intelligence file engine database every day. You can change the update configuration of the AV intelligence file engine database as needed. Only X86-based or ARM-based devices support the function.

.....

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest AV intelligence file engine database as needed. To configure the update the server, in the global configuration mode, use the following command:

av-file-engine update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of server1 is update1.hillstonenet.com, and the default value of server2 is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an ip-addressor a domain-name, for example, update1.hillstonenet.com.

- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the anti-virus intelligence file engine database. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no av-file-engine update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Anti-Virus** topic in *StoneOS CLI User Guide*. FR 44095

Updating Sandbox Whitelist Database

By default system updates the sandbox whitelist database everyday automatically. You can change the update configuration as needed.

.....

Configure an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest sandbox whitelist as needed. To configure the update the server, in the global configuration mode, use the following command:

sandbox whitelist update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the sandbox whitelist. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no sandbox whitelist update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Sandbox** topic in *StoneOS CLI User Guide*. FR 44095

Updating IPS Signature Database

By default StoneOS updates the IPS signature database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. StoneOS supports auto update and local update. Non-root VSYS does not support this feature. For more information about the signature database configurations, please refer to the table below.

Configuration	CLI
To configure an update mode (auto by default)	In the global configuration mode, use the following command: • Specifying the update mode: **ips signature update mode {auto | manual}** • Restoring to the default: **no ips signature update mode**
To configure an update protocol	In the global configuration mode, use the following command:

Configuration	CLI
(HTTPS by default)	• Specifying the update protocol: **ips signature update protocol HTTP** • Restoring to the default: **no ips signature update protocol HTTP**
To configure an update server	In the global configuration mode, use the following command. The IPv4 and IPv6 address are supported for configuring the update server address. • Specifying the update server: **ips signature update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] • Canceling the server: **no ips signature update** {**server1** | **server2** | **server3**}
To configure an update schedule	In the global configuration mode, use the following command to make the IPS signature database update daily or weekly: **ips signature update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*] In the global configuration mode, use the following command to make the IPS signature database update hourly: **ips signature update schedule hourly***minute* • *minute* – Specifies the minute that the update starts.
To update now	In the execution mode, use the following command: **exec ips signature update**
To update locally	In the execution mode, use the following command: **import ips signature from** {{**ftp** | **ftps** | **sftp**} **server***ip-address* [**user***user-name***password***password* | **vrouter***vr-name*] | **tftp server***ip-address* [**vrouter***vr-name*]} *file-name*

Configuration	CLI
To view signature statistics	**show ips signature info**
To view signature database configurations	**show ips signature update**

For more information, refer to the **Threat Prevention** > **IPS** topic in *StoneOS CLI User Guide*. FR 44095

Configuring IP Reputation Filtering

By default StoneOS updates the IP reputation database everyday automatically. You can change the update configuration as needed.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest IP reputation as needed. To configure the update the server, in the global configuration mode, use the following command:

ip-reputation update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*s, or a *domain-name*, for example, update1.hillstonenet.com.

- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the IP reputation database. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no ip-reputation signature update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Perimeter Traffic Filtering** topic in *StoneOS CLI User Guide*. FR 44095

Updating Geolocation Information Database

By default StoneOS updates the geolocation information database everyday automatically. You can change the update configuration as needed.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest geolocation informations as needed. To configure the update the server, in the global configuration mode, use the following command:

geolocation-IP-signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1 | server2 | server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of

server1is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the geolocation information database. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no geolocation-IP-signature update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Geolocation Information Database** topic in *StoneOS CLI User Guide*. FR 44095

Updating MITRE ATT&CK® Knowledge Base

By default StoneOS updates the MITRE ATT&CK® knowledge base everyday automatically. You can change the update configuration as needed.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest MITRE ATT&CK® knowledge base as needed. To configure the update server, in the global configuration mode, use the following command:

ATT&CK update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1 | server2 | server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address* or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the MITRE ATT&CK® knowledge base. If not specified, the management port will be used as the default source interface.

To cancel the specified update server, in the global configuration mode, use the following command:

no ATT&CK update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention > MITRE ATT&CK® Knowledge Base** topic in *StoneOS CLI User Guide*. FR 44095

Updating Botnet Prevention Signature Database

By default system updates the botnet prevention signature database everyday automatically. You can change the update configuration as needed.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest

botnet prevention signatures as needed. To configure the update the server, in the global configuration mode, use the following command:

botnet-c2-prevention signature update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the Botnet Prevention signature database. If not specified, the management port will be used as the default source interface.

To cancel the specified update the server, in the global configuration mode, use the following command:

no botnet-c2-prevention signature update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Botnet Prevention** topic in *StoneOS CLI User Guide*. FR 44095

Updating Encrypted Traffic Detection Database

By default, the system automatically updates the encrypted traffic detection database everyday. You can change the encrypted traffic detection database configuration as needed.

.....

Configuring an Update Server

The system provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers as needed. To configure an update server, use the following command in the global configuration mode:

etd update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1** is update1.hillstonenet.com, and the default value of **server2** is update2.hillstonenet.com.
- *ip-address* | *domain-name* – Specifies the name of the update server. It can be an *ip-address*or a *domain-name*, for example, update1.hillstonenet.com.
- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the encrypted traffic detection database. If not specified, the management port will be used as the default source interface.

To cancel a specified update server, use the following command in the global configuration mode:

no etd update {**server1** | **server2** | **server3**}

For more information, refer to the **Threat Prevention** > **Encrypted Traffic Detection** topic in *StoneOS CLI User Guide*. FR 44095

Updating the Predefined URL Database

By default, the system updates the predefined URL database every day. You can change the update parameters according to your own requirements. Hillstone provides two default URL database

update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can update your URL database online or manually. For more information about how to configure the predefined URL database, see the following table:

Configuration	CLI
Specifying the update mode	In the global configuration mode, use the following command: **url-db update mode** {**auto** | **manual**}
To configure an update protocol (HTTPS by default)	In the global configuration mode, use the following command: • Specifying the update protocol: **url-ub update protocol HTTP** • Restoring to the default: **no url-ub update protocol HTTP**
Configuring the update server	In the global configuration mode, use the following command: **url-db update** {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]
Specifying the update schedule	In the global configuration mode, use the following command: **url-db update schedule** {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]
Updating now	In the execution mode, use the following command: **exec url-db update**
Updating manually	In the execution mode, use the following command: **import url-db from** {**ftp server***ip-address* [**vrouter***vrouter-name*] [**user***user-name***password***password*] | **tftp server***ip-address* | **usb0** | **usb1**} *file-name*

Configuration	CLI
	Note: Non-root VSYS does not support this command.
Viewing URL DB info	**show url-db info**
Viewing URL DB update configuration	**show url-db update**
Viewing URL statistics	**show statistics-set***name* [{**current** | **history** | **history-max**} [**sort-by** {**up** | **down** | **item**}]]
Refreshing URL information in the local cache manually	**exec url-db refresh** {**all** | **url** *url-string*} • **all**- Refresh all URL information in the local cache. • **url** *url-string*- Refresh the specified URL in the local cache.
Viewing the count of URL statistics	**show url-db statistics**
Clearing the count of URL statistics	**clear url-db statistics**

For more information, refer to the **Data Security & URL Filtering** > **Object Configuration** topic in *StoneOS CLI User Guide*. FR 44095

Share Access Signature Database

You can change the update configurations of share access signature database as needed. The update configurations include:

- Configuring the update mode of share access signature database
- Updating now
- Importing a share access signature file

- Viewing update information of share access signature database
- Viewing information of share access signature database

Non-root VSYS also supports the share access function, but does not support the update configurations of share access signature database.

Configuring the Update Mode of Share Access Signature Database

To update the share access signature database, in the global configuration mode, use the following command:

share-access-detect signature update [**mode** {**auto** | **manual**} | **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* | **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] } | **server1** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **server2** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **server3** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **protocol HTTP**]

- **mode** {**auto** | **manual**} – Specifies the update mode of share access. System supports automatic and manual update modes. The default mode is automatic update.
- **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* – Specifies the proxy server of share access database update.
- **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] – Specifies the automatic update schedule of share access database.
- **server1** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 1.
- **server2** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 2.
- **server3** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 3.

- **protocol HTTP** - Specifies the update protocol as HTTP, and the default protocol is HTTPS.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the share access signature database. If not specified, the management port will be used as the default source interface.

For more information, refer to the **Policy** > **Share Access** topic in *StoneOS CLI User Guide*. FR 44095

Updating SSL Proxy Domain Whitelist Signature Database

You can change the update configuration as needed. By default, the system updates the SSL proxy domain whitelist signature database everyday automatically.

.....

Configuring an Update Server

System provides two default update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can also configure another up to three update servers to download the latest domain whitelist signature as needed. To configure the update server, in the global configuration mode, use the following command:

sslproxy-exempt-domain update {**server1** | **server2** | **server3**} {*ip* | *dns-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1** | **server2** | **server3** – Specifies the update server you want to configure. The IPv4 and IPv6 address are supported for configuring the update server address. The default value of **server1**is update1.hillstonenet.com, and the default value of **server2**is update2.hillstonenet.com.
- *ip* | *dns-name* – Specifies the name of the update server. It can be an *ip-address*, or a *domain-name*, for example, update1.hillstonenet.com.

- **vrouter***vrouter-name* – Specifies the virtual router to which the update server is bound. If not specified, **trust-vr** is used.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the SSL proxy domain whitelist signature database. If not specified, the management port will be used as the default source interface.

To cancel the specified update server, in the global configuration mode, use the following command:

no sslproxy-exempt-domain {**server1** | **server2** | **server3**}

For more information, refer to the **Data Security & URL Filtering** > **SSL Proxy** topic in *StoneOS CLI User Guide*. FR 44095

Updating the Trusted Root Certificate Database

To ensure that the root certificates stored on your device are sufficient and up-to-date, and to reduce errors occurred during server certificate verification, you need to update the trusted root certificate database timely. You can change the update configurations of the trusted root certificate database as needed. The update configurations include:

- Configuring the update mode of the trusted root certificate database
- Updating now
- Importing a trusted root certificate database file
- Viewing update information of the trusted root certificate database
- Viewing information of the trusted root certificate database

Configuring the Update Mode of the Trusted Root Certificate Database

To configure the update mode of the trusted root certificate database, in the global configuration mode, use the following command:

trusted-root-ca-store update {**mode** {**auto** | **manual**} | **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* | **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} | **server1** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **server2** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **server3** {*domain* | *ip*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*] | **protocol HTTP**}

- **mode** {**auto** | **manual**} – Specifies the update mode of the trusted root certificate database. System supports automatic and manual update modes. The default mode is automatic update.
- **proxy-server** {**main** | **backup**} *proxy-ip proxy-port* – Specifies the proxy server for updating the trusted root certificate database.
- **schedule** {**daily** | **weekly** {**sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat**} | **monthly** *date*} [*HH:MM*] – Specifies the schedule for automatically updating the trusted root certificate database.
- **server1** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 1.
- **server2** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 2.
- **server3** {*domain* | *ip*} [**vrouter***vrouter-name*] – Specifies the domain, IP address and VRouter of update server 3.
- **protocol HTTP** - Specifies the update protocol as HTTP, and the default protocol is HTTPS.
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be within the virtual router. Once specified, the system accesses the update server via this source interface when updating the trusted root certificate database. If not specified, the management port will be used as the default source interface.

For more information, refer to the **Data Security & URL Filtering** > **SSL Proxy** topic in *StoneOS CLI User Guide*. FR 44095

Adding Multiple Check Items for ZTNA Endpoint Tag Rule of Windows and macOS

WebUI

Configuring Endpoint Items

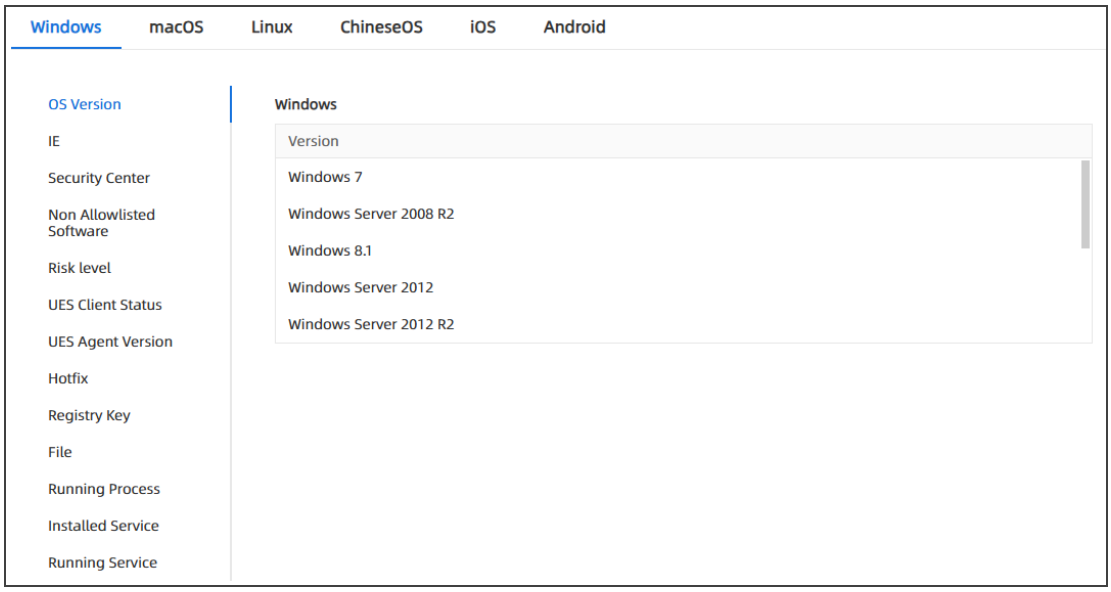
The system supports endpoint item management of the following operating systems:

- Windows endpoint item management
- macOS endpoint item management
- Linux endpoint item management
- ChineseOS endpoint item management
- iOS endpoint item management
- Android endpoint item management

Windows Endpoint Item Management

To manage Windows endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **Windows**.



2. View the Window endpoint items that the system support to collect and configure custom items.

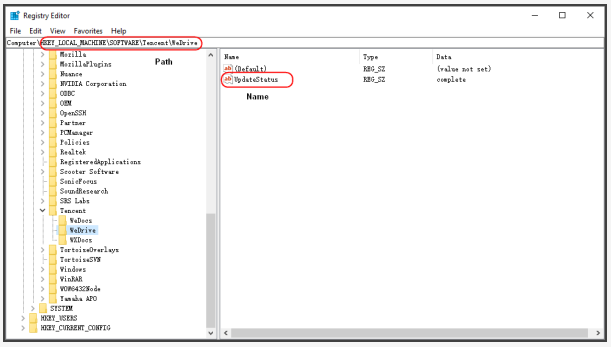
Windows Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the Windows endpoint. Click **OS Version** to view the Windows versions that the system supports to check, including: • Windows 7/8.1/10/11 • Windows server 2008 R2/2012/2012 R2/2016/2019/2022
IE	Checks the IE version and security level of the Windows endpoint. Click **IE** to view the IE versions and IE security levels that the system supports to collect:

Option	Description
	• IE Version: IE7 ~ IE11 • IE Security Level: custom define, low, medium low, medium, medium high, high
Security Center	Checks the system security of the Windows endpoint. Click **Security Center** to view the security items that the system supports to check: • Whether anti-spyware software is installed, enabled and updated. • Whether anti-virus software is installed, enabled and updated. • Whether firewall software is installed and enabled. • Whether windows-update is enabled.
Non Allowlisted Software	Checks whether any software not on the allowlist is installed on the Windows endpoint.
Risk level	Checks the risk level of the Windows endpoint. Click **Risk level** to display information about the risk levels supported by the system, including normal, low, medium, high, and critical.
UES Client Status	Checks whether the UES client on the Windows endpoint is online.

Windows Endpoint Items - Custom

Option	Description
UES Agent Version	Checks the UES client version on the Windows endpoint. Click **UES Agent Version**. On the **UES Agent Version** page, click **New**, enter the UES agent version information to be collected, and click **OK**. You can customize up to 5 UES agent version information entries to be collected. • Alias: Specify the UES agent version's alias. The length is 1 to 31 characters. • UES Agent version: Specify the UES agent version number.
Hotfix	Checks whether the specified hot fix is installed in the Windows endpoint. You can add up to 5 hot fixes as Windows endpoint items. Click **Hotfix** and then **New** on the Hotfix page. Define hot fix information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the hot fix's alias. The length is 1 to 31 characters. • Hotfix: Specify the actual name of the hot fix. The length is 1 to 255 characters.
Registry Key	Checks whether the specified registry key exists in the Windows endpoint. You can add up to 5 registry keys as Windows endpoint items. Click **Registry Key** and then **New** on the Registry Key page. Define registry key information that needs to be col-

Option	Description
	lected and then click **OK** to save the configuration. • Alias: Specify the registry key's alias. The length is 1 to 31 characters. • Key: Specify the actual name of the registry key. The length is 1 to 255 characters. The content filled in the text box is "key path + name". For example, in the following figure, the content filled in is HKEY_ LOCAL_ Machine\Software\Tencent \ WeDrive\UpdateStatus. 
File	Checks whether the specified file exists in the Windows endpoint. You can add up to 5 files as endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.

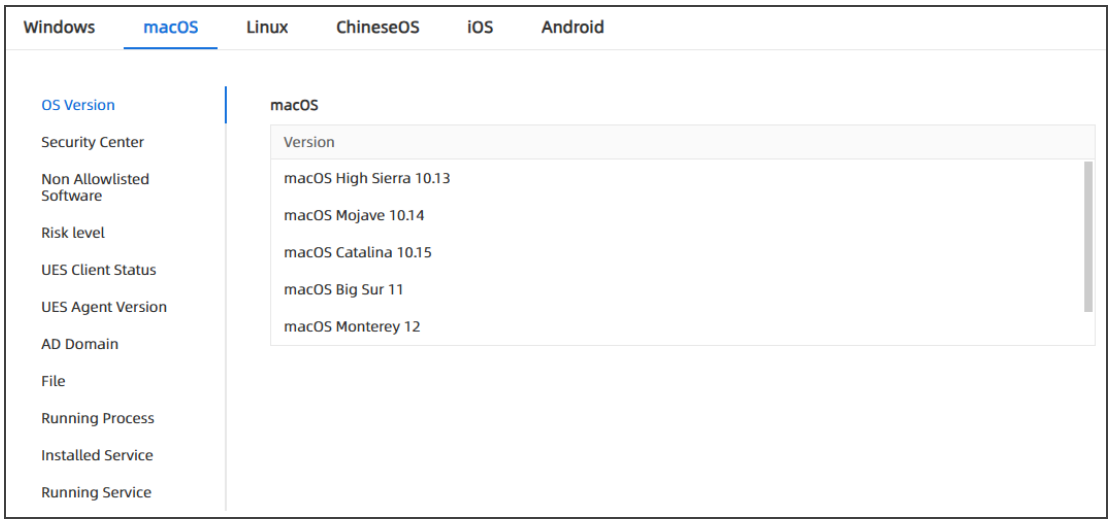
Option	Description
Running Process	Checks whether the specified process is running in the Windows endpoint. You can add up to 5 running processes as Windows endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the process. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the Windows endpoint. You can add up to 5 installed services as Windows endpoint items. Click **Installed Service** and then **New** on the Installed Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.
Running Service	Checks whether the specified service is running in the Windows endpoint. You can add up to 5 running services as Windows endpoint items. Click **Running Service** and then **New** on the

Option	Description
	Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

macOS Endpoint Item Management

To manage macOS endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **macOS**.



2. View the macOS endpoint items that the system support to collect and configure custom items.

macOS Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the macOS endpoint. Click **OS**

Option	Description
	Version to view the macOS versions that the system supports to check, including: • macOS High Sierra 10.13 • macOS Mojave 10.14 • macOS Catalina 10.15 • macOS Big Sur 11 • macOS Monterey 12 • macOS Ventura 13
Security Center	Checks the system security of the macOS endpoint. Click **Security Center** to view the security items that the system supports to check, that is, whether FileVault is enabled.
Non Allowlisted Software	Checks whether any software not on the allowlist is installed on the macOS endpoint.
Risk level	Checks the risk level of the macOS endpoint. Click **Risk level** to display information about the risk levels supported by the system, including normal, low, medium, high, and critical.
UES Client Status	Checks whether the UES client on the macOS endpoint is online.

macOS Endpoint Items - Custom

Option	Description
UES Agent Version	Checks the UES client version on the macOS endpoint. Click **UES Agent Version**. On the **UES Agent Version** page, click **New**, enter the UES agent version information to be collected, and click **OK**. You can customize up to 5 UES agent version information entries to be collected. • Alias: Specify the UES agent version's alias. The length is 1 to 31 characters. • UES Agent version: Specify the UES agent version number.
AD Domain	Checks the AD domain name of the macOS endpoint. You can add one AD domain name as the macOS endpoint item. Click **AD Domain** and then **New** on the AD Domain page. Define AD Domain information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the AD domain name's alias. The length is 1 to 31 characters. • AD Domain: Specify the AD domain name. The length is 1 to 255 characters.
File	Checks whether the specified file exists in the macOS endpoint. You can add up to 5 files as macOS endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration.

Option	Description
	• Alias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.
Running Process	Checks whether the specified process is running in the macOS endpoint. You can add up to 5 running processes as macOS endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the process. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the macOS endpoint. You can add up to 5 installed services as macOS endpoint items. Click **Installed Service** and then **New** on the Installed Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.

Option	Description
Running Service	Checks whether the specified service is running in the macOS endpoint. You can add up to 5 running services as macOS endpoint items. Click **Running Service** and then **New** on the Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

For more information, refer to the **ZTNA > Managing Endpoint Items** topic in *StoneOS WebUI User Guide*. FR 45429

CLI

Managing Endpoint Items

The system supports endpoint item management of the following operating systems:

- Windows endpoint item management
- macOS endpoint item management
- Linux endpoint item management
- iOS endpoint item management
- Android endpoint item management
- ChineseOS endpoint item management

Windows Endpoint Item Management

The following table shows the types of predefined Windows endpoint items supported by the system.

Predefined Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the Windows endpoint.	is, is-not	windows-7/8.1/10/11；windows-server-2008-R2/2012/2012-R2/2016/2019/2022
anti-virus	Checks whether anti-virus software is installed, enabled and updated in the Windows endpoint.	is, is-not	installed, enabled, updated
firewall	Checks whether firewall is installed and enabled in the Windows end-	is, is-not	installed, enabled

Predefined Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	point.		
anti-spyware	Checks whether anti-spy software is installed, enabled and updated in the Windows end-point.	is, is-not	installed, enabled, updated
windows-update	Checks whether Win-dows update is enabled in the Windows end-point.	is, is-not	enabled
ie-version	Checks the IE version of the Windows end-point.	=, !=, >, <, >=, <=	IE7 ~ IE11
ie-security-level	Collects the IE security level of the Win-dows end-	=, !=, >, <, >=, <=	custom-define, low, medium-low, medium, medium-high, high

Predefined Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	point.		
non-allowl-isted-software	Checks whether any software not on the allowl-ist is installed on the Win-dows end-point.	is, is-not	exist
risk-level	Checks the risk level of the Windows end-point.	=, !=, >, <, >=, <=	normal, low, medium, high, critical
ues-client-status	Checks whether the UES client on the Windows endpoint is online.	is, is-not	online

The following table shows the types of custom Windows endpoint items supported by the system.

Custom Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
process	Checks whether the specified process is running in the Windows endpoint.	exist, not-exist	Alias of the specified process
service-installed	Checks whether the specified service is installed in the Windows endpoint.	exist, not-exist	Alias of the specified service
service-running	Checks whether the specified service is running in the Windows endpoint.	exist, not-exist	Alias of the specified service
registry-key	Checks whether the specified registry key exists in the Windows endpoint.	exist, not-exist	Alias of the specified registry key
file	Checks whether the specified file exists in the Win-	exist, not-exist	Alias of the specified file

Custom Windows Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	dows endpoint.		
hotfix	Checks whether the specified Windows hot fix is installed in the Windows endpoint.	exist, not-exist	Alias of the specified hot fix
ues-agent-version	Checks the UES client version on the Windows endpoint.	=, !=, >, <, >=, <=	Alias of the specified UES client version

.....

Defining UES Client Version as Endpoint Item

You can configure the UES client version as a Windows endpoint item. The ZTNA client will periodically collect and report the UES client version information to the firewall, which will check whether the specified UES client version is installed on the Windows endpoint. Based on the check results, the firewall will update the endpoint tag and the application resources that the endpoint is allowed to access.

To customize the UES client version information to be collected, in ztna-endpoint-information-windows-profile configuration mode, use the following command:

ues-agent-version alias*alias-name***value***ues-agent-version-name*

- **alias***alias-name* - Specifies an alias of the UES client version, which needs to be 1 to 31 characters in length.
- **value***ues-agent-version-name* - Specifies the real version number of the UES client, which needs to be 1 to 255 characters in length.

You can repeat the command above to customize up to 5 UES client version information entries to be collected.

To delete the specified UES client version information item configuration, in ztna-endpoint-information-windows-profile configuration mode, use the following command:

no ues-agent-version alias*alias-name*

macOS Endpoint Item Management

The following table shows the types of predefined macOS endpoint items supported by the system.

Predefined macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
os-version	Checks the OS version of the macOS endpoint.	is, is-not	10.13/10.14/10.15/11/12/13
fileVault	Checks whether the FileVault function is enabled in the macOS	is, is-not	enabled

Predefined macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
	endpoint.		
non-allowl-isted-soft-ware	Checks whether any software not on the allowlist is installed on the macOS endpoint.	is, is-not	exist
risk-level	Checks the risk level of the macOS endpoint.	=, !=, >, <, >=, <=	normal, low, medium, high, critical
ues-client-status	Checks whether the UES client on the macOS end-point is online.	is, is-not	online

The following table shows the types of custom macOS endpoint items supported by the system.

Custom macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
ad-domain	Checks the AD domain name of the macOS endpoint.	is, is-not	Alias of the specified AD domain name
process	Checks whether the specified process is running in the macOS endpoint.	exist, not-exist	Alias of the specified process
service-installed	Checks whether the specified service is installed in the macOS endpoint.	exist, not-exist	Alias of the specified service
service-running	Checks whether the specified service is running in the macOS endpoint.	exist, not-exist	Alias of the specified service
file	Checks whether the specified file exists in the macOS endpoint.	exist, not-exist	Alias of the specified file

Custom macOS Endpoint Items			
Endpoint Item Name (key-name)	**Description**	**Operator**	**Value**
ues-agent-version	Checks whether the specified UES client version exists in the macOS endpoint.	=, !=, >, <, >=, <=	Alias of the specified UES client version

.....

Defining UES Client Version as Endpoint Item

You can configure the firewall to check whether the specified UES client version exists in the macOS endpoint.

To customize the UES client version information to be collected, in ztna-endpoint-information-macos-profile configuration mode, use the following command:

ues-agent-version alias*alias-name***value***ues-agent-version-name*

- **alias***alias-name* - Specifies an alias of the UES client version, which needs to be 1 to 31 characters in length.
- **value***ues-agent-version-name* - Specifies the real version number of the UES client.

You can repeat the command above to customize up to 5 UES client version information entries to be collected.

To delete the specified UES client version information item configuration, in ztna-endpoint-information-macos-profile configuration mode, use the following command:

no ues-agent-version alias*alias-name*

Configuring the Endpoint Monitoring Period

After a user logs in successfully, the system will continuously monitor the endpoint state and adaptively adjust the resource access range granted to the user. The system supports configuration of the endpoint monitoring period. If endpoint information collection fails within the specified monitoring period and the number of consecutive failures reaches the specified threshold, the system will clear the user's endpoint tag and rematch ZTNA policies.

To configure the endpoint monitoring period, in the global configuration mode, use the following command:

ztna-endpoint-information-monitor { [**interval***interval-value*] [**threshold***threshold-value*] }

- **interval***interval-value* - Specifies the report period. The value ranges from 10 to 65535 minutes. The default value is 20.
- **threshold***threshold-value* - Specifies the threshold for the number of consecutive failures of endpoint information report. The value ranges from 2 to 65535. The default value is 2.

For more information, refer to the **ZTNA > Managing Endpoint Items** topic in *StoneOS CLI User Guide*. FR 45429

Adding the HA Monitor Page on the WebUI

WebUI

HA Monitor

To facilitate O&M personnel in conducting HA status inspection on devices, the system provides the HA Monitor page. This page visually displays detailed information about various HA statuses in the system, such as HA working mode, operating status, link interface status, peer status, etc., and provides corresponding quick configuration operations.

Before you start

- Read HA Introduction
- Learn about HA Basic Concepts

Viewing the HA Monitor Page

Select **System** > **HA** > **Monitor**.

> **Notes:** This page displayed may vary based on different platforms.



HA Monitoring Project Status Description

Monitoring Project	Status	Operation
Working Mode	The current HA deployment mode, which can be "Standalone", "Active-Passive", and "Peer Active-Active".	-
HA Admin Role	The role of the current device in the HA cluster, which can be "Master" or "Backup."	HA Master Switch Over
Twin-mode Admin Role	The administrator role of the device after enabling Twin-mode, which can be "Master" or "Backup." This project is not displayed when Twin-mode is not enabled.	-
Cluster Running Time	The operating duration when the HA function is enabled on the device and a peer device exists. When	-

	there is only one device in the HA cluster, the cluster running time is empty.	
Last Status Change	Records the time and reason for the HA status change.	-
Heartbeat Status	Monitors whether devices in the HA cluster can send and receive heartbeat messages normally.	-
Link Interface Status	Displays the status of interfaces configured on the HA configuration page. Different colors indicate different interface statuses, with blank spaces separating different types of interfaces. Hovering your mouse over the corresponding interface icon will show detailed information about the interface. • Green indicates the current interface status is normal, and the link quality is normal. • Yellow indicates the current interface status is normal, but link quality is poor, with packet loss. • Red indicates the current interface status is normal, but the link quality is unavailable; the current link may still send and receive messages, but severe packet loss will affect normal HA communication and configuration synchronization between HA. • Gray indicates the current interface is unavailable: the physical status, management status, or link status is down, which may be due to an unplugged interface or being shut down.	HA Interface Traffic Monitor

HA Status	The status of the current device's HA group. The HA status varies based on different working modes, as follows: • When the working mode is "Standalone," this project is not displayed. • When the working mode is "Active-Passive," it can be either "Master" or "Backup." • When the working mode is "Peer Active-Active," it can be either "Group 0: Master Group 1: Disabled" or "Group 0: Disabled Group 1: Master."	-
HA Link IP	The HA link IP address of the current device.	-
Peer Device SN	The SN of the peer device, which is not displayed if the peer does not exist.	-
Peer Status	The HA status of the peer device, which is not displayed if the peer does not exist.	-
Peer Link IP	The link IP address of the peer device, which is not displayed if the peer does not exist.	-
Configuration Sync Status	Displays the HA configuration synchronization mode as "Auto Synchronization." When the "HA Admin Role" is "Master," you can click **HA Synchronize Configuration** to perform manual synchronization.	HA Synchronize Configuration
Session Sync Status	The configuration status of the current session synchronization, which can be either "Auto Synchronization" or "Not Synchronized." When the "HA Admin Role" is "Master," you can click	HA Synchronize Session

	HA Synchronize Session to perform manual synchronization.	
Configuration Consistency of Master and Backup	Displays whether the configurations of the current HA master and backup devices are consistent, the check time, and the check method. If the result is empty, it indicates that no HA master-backup consistency check has been performed on the current device.	Configuration Consistency Check
HA Track Object: Information about current track object that is bound with the HA group, which is not displayed if no track objects are bound.		
Option	**Description**	
Status	Displays the status information about the current track object. If the tracking fails, HA will perform a master-backup switchover or redirect traffic to the peer device.	
Name	Displays the name of the track object.	
Threshold	Displays the alarm threshold of the track object. If the sum of the weights of all failed track members in the track object is greater than or equal to the configured alarm threshold, the tracking fails.	
Type	Displays the type of the track object, which includes Interface, Protocol, Link Quality Detection, and System Resource.	
Associated Item	Displays the name and group ID of the function module bound with the track object.	

Quick Operation Buttons

- **HA Master Switch Over:** When the working mode is "Active-Passive," you can click **HA Master Switch Over** to perform master-backup switchover. This button is not displayed in

other working modes.

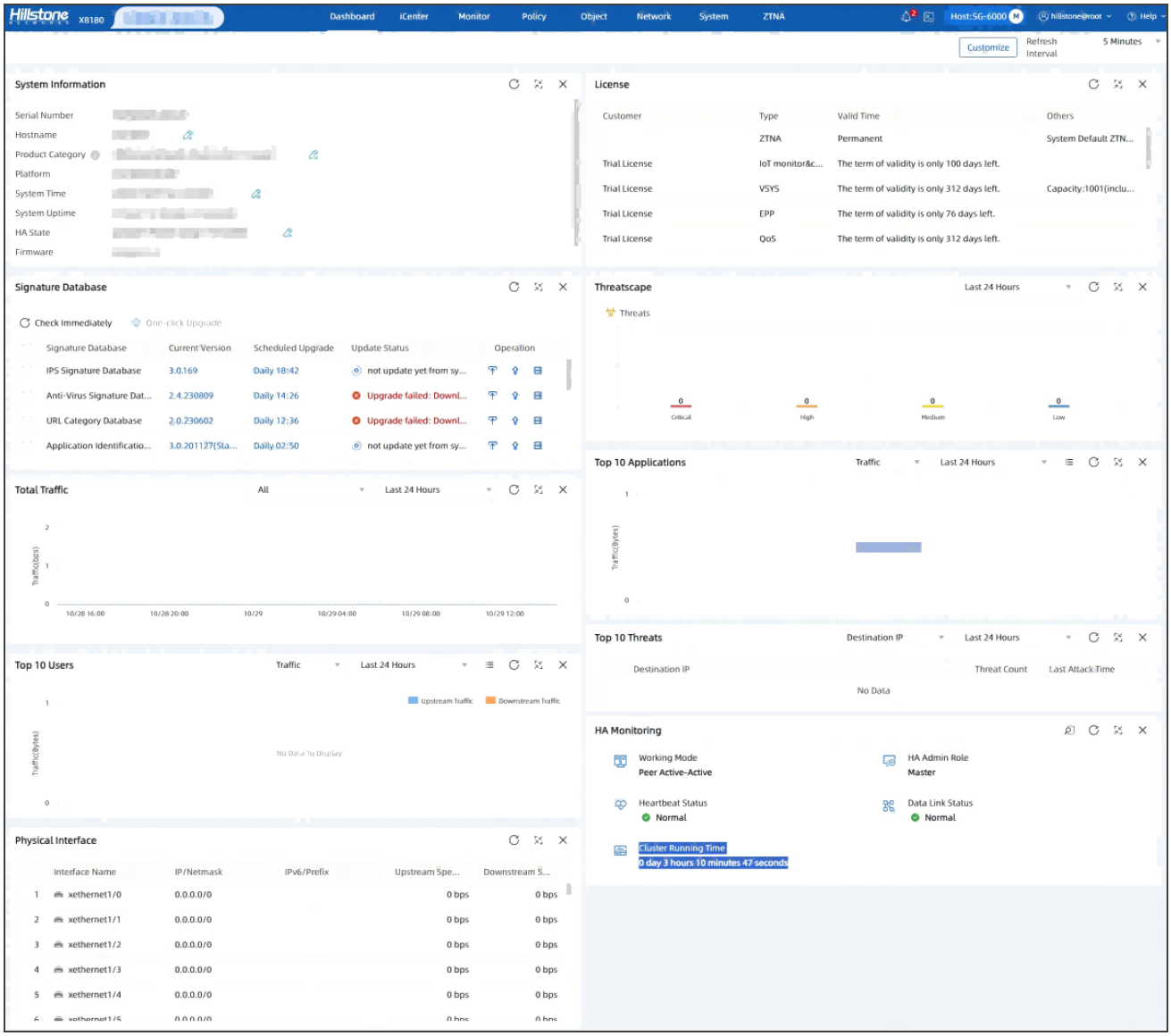
- **HA Interface Traffic Monitor:** Click HA Interface Traffic Monitor to view the historical traffic trend of the HA interface within the specified time period. For more information, see HA Interface Traffic Monitor. Note: At least one HA link interface needs to be configured; otherwise, this button will not be displayed.
- **HA Synchronize Configuration:** When the "HA Admin Role" is "Master," you can click **HA Synchronize Configuration** to perform manual synchronization. This button is not displayed in other roles.
- **HA Synchronize Session:** When the "HA Admin Role" is "Master," you can click **HA Synchronize Session** to perform manual synchronization. This button is not displayed in other roles.
- **Configuration Consistency Check:** When the "HA Admin Role" is "Master," you can click **Configuration Consistency Check** to check the configuration consistency between the master and backup immediately. If the master-backup configuration check results are inconsistent, the system will pop up a master-backup configuration comparison window. This button is not displayed in other roles.

For more information, refer to the **HA** > **HA Monitor** topic in *StoneOS WebUI User Guide*. FR 45431

Dashboard

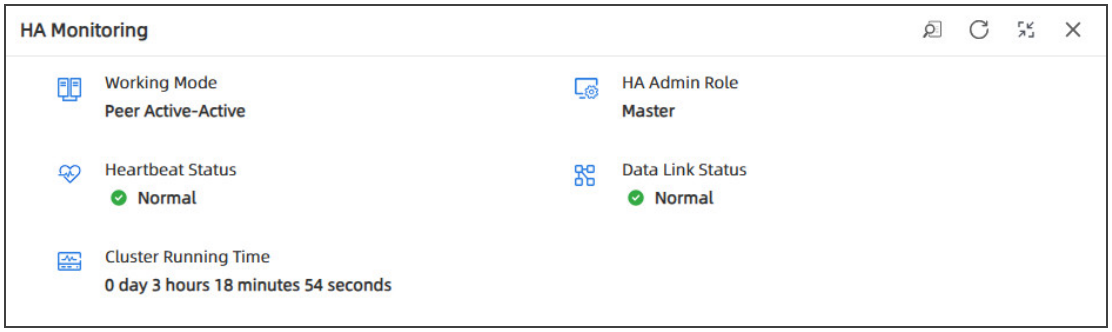
This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

The dashboard shows the system and threat information. The layout of the dashboard is shown below:



HA Monitor

Display the main information of the current HA configuration. You can click to go to the **HA Monitor** page to view detailed information about the various HA statuses in the system. The **HA Monitor** page also provides corresponding quick configuration operations.



In Standalone mode:

- Working mode: The current HA deployment mode is "Standalone."

In HA mode (Active-Passive and Peer Active-Active modes):

- Working Mode: The current HA deployment mode, which can be either "Active-Passive" or "Peer Active-Active."
- HA Admin Role: The role of the current device within the HA cluster, which can be "Master" or "Backup."
- Heartbeat Status: Monitors whether devices in the HA cluster can send and receive heartbeat messages normally.
- Data Link Status: Monitors whether the data link status of interface is normal. (This option is not displayed in the CloudEdge system)
- Cluster Running Time: The operation duration of the device when the HA function is enabled and a peer device exists.

For more information, refer to the **Dashboard** topic in *StoneOS WebUI User Guide*. FR 45431

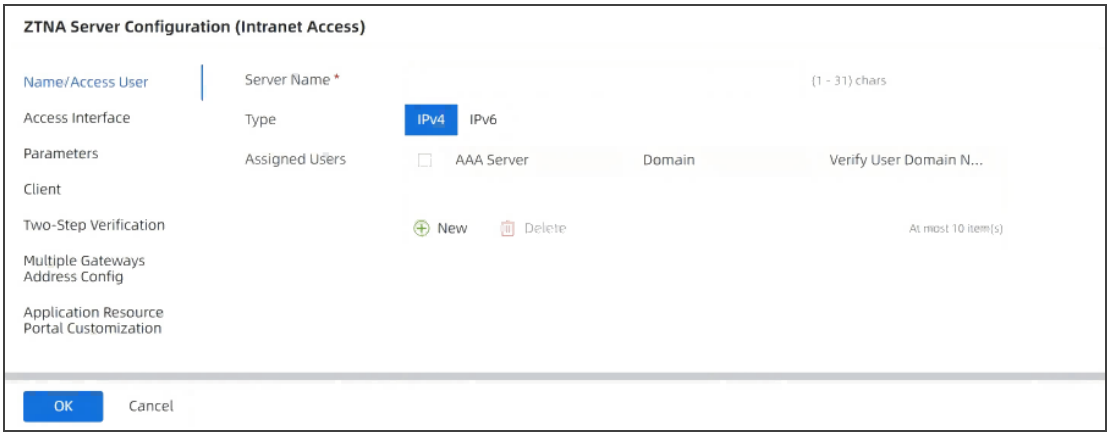
Supporting to Customize Logo and Title of the ZTNA Portal Page

WebUI

Configuring ZTNA Intranet Access

To configure ZTNA intranet access, take the following steps:

1. Select **ZTNA** > **Gateway**.
2. Click **New** > **Intranet Access**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
Server Name	Type the name of the ZTNA instance. The length is 1 to 31 characters.
Type	Select IPv4 or IPv6 to specify the service type of the ZTNA instance. The IPv6 option can only be configured when the version is IPv6.
Assigned Users (at most 10 items)	
AAA Server	Click **New** and select a AAA server from the **AAA Server** drop-down list. Or, you can click **New** in the drop-down list to create an AAA server. **Note**: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server. The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, the system will verify the user name and its domain name. **Note**: The OAuth2 server does not support user domain name verification.

In the Interface tab, configure the corresponding options.

Option	Description
Egress Interface	Specifies the interface used to listen to the request from ZTNA clients. Select the interface from the drop-down list. Or, click **New** in

Option	Description
	the drop-down list to create an interface. At most 8 interfaces can be selected.
Service Port	Specifies the ZTNA service port number. The value range is 1 to 65535.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. The option **any** indicates one of TLSv1, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If **TLSv1.2** or **any** is specified in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the TLSv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 – in oldcert.pfx – out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports TLSv1.2 protocol. **openssl pkcs12 – export – in cert.pem – out newcert.pfx – CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"**

Security Kit	
	3. Import the newly generated .pfx format certificate into your browser or USB Key.
Trust Domain	Specifies the PKI trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation. The default value is trust_domain_default.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must configure this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Client Connection	
Allow Download Client from Browser	After you enable this function, you can download the Hillstone Secure Connect client on the Web page of the browser. By default, this function is enabled. When disabled, you can only download the Hillstone Secure Connect client from the official website of Hillstone Networks. Note: The method to download the client via the browser is as follows: "https://IP-Address:Port-Number", where "IP-Address" is the IP address configured for the egress interface in the Interface tab and "Port-Number" is the service port configured here.
Forced Timeout	Specifies the time that a client stays online. After waiting for the time, the server will disconnect from the client. The value range is 10 minutes to 7 days. The default value is 7 days.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list.

Security Kit	
	When the schedule takes effect, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • ZTNA users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple login	Click **Enable** to permit a user to log in from more than one place simultaneously.
Multiple login times	Specifies the number of simultaneous login with the same user-name. The value range is 0 to 99,999,999. The value 0 indicates that the number of simultaneous login times is not limited. The default value is 0.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Specifies the ZTNA client types that are allowed to access. By default, the three types of ZTNA clients are allowed to access: Windows, macOS, Linux. You can select one or more client types as required.
Change Pass-word URL	Specifies the URL address where the user will be redirected to modify the password. The length is 0 to 255 characters.
Forgot Pass-	Specifies the URL address where the user will be redirected to

Client Configuration	
word URL	reset the password. The length is 0 to 255 characters.
Redirect URL	This function redirects the client to the specified URL address after a successful authentication. The length is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+user-name=$USER&password=$PWD, e.g., http://www.- abc.- com/oa/- login.do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+user-name=$GBUSER&password=$PWD, e.g., http://www.- 443 Chapter 7 VPN abc.- com/oa/- login.- do?user-name=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.- abc.com
Title	Specifies description for the redirect URL. The length is 0 to 31 characters. This title will appear as a client menu item.
Client Certificate Authentication	
Authentication	Enable this function to request client certificate authentication. There are two options available: "Username/Password + Digital Certificate" and "Digital Certificate only". When **Digital Certificate only** is selected:

Client Configuration	
	• System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length 0 to 63 characters.
Trust Domain	To configure the trust domain and the subject & username check function: 1. From the **Trust domain** drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the

Client Configuration	
	subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU Matching** box to determine whether matches them. 3. You can click **New** to add more items. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Enable** to enable two-step verification. It means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS authentication, token authentication or email authentication after the username and password are entered. The user must enter the random verification code received in order to log in and access intranet resources.
Type	Specifies the verification type, including **SMS Authentication**, **Token Authentication** and **Email Authentication**: • SMS Authentication: Click **SMS Modem** or **SMS Gateway** to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Click **Token Authentication** and enter the prompt message as needed. The length is 0 to 255

Option	Description
	characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Auth Type	Select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from the drop-down list. For more information about the SMS gateway, see SMS Gateway.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code, in minutes. The value range is 1 to 10. The default value is 10. If the user does not enter the SMS authentication code within the specified time and does not apply for a new code, ZTNA server will disconnect the user.
Sender Name	Specifies a message sender name to display in the message content. The length is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8.
SMS Temple	Specifies the SMS verification content. The input must contain

Option	Description
	" $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.
Sign Name	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the ALIYUNSMS.
Template Code	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the ALIYUNSMS.
Email Authentication	
Mail Server	Select an existing mail server from the drop-down list. Or, click **New** to create a mail server. For more information about the configuration of a mail server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code, in minutes. The value range is 1 to 10. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code, ZTNA server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the

Option	Description
	mail from being identified as spam, it's recommended that users configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8 . The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".

Multiple Gateways Address Config

Option	Description
When the ZTNA service is enabled for multiple devices in the network, you can add the service addresses (egress interface addresses or domain names) of these devices to the gateway address list. When the client establishes a ZTNA connection with the device, it can select the address with the best link quality from the list to establish the connection. When the device is configured with a gateway address list, the client can enable gateway detection function to select the desired ZTNA gateway for connection.	
Name	Click **New** to add a gateway address configuration in the gateway address list. Enter the gateway name. The range is 1 to 31 characters. Up to 24 gateways can be configured. When you configure multiple gateways, the ZTNA configurations on the multiple gate-

Option	Description
	ways need to be the same as those on the master ZTNA gateway.
Gateway Address	Specifies the IPv4 address or domain name of multiple gateways. The range for a domain is 255 characters and the maximum length between the two periods (.) cannot exceed 63 characters.

In the Application Resource Portal Customization tab, configure the corresponding options.

Option	Description
Title	Modifies the title of the ZTNA Portal page. Default value: ZTNA Portal. Enter a new title in the text box, which cannot exceed 63 characters in length. You can preview the change in real time in the **Preview** section below.
Logo	Modifies the logo image in the upper-left corner of the ZTNA Portal page. To do this, click **Upload** to upload a local image. You can preview the changes in real-time in the **Preview** section below. **Note**: The logo image file supports svg, webp, ico, png, jpg, jpeg formats, with a size limit of 24KB. The recommended size is 24px*24px, and it is recommended to choose a logo image with a transparent background to ensure optimal appearance after replacement.
Preview	When the Title and Logo are modified, the system will automatically update the page preview in the **Preview** section.

2. Click **OK**.

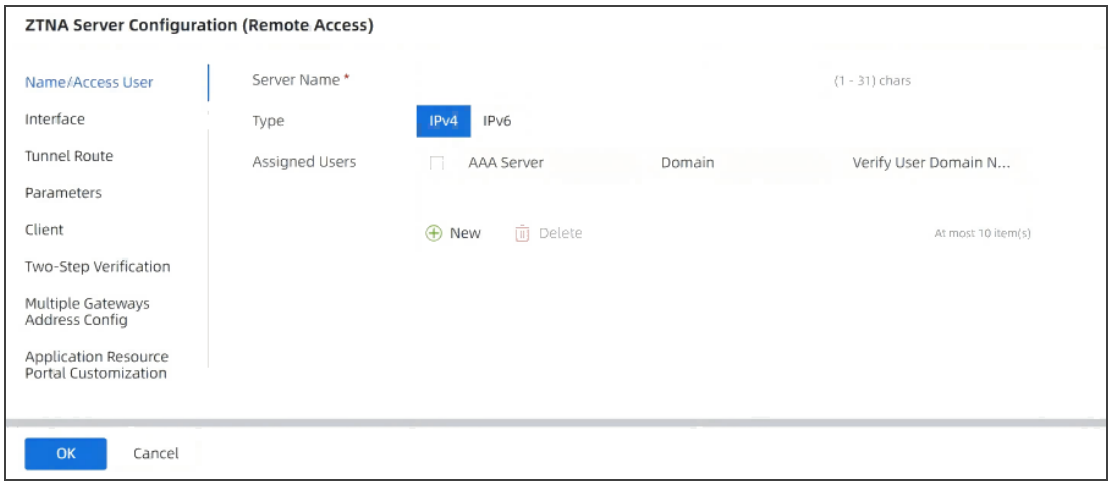
For more information, refer to the **ZTNA** > **Configuring ZTNA Gateway** topic in *StoneOS WebUI User Guide*. FR 45433

Configuring ZTNA Remote Access

To configure ZTNA remote access, take the following steps:

1. Select **ZTNA** > **Gateway**.

2. Click **New** > **Remote Access**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
Server Name	Type the name of the ZTNA instance. The length is 1 to 31 characters.
Type	Select IPv4, IPv6, or Dual Stack to specify the service type of the ZTNA instance. The IPv6 and Dual Stack options are available only when the version is IPv6. **Related Concept:**Dual stack is a network technology that allows both IPv4 and IPv6 protocol stacks to run simultaneously on a network device, enabling seamless switching and communication between IPv4 and IPv6 networks.
Assigned Users (at most 10 items)	
AAA Server	Click **New** and select a AAA server from the **AAA Server** drop-down list. Or, you can click **New** in the drop-down list to create an AAA server. If you select an OAuth2 server, the client supports OAuth2 authentication. **Note**: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server. The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, the system will verify the user name and its domain name. **Note**: The OAuth2 server does not support user domain name verification.

In the Interface tab, configure the corresponding options.

Option	Description
Egress Interface	Specifies the interface used to listen to the request from ZTNA clients. Select the interface from the drop-down list. Or, click **New** in the drop-down list to create an interface. At most 8 interfaces can be selected.
Service Port	Specifies the ZTNA service port number. The value range is 1 to 65535.
Tunnel Interface	Specifies the tunnel interface for the ZTNA instance. Select a tunnel interface from the drop-down list. Or, click **New** in the drop-down list to create a tunnel interface.
IPv4 Address Pool	Specifies the ZTNA address pool. Select an address pool from the drop-down list. Or, click **New** in the drop-down list to create a new address pool. • When configuring IPv4 ZTNA, you need to specify the IPv4 ZTNA address pool. • When configuring IPv6 ZTNA, you need to specify the IPv6 ZTNA address pool. • When configuring dual stack ZTNA, you need to specify both the IPv4 and IPv6 ZTNA address pools.
IPv6 Address Pool	

In the Tunnel Route tab, configure the following options.

Tunnel Route	
• When configuring IPv4 ZTNA, you need to specify the IPv4 tunnel route so that you can access IPv4 intranet resources. • When configuring IPv6 ZTNA, you need to specify the IPv6 tunnel route so that you can access IPv6 intranet resources. • When configuring dual stack ZTNA, you need to specify both the IPv4 and IPv6 tunnel routes so that you can access IPv4 and IPv6 intranet resources.	
A tunnel route created based on a network segment will be distributed to the ZTNA client. ZTNA client uses it to generate the route to the specified destination.	
New	Click **New** to add a route.
IP	Type the destination IP address.
Netmask	Type the netmask of the destination IP address.
Metric	Type the metric value. The value range is 1 to 9999.
Type	Sets the user type to **User Group** or **Role**.
User Group/Role	When the type is set to **User Group**, select the AAA server to which the user group belongs and the user group name from the drop-down list. Only users in this user group can access the specified network segment in the tunnel route. You can also click ⊕ and create a user group in the **User Group Configuration** panel. For more information, see Creating a User Group. When the type is set to **Role**, select the role name from the drop-down list. Only users corresponding to this role can access the specified network segment in the tunnel route. You can also click ⊕

Tunnel Route	
	and create a role in the **Role Configuration** panel. For more information, see Creating a Role.
Delete	Click **Delete** to delete the selected route.
Add Default Route	Click **Add Default Route** to add a default route with both the IP address and netmask being all 0.
Enable Dedicated ZTNA Tunnel	
Click the button to enable the dedicated ZTNA tunnel function. This way, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to ZTNA. **Notes:** • The client versions that support the dedicated ZTNA tunnel function include: the latest version of the ZTNA client for Windows, the latest version of the ZTNA client for macOS, the latest version of the ZTNA client for Linux, and the latest version of the ZTNA client for ChineseOS. • The dedicated ZTNA tunnel function cannot be used together with the domain route function. • After you enable the dedicated ZTNA tunnel function, we recommend that you do not configure a default route in the tunnel routing.	
Enable Domain Route	
After clicking the **Enable** button, the system will distribute the specified domain	

Tunnel Route	
names to the ZTNA client, and the client will generate the route to the specified destination according to the resolving results from the DNS. **Notes:** The domain route function cannot be used together with the dedicated ZTNA tunnel function.	
Maximum	Specifies the maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value range is 1 to 10000. The default value is 1000.
New	Click **New** to add the domain name to the list and you can add up to 64 domain names.
Domain	Specifies the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot. Both wildcards and a single top level domain, e.g. com and .com are not supported.
Delete	Click **Delete** to delete the selected domain name.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. The option **any** indicates one of TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If **TLSv1.2** or **any** is specified in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the TLSv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 – in oldcert.pfx – out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports TLSv1.2 protocol. **openssl pkcs12 – export – in cert.pem – out newcert.pfx – CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"**

	3. Import the newly generated .pfx format certificate into your browser or USB Key.
Trust Domain	Specifies the PKI trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation. The default value is trust_domain_default.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must configure this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the ZTNA tunnel. **NULL** indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm. The default value is AES.
Hash	Specifies the hash algorithm of the ZTNA tunnel. **NULL** indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm. The default value is MD5.
Compression	Specifies the compression algorithm of the ZTNA tunnel. By default, no compression algorithm is used.
Client Connection	
Allow Download Client from Browser	Select the check box of the client type to specify the allowed type of ZTNA client. By default, you are allowed to access the system with five types of ZTNA clients, which are ZTNA client for Windows, ZTNA client for Android, ZTNA client for iOS, ZTNA cli-

	ent for macOS, and ZTNA client for Linux. You can configure to access the system only via the specified types of ZTNA clients as needed.
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client.The value range is 1 minute to 25 hours. The default value is 30 minutes.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list. When the schedule takes effect, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • ZTNA users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple login	Click **Enable** to permit a user to log in from more than one place simultaneously.
Multiple login times	Specifies the number of simultaneous login with the same username. The value range is 0 to 99,999,999. The value 0 indicates that the number of simultaneous login times is not limited. The default value is 0.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.

DF-Bit	Specifies whether to permit packet fragmentation on the device forwarding the packets. The actions include: • Set - Forbids packet fragmentation. • Copy - Copies the DF value from the destination of the packet. It is the default value. • Clear - Permits packet fragmentation.
Port (UDP)	Specifies the UDP port number for the ZTNA connection. The value range is 1 to 65535.
Port (TCP)	Specifies the TCP port number for the ZTNA connection. The value range is 1 to 65535.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Specifies the ZTNA client types that are allowed to access. By default, the six types of ZTNA clients are allowed to access: Windows, macOS, Linux, ChineseOS, iOS, and Android. You can select one or more client types as required.
Change Password URL	Specifies the URL address where the user will be redirected to modify the password. The length is 0 to 255 characters.
Forgot Password URL	Specifies the URL address where the user will be redirected to reset the password. The length is 0 to 255 characters.
Redirect URL	This function redirects the client to the specified URL address after a successful authentication. The length is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding

	fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.- abc.- com/oa/- login.- do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+user-name=$GBUSER&password=$PWD, e.g., http://www.- 443 Chapter 7 VPN abc.- com/oa/- login.- do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.abc.com
Title	Specifies description for the redirect URL. The length is 0 to 31 characters. This title will appear as a client menu item.
Client Certificate Authentication	
Authentication	Enable this function to request client certificate authentication. There are two options available: • Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username and password. The USB Key certificate users also need to type the USB Key password. • Digital Certificate only - To pass the authentication,

	you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificate users also need to type the USB Key password. No username or user's password is required. When **Digital Certificate only** is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length 0 to 63 characters.
Trust Domain Subject&Username Checking CN Matching OU Matching	To configure the trust domain and the subject & username check function: 1. From the **Trust domain** drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed.

	2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU Matching** box to determine whether matches them. 3. You can click **New** to add more items. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Enable** to enable two-step verification. It means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS authentication, token authentication or email authentication after the username and password are entered. The user must enter the random verification code received in order to log in and access intranet resources.
Type	Specifies the verification type, including **SMS Authentication**, **Token Authentication** and **Email Authentication**: • SMS Authentication: Click **SMS Modem** or **SMS Gateway**

Option	Description
	to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Click **Token Authentication** and enter the prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Auth Type	Select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from the drop-down list. For more information about the SMS gateway, see SMS Gateway.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code, in minutes. The value range is 1 to 10. The default value is 10. If the user does not enter the SMS authentication code within the specified time and does not apply for a new code, ZTNA server will disconnect the user.
Sender Name	Specifies a message sender name to display in the message content. The length is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.

Option	Description
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8.
SMS Temple	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.
Sign Name	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the ALIYUNSMS.
Template Code	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the ALIYUNSMS.
Email Authentication	
Mail Server	Select an existing mail server from the drop-down list. Or, click **New** to create a mail server. For more information about the configuration of a mail server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code, in minutes. The value range is 1 to 10. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code,

Option	Description
	ZTNA server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8 . The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".
Multiple Gateways Address Config	
When the ZTNA service is enabled for multiple devices in the network, you can add the service addresses (egress interface addresses or domain names) of these devices to the gateway address list. When the client establishes a ZTNA connection with the device, it can select the address with the best link quality from the list to establish the connection. When the device is configured with a gateway address list, the client can enable gateway detection function to select the desired ZTNA gateway for connection.	
Name	Click **New** to add a gateway address configuration in the gateway address list. Enter the gateway name. The range is 1 to 31 char-

Option	Description
	acters. Up to 24 gateways can be configured. When you configure multiple gateways, the ZTNA configurations on the multiple gateways need to be the same as those on the master ZTNA gateway.
Gateway Address	Specifies the IPv4 address, IPv6 address, or domain name of multiple gateways. The range for a domain is 255 characters and the maximum length between the two periods (.) cannot exceed 63 characters.

In the Application Resource Portal Customization tab, configure the corresponding options.

Option	Description
Title	Modifies the title of the ZTNA Portal page. Default value: ZTNA Portal. Enter a new title in the text box, which cannot exceed 63 characters in length. You can preview the change in real time in the **Preview** section below.
Logo	Modifies the logo image in the upper-left corner of the ZTNA Portal page. To do this, click **Upload** to upload a local image. You can preview the changes in real-time in the **Preview** section below. **Note**: The logo image file supports svg, webp, ico, png, jpg, jpeg formats, with a size limit of 24KB. The recommended size is 24px*24px, and it is recommended to choose a logo image with a transparent background to ensure optimal appearance after replacement.
Preview	When the Title and Logo are modified, the system will automatically update the page preview in the **Preview** section.

2. Click **OK** to save the settings.

For more information, refer to the **ZTNA > Configuring ZTNA Gateway** topic in *StoneOS WebUI User Guide*. FR 45433

CLI

Configuring ZTNA Instance

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

tunnel ztna*instance-name* [**intranet** | **remote**]

- *instance-name* - Specifies a name for the ZTNA instance. The length is 1 to 31 characters.
- **intranet** | **remote** - Specifies the ZTNA instance type, which can be **intranet** or **remote**. By default, **remote** is selected.

This command creates a ZTNA instance with the specified name and leads you into the corresponding ZTNA instance configuration mode, including intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode; if the instance exists, you will enter this ZTNA instance configuration mode directly.

To delete a ZTNA instance, in the ZTNA instance configuration mode, use the following command:

no tunnel ztna *instance-name* {**intranet** | **remote**}

Notes: The number of ZTNA gateways that can be created varies based on different platforms.

In intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, you can configure the following:

- Enabling/Disabling ZTNA Instance
- Specifying the Service Type

- Specifying an Access Address Pool (applicable only to remote access ZTNA instance)
- Specifying a Server Interface
- Specifying an SSL Protocol Version
- Specifying a PKI Trust Domain
- Specifying an Encryption Trust Domain
- Specifying the Tunnel Cipher Suite (applicable only to remote access ZTNA instance)
- Specifying an AAA Server
- Specifying an SSL Port Number
- Specifying the Transport Protocol (applicable only to remote access ZTNA instance)
- Configuring a ZTNA Tunnel Route (applicable only to remote access ZTNA instance)
- Configuring Anti-Replay (applicable only to remote access ZTNA instance)
- Configuring Packet Fragmentation (applicable only to remote access ZTNA instance)
- Configuring Forced Timeout (applicable only to intranet access ZTNA instance)
- Configuring Idle Time (applicable only to remote access ZTNA instance)
- Configuring forced logoff schedule
- Configuring Multi-logon
- Configuring Multi-Gateway Address
- Configuring URL Redirection
- Enabling/Disabling the Browser Download Function

- Binding Remote Access ZTNA Instance to a Tunnel Interface (applicable only to remote access ZTNA instance)
- Authentication with USB Key Certificate
- Configuring the Title of the ZTNA Portal Page

.....

Configuring the Title of the ZTNA Portal Page

The system supports to customize the title of the ZTNA Portal page. To do this, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

resource-portal title*title-name*

- *title-name* - Specifies the title of the ZTNA Portal page, which is "ZTNA Portal" by default. The title cannot exceed 63 characters in length.

For more information, refer to the **ZTNA > Configuring ZTNA Service > Configuring ZTNA Instance** topic in *StoneOS CLI User Guide*. FR 45433

Supporting to Configure the LACP Working Mode of Interface

WebUI

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network > Interface**.
2. Select the interface you want to edit from the interface list and click **Edit**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the interface.
Description	Enter descriptions for the interface.
Binding Zone	Specifies the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. You can also specify the firewall information (firewall's IPv4 or IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP mode and this interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone

Option	Description
	with this interface bound, and the action of the share access rule is Block; • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the end point profile that referenced by the security policy is Block; • The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, you should also select an aggregate interface/redundant interface: • Aggregate Interface: The interface you specified belongs to a aggregate interface. • Interface: Choose an aggregate interface which the aggregate interface belongs to from Interface drop-down list. • Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.

Option	Description
	• Port LACP working mode: Specifies the LACP working mode of the port, which includes active and passive modes. In active mode, the interface actively sends LACPDU to attempt forming an LACP connection. That is, the interface actively tries to negotiate LACP with the peer device and sends LACPDU to establish a link aggregation group. This mode is the default LACP working mode for the interface. In passive mode, the interface can respond to LACP negotiation but does not actively send LACPDU. Instead, it waits for the peer device to initiate an LACP negotiation request. If the peer device is in active mode and sends LACPDU, the device in passive mode will respond to the request and negotiate LACP with the peer device, eventually establishing a link aggregation group. **Notes:** We recommend that you check the LACP working mode of interfaces on both ends after configuration. If the interfaces on both devices are in passive mode, neither will actively send LACPDU, making it impossible to initiate LACP nego-

Option	Description
	tiation and thus unable to establish a link aggregation group. • Port timeout mode: The LACP timeout refers to the time interval for the members The system supports **Fast** (1 second) and **Slow** (30 seconds, the default value) waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. • Redundant Interface: This interface belongs to a redundant interface. Select that redundant interface from the Interface drop-down list. • None: This interface does not belong to any object.
Aggregate mode	• Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally. • Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are: • System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is

Option	Description
	32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be. • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby. • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see DHCP.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced:

Option	Description
	• Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, the function of obtaining the server MTU is enabled for the interface eth0/0 of CloudEdge. For other interfaces, this function is disabled.

DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.

Password: Specifies PPPoE user's password.

Confirm Password: Enter the password again to confirm.

Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.</td></tr>
</table>

Option	Description	
	Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.	
	Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.	
	Advanced	Access concentrator: Specifies a name for the concentrator.
		Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.
		Netmask: Specifies a netmask for the IP address obtained via PPPoE.
		Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.
		Service: Specifies allowed service. The specified service must be the same with that provided by the

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see DDNS.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td colspan="2">WebAuth</td></tr>
<tr><td>Auth Service</td><td>Click the Enable， Close or Global Default radio button as needed.
Enable：Enable the WebAuth function of the specified interface.
Close：Disable the WebAuth function of the specified interface.
Global Default：Specify that the interface uses the global</td></tr>
</table>

Option	Description
	default configuration of WebAuth. For the global default configuration of WebAuth function, see Web Authentication.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the

Option	Description
	WebAuth domain name.

4. Expand IPv6 Configuration, configure the following.

5. Expand Interface Properties, configure properties for the interface.

Property	Description
Duplex	Specifies a duplex working mode for the interface. Options include auto, full duplex and half duplex. Auto is the default working mode, in which system will select the most appropriate duplex working mode automatically. 1000M half duplex is not supported.
Rate	Specifies a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported. For 1GE(SFP) optical port of certain A-series devices, you can set the data rate to 100 Mbps or 1,000 Mbps. The default data rate is 1000 Mbps. When you set the data rate to 100 Mbps, the optical port can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers. **Note**: Only the following devices allow you to backward switch the data rate of 1GE(SFP) optical port: SG-6000-A5500, A5200, A5100, A3800, A3700, A3600, A3000, A2800, and A2700.
Channel-Speed	Converts the data rate of 10GE (SFP+) optical interfaces. • 1G: Convert the data rate of 10GE (SFP+) optical interfaces from 10Gbps to 1Gbps.

Property	Description
	• Close: Do not convert the data rate of the 10GE (SFP+) optical interface, which is 10Gbps by default.
Optical Interface to Electrical Interface	This option applies to the X8180 devices' 10GE (SFP+) optical port, and by default, Optical Interface to Electrical Interface function is disabled. To enable this function, take the following steps: 1. Insert a copper SFP module. 2. Channel-Speed option is configured to "1G". 3. Click the **Enable** button, convert optical port to electrical port.
Combo type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, and the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: • Auto: The above default scenario. • Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this

Property	Description
	option configured, the device will migrate the traffic on the copper port to the fiber port automatically without reboot.
MTU	The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive

Property	Description
	packets.
MAC clone	System clones a MAC address to the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will retore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. Note: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Band-	Specifies the maximum value of the down bandwidth of the inter-

Property	Description
width	face.

6. Expand Advanced Configuration, configure advanced options for the interface.
7. Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface.
8. Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface.
9. Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface.
10. Click **OK**.

Notes:

- Before deleting an aggregate/redundant interface, you must cancel other interfaces' bindings to it, aggregate/redundant sub-interface's configuration, its IP address configuration and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.
- When a VSwitch interface is deleted, the corresponding VSwitch will be deleted as well.
- The HA interface can not bind the track object.

For more information, refer to the **Network** > **Interface** > **Configuring an Interface** topic in *StoneOS WebUI User Guide*. FR 45435

CLI

Link Aggregation

Link aggregation combines multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails.

The device supports forced link aggregation and LACP (Link Aggregation Control Protocol). The forced link aggregation is implemented by the aggregate interface. For more information, see Configuring an Aggregate Interface. This section mainly describes the usage of LACP.

LACP

LACP (Link Aggregation Control Protocol) is designed to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that is also enabled with LACP).

Hillstone devices use the aggregate interface to implement the LACP function. The aggregate interface with LACP enabled is named as aggregate group, and the physical interfaces in the aggregate group is the member of the aggregate group. After enabling LACP on an aggregate interface, the member interface sends the LACPDU packets to the peer to notify its system priority, system MAC address, port priority, port number, and operating key. The peer receives the LACPDU and compare the information with the local information to select a proper member interface, thus the both sides can decide which link will be used to transfer data.

Member Status in an Aggregate Group

There are four statuses for the member interfaces in an aggregate group:

- Unselected: The interface is selected by the aggregate group and cannot forward traffic. This status is usually caused by physical reasons, e.g., the interface mode is non-duplex, rates of both sides are inconsistent, physical connection failure, etc.

- Selected: The interface is in aggregate group, but its peer is not ready, so the interface cannot forward traffic. When it receives LACPDU packets from the peer, and learns the status of its peer is Selected, the status of the interface will switch to Active. The interface in Active status can forward traffic.
- Standby: The interface is a backup interface, and cannot forward traffic. If the LACP priority of the interface is promoted, the interface will replace the existing Selected interface and change its own status to Selected, and the status of the replaced interface will switch to Standby. When other interfaces become Unselected, the Standby interface will change to Selected interface automatically.
- Active: The interface is aggregated successfully and forwards traffic. If the interface has not received LACPDU packets from the peer in three LACPDU timeouts, it will be concluded as link down. In such a case, the status of the interface will switch to Selected, and the interface will stop forwarding traffic.

LACP Working Mode of Interface

LACP working mode is divided into active mode and passive mode.

- **Active Mode:** In active mode, the interface actively sends LACPDU to attempt forming an LACP connection. That is, the interface actively tries to negotiate LACP with the peer device and sends LACPDU to establish a link aggregation group. This mode is the default LACP working mode for the interface.
- **Passive Mode:** In passive mode, the interface can respond to LACP negotiation but does not actively send LACPDU. Instead, it waits for the peer device to initiate an LACP negotiation request. If the peer device is in active mode and sends LACPDU, the device in passive mode will respond to the request and negotiate LACP with the peer device, eventually establishing a link aggregation group.

Notes: If the interfaces on both devices are in passive mode, neither will actively send LACPDU, making it impossible to initiate LACP negotiation and thus unable to establish a link aggregation group.

For more information, refer to the **Firewall** > **Interface** > **Link Aggregation** topic in *StoneOS CLI User Guide*. FR 45435

Configuring LACP

The configurations of LACP include:

- Enabling/Disabling LACP
- Specifying LACP System Priority
- Specifying Interface LACP Priority
- Specifying Interface LACP Working Mode
- Specifying LACP Timeout
- Specifying the Maximum Active Links
- Specifying the Minimum Active Links
- Specifying Load Balance Mode

Enabling/Disabling LACP

LACP can be enabled on the aggregate interfaces (aggregate sub-interface, aggregate virtual forward interface do not support LACP). To enable/disable LACP, in the aggregate interface configuration mode, use the following commands:

- Enable: **lacp enable**
- Disable: **no lacp enable**

Specifying LACP System Priority

LACP system priority is used to determine the priority between devices in both sides. The interface with higher LACP system priority will be defined as the standard selected interface. The smaller the number is, the higher the priority will be. If both sides have the same LACP system priority, the system will choose the interface with smaller MAC address to be the standard selected interface.

To configure the LACP system priority, in the aggregate interface configuration mode, use the following command:

lacp system-priority*value*

- *value* – Specifies the LACP system priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default LACP system priority, in the aggregate interface configuration mode, use the following command:

no lacp system-priority

Specifying Interface LACP Priority

Interface LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority.

To configure the interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

lacp port-priority*value*

- *value* – Specifies the interface LACP priority. The value range is 1 to 32768. The default value is 32768.

To restore to the default interface LACP priority, in the configuration mode of the interface in the aggregate group, use the following command:

no lacp port-priority

Specifying LACP Working Mode of Interface

LACP working mode is divided into active mode and passive mode.

In active mode, the interface actively sends LACPDU to attempt forming an LACP connection. That is, the interface actively tries to negotiate LACP with the peer device and sends LACPDU to establish a link aggregation group. In passive mode, the interface can respond to LACP negotiation but does not actively send LACPDU. Instead, it waits for the peer device to initiate an LACP negotiation request. If the peer device is in active mode and sends LACPDU, the device in passive mode will respond to the request and negotiate LACP with the peer device, eventually establishing a link aggregation group.

To specify the LACP working mode of member interface, in interface configuration mode of physical interface that is added to the aggregate interface, use the following command:

lacp mode {**active** | **passive**}

- **active** – Specifies the LACP working mode of interface as the active mode. This is the default mode.
- **passive** – Specifies the LACP working mode of interface as the passive mode.

Notes: We recommend that you check the LACP working mode of interfaces on both ends after configuration. If the interfaces on both devices are in passive mode, neither will actively send LACPDU, making it impossible to initiate LACP negotiation and thus unable to establish a link aggregation group.

.....

For more information, refer to the **Firewall** > **Interface** > **Link Aggregation** topic in *StoneOS CLI User Guide*. FR 45435

Supporting to Set Categories for Application Resources

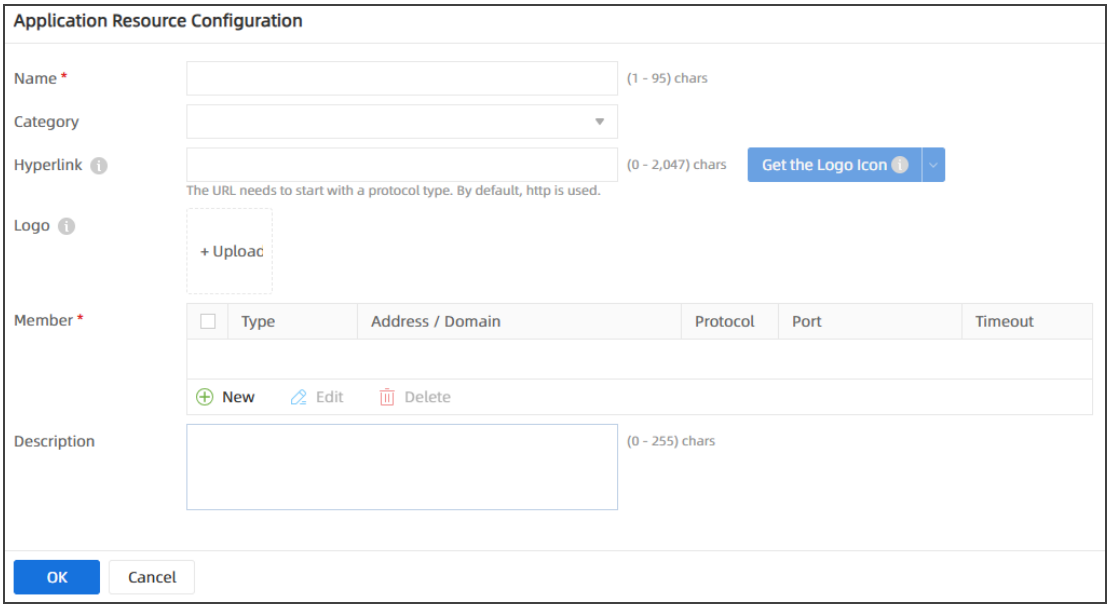
WebUI

Configuring an Application Resource

To configure an application resource, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource**. Or select **ZTNA** > **Application Resource Book** > **Application Resource**.

2. Click **New**.



Option	Description
Name	Type the name of the application resource. The length is 1 to 95 characters.
Category	Select the category to which the application resource belongs from the drop-down list. The ZTNA Portal page will display the application resource based on the selected category. You can also click

Option	Description
	⊕ to create a category. For more information, see Creating an Application Resource Category.
Hyperlink	Type the hyperlink of the application resource. The length is 0 to 2047 characters. On the ZTNA portal displayed after a user logs in, the user can copy the hyperlink to access an application resource in a browser if the application resource is configured with an hyper-link; or, the user can directly click the application resource icon to access it (make sure the link work). An application resource without a hyperlink configured will not be displayed on the ZTNA portal. If the specified hyperlink does not contain the protocol type, the default HTTP protocol will be used. **Get the Logo Icon**: After a URL is configured, click this button. The system will automatically obtain the logo image corresponding to this URL. If no logo image can be obtained, the "The LOGO Icon is not found" prompt will appear. You can click ⌄ to select a virtual router to which the URL belongs from the drop-down list.
Logo	Specifies the logo of the application resource, which is used to be displayed on the ZTNA Portal page. To do this, click **Upload** and select an authentication logo from your PC. The logo needs to be in the svg, ico, png, jpg, or jepg format, which cannot exceed 24 KB in size. Note: If you do not upload the logo of the application resource or automatically obtain the logo by configuring a URL, a default logo generated based on the first character of the application resource

Option	Description
	name is displayed in the application resource list and on the ZTNA Portal page.
Member	Click **New** to add a resource entry and configure the options. Each application resource can contain up to 16 entries. • Type: Specify the address type of the resource entry, including IPv4/Netmask, IPv6/Prefix, IPv4 Range and IPv6 Range and Domain. • Address: Specify the IP address or IP range of the resource entry. • Protocol: Specify the protocol type of the resource entry. TCP and UDP are supported for application resources defined based on IP address. HTTP and HTTPS are supported for application resources defined based on domain name. • Port: Specify the port number or port range of the resource entry. If you specify a port number, the minimum port number and the maximum port number need to be the same. The value ranges from 1 to 65535. • Timeout: Specify the timeout value in seconds or days. The value range is 1 to 65535 when it is expressed in seconds and 1 to 1000 when in days. The default value is 1800s when the protocol is TCP, HTTP or HTTPS, and 60s when UDP.
Description	Type description for the application resource. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.

4. On the Application Resource page, by clicking the "+" button in the list to unfold an application resource, you can view more details about it, including the group it belongs to and the ZTNA policy ID that is bound to it.

Application Resource Category

As the number of application resources increases, you may find it inconvenient to locate specific application resources on the ZTNA Portal page. To enhance user experience and operation convenience, the system supports to group application resources by category. Grouping application resources by category not only allows you to locate desired resources more efficiently but also makes the ZTNA Portal page appear more organized and orderly.

The configuration for application resource category includes:

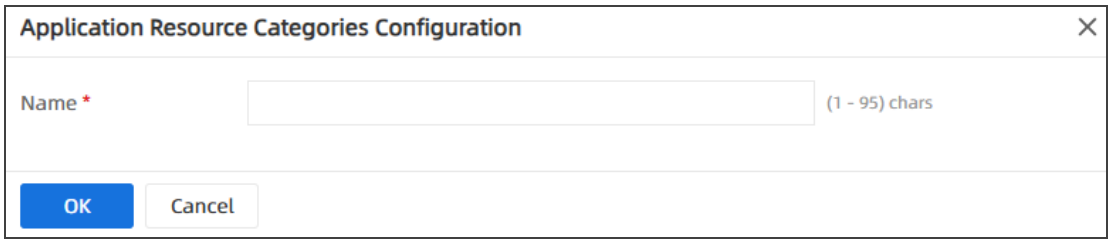
- Configuring an Application Resource Category
- Setting a Category for Application Resource

Configuring an Application Resource Category

To configure an application resource category, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource**. Or select **ZTNA** > **Application Resource Book** > **Application Resource**.

2. Click **Category Management** in the upper-right corner. In the **Application Resource Categories** panel, click **New**. In the **Application Resource Categories Configuration** panel, enter the category name in the **Name** text box, which needs to be 1 to 95 characters in length.



3. Click **OK**.

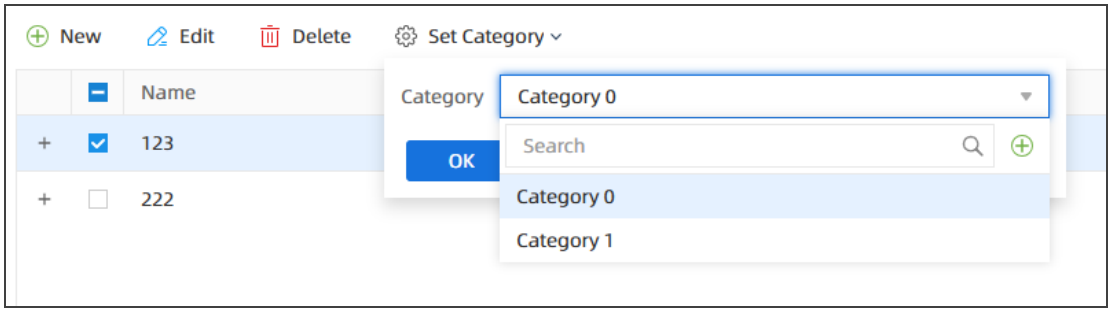
4. In the **Application Resource Categories** panel, you can view the number of application resources under each category. When you click the number, a filter condition will be added to the application resource list to display only resources within this category. You can also click or to modify or delete an existing category.

Notes: Categories in use by application resources cannot be deleted.

Setting a Category for Application Resource

1. Select **Object** > **Application Resource Book** > **Application Resource**. Or select **ZTNA** > **Application Resource Book** > **Application Resource**.

2. Select the application resource for which you want to set a category and click Set Category above the list. From the drop-down list, select a category for the selected application resource. You can also click to create a category. For more information, see Creating an Application Resource Category.



3. Click **OK**.

For more information, refer to the **Object** > **Application Resource/Application Resource Group** topic in *StoneOS WebUI User Guide*. FR 45437

CLI

Configuring an Application Resource Category

As the number of application resources increases, you may find it inconvenient to locate specific application resources on the ZTNA Portal page. To enhance user experience and operation convenience, the system supports to group application resources by category. Grouping application resources by category not only allows you to locate desired resources more efficiently but also makes the ZTNA Portal page appear more organized and orderly.

The configuration for application resource category includes:

- Creating an Application Resource Category
- Renaming the Application Resource Category
- Setting a Category for Application Resource
- Viewing Configuration Information about an Application Resource Category

Creating an Application Resource Category

To create an application resource category, in global configuration mode, use the following command:

application-resource-category*category-name*

- *category-name* - Specifies the name of the application resource type, which is not case-sensitive and needs to be 1 to 95 characters in length.

To delete the specified application resource category, in global configuration mode, use the following command:

no application-resource-category*category-name*

Renaming the Application Resource Category

To rename the application resource category, in global configuration mode, use the following command:

rename application-resource-category*original-category-name**new-category-name*

- *original-category-name* - Specifies the original name of the application resource category.
- *new-category-name* - Specifies the name of the application resource category, which is not case-sensitive and needs to be 1 to 95 characters in length.

Setting a Category for Application Resource

To set a category for application resource, in application resource configuration mode, use the following command:

category *category-name*

- *category-name* - Specifies the category name of application resource.

To delete the category for application resource, in application resource configuration mode, use the following command:

no category

Viewing Configuration Information about an Application Resource Category

To view configuration information about an application resource category, in any mode, use the following command:

show application-resource-category [**name***category-name*]

- **name***category-name* - Specifies the name of the application resource category whose configuration information you want to view. If not specified, the configuration information of all application resource categories will be displayed.

Sample response:

```
hostname#show application-resource-category
Total count: 4
```

```
==========================================================-
============
Name App-Resource-Count
-------------------------------------------------------------------------------
Category0 1
Category1 2
Category2 3
==========================================================-
============
hostname#show application-resource-category nameCategory0
Name: Category0
Application resource count: 1
|_appres1
```

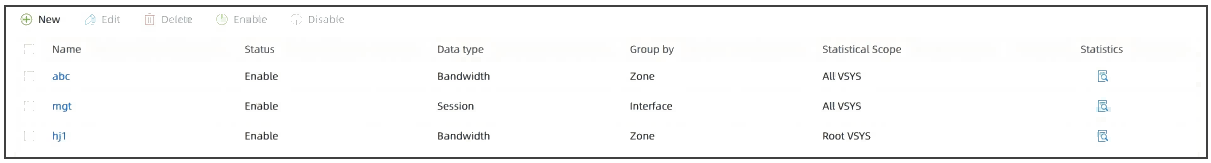
For more information, refer to the **ZTNA > Configuring Application Resource/Application Resource Group** topic in *StoneOS CLI User Guide*. FR 45437

Optimizing the WebUI of the Custom Monitor Function

WebUI

Configuring User-defined Monitor

A user-defined stat-set provides a more flexible approach to view the statistics. You can view the statistics as needed. Click **Monitor>User-defined Monitor**.



- Click **New**. For more information, see Creating a User-defined Stat-set.
- Click the name of a monitor stat-set to view configuration details about it.
- Click  in the **Statistics** column to view user-defined stat-set statistics.

Creating a User-defined Stat-set

To create a user-defined stat-set, take the following steps:

1. Click **Monitor > User Defined Monitor**.
2. Click **New**.

Option	Description
Name	Type the name for the stat-set into the Name box.
Data Type	Select an appropriate data type from the Data type list.
Group by	Select an appropriate grouping method from the Group by list.
Statistical Scope	Specifies the statistical scope of user-defined monitor, which includes **All VSYS** and **Root VSYS**. This option will take effect when the data type is Traffic, Session, Ramp-up rate, or URL hit. If the data grouping method is configured to VSYS, this option will be unavailable.
Advanced Configuration	To configure a filtering condition, expand Advanced Configuration. In the Advanced Configuration page, select a filter condition from the Type drop-down list. For more details about this option, see The_filtering_conditions_supported_table.

3. Click **OK** to save your settings . The configured stat-set will be displayed .

Notes: You need to pay attention to the following when configure a stat-set.

- If the Data type is Traffic, Session, Ramp-up rate, Virus attack count, Intrusion count or URL hit count, then the Filter should not be Attack log.
- If the Data type is URL hit count, then the Filter should not be Service.
- System will hide unavailable options automatically.

Viewing User-defined Monitor Statistics

To view user-defined monitor statistics, in the user-defined monitor stat set list, click  in the **Statistics** column to view its statistics.

- Displays the top 10 statistical result from multiple aspects in forms of bar chart.
- Click the **Monitor Name** drop-down list in the upper-left corner to quickly switch and display statistical results for different monitor stat sets.
- View specified historic statistics by selecting a period from the statistic period drop-down list.
- Click **All Data** to view all the statistical result from multiple aspects in forms of list, trend. Click **TOP 10** returns bar chart.

For more information, refer to the **Monitor** > **User-defined Monitor** topic in *StoneOS WebUI User Guide*. FR 45439

Supporting to Configure Multiple ZTNA Instances

WebUI

Configuring ZTNA Gateway

This topic consists of the following sections:

- Configuring ZTNA Remote Access
- Configuring ZTNA Intranet Access
- Enabling/Disabling ZTNA Instance

Notes: The number of ZTNA gateways that can be created varies based on different platforms.

Enabling/Disabling ZTNA Instance

When a ZTNA instance is enabled and fully configured, the client can connect normally. If a client is already connected to ZTNA, when the ZTNA instance is disabled, the connected client users will be disconnected.

To enable/disable a ZTNA instance, take the following steps:

1. Select **ZTNA** > **Gateway**.
2. Select the ZTNA instance from the list that you want to enable or disable.
3. Click **Enable** or **Disable** at the top of the list to enable or disable the ZTNA instance. When the instance is enabled and fully configured, its "Status" in the ZTNA list will be displayed as

. If the instance is enabled but not fully configured, its "Status" in the ZTNA list will be displayed as .

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Configuring ZTNA Gateway** topic in *StoneOS WebUI User Guide*. FR 36857

Monitor

Select **ZTNA** > **Monitor** > **Summary** to enter the ZTNA monitor page.

……

Viewing and Managing Online Users

To manage and view the status information of all ZTNA online users, take the following steps:

1. Select **ZTNA** > **Monitor** > **User Status**.
    a. Login Time: indicates the login time of the online user;
    b. User Name: indicates the user name of the online user;
    c. AAA Server: indicates the AAA server name to which the online user belongs;
    d. ZTNA Server: indicates the ZTNA service name that the online user accesses;
    e. User IP(v4): indicates the IPv4 address of the online user that the ZTNA server assigns;
    f. User IP(v6): indicates the IPv6 address of the online user that the ZTNA server assigns;
    g. Endpoint Name: indicates the user endpoint name;
    h. Endpoint IP: indicates the user endpoint IP address, i.e. the public IP address of the user;
    i. OS: indicates the operating system of the user endpoint;
    j. Endpoint Tag: indicates the endpoint tag associated with the online user;

k. Client Version Number: indicates that the version number of the ZTNA client used by the online user.

l. Allowed Application Resources: indicates the application resources that the online user is granted access;

m. Denied Application Resources: indicates the application resources that the online user is not granted access;

n. Upstream Speed: indicates the upstream speed of the online user;

o. Downstream Speed: indicates the downstream speed of the online user.

2. Click **Filter** to add filter conditions to view the detailed information of ZTNA online users that meet the filter conditions.

3. By selecting one or more users and clicking **Force Log Off**, you can force disconnecting a user with the ZTNA server.

Note: To view upstream and downstream speed statistics, make sure the ZTNA monitor function is enabled.

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Monitor** topic in *StoneOS WebUI User Guide*. FR 36857

CLI

Configuring ZTNA Instance

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

tunnel ztna*instance-name* [**intranet** | **remote**]

- *instance-name* - Specifies a name for the ZTNA instance. The length is 1 to 31 characters.
- **intranet** | **remote** - Specifies the ZTNA instance type, which can be **intranet** or **remote**. By default, **remote** is selected.

This command creates a ZTNA instance with the specified name and leads you into the corresponding ZTNA instance configuration mode, including intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode; if the instance exists, you will enter this ZTNA instance configuration mode directly.

To delete a ZTNA instance, in the ZTNA instance configuration mode, use the following command:

no tunnel ztna *instance-name* {**intranet** | **remote**}

Notes: The number of ZTNA gateways that can be created varies based on different platforms.

In intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, you can configure the following:

- Enabling/Disabling ZTNA Instance
- Specifying the Service Type
- Specifying an Access Address Pool (applicable only to remote access ZTNA instance)
- Specifying a Server Interface
- Specifying an SSL Protocol Version
- Specifying a PKI Trust Domain
- Specifying an Encryption Trust Domain
- Specifying the Tunnel Cipher Suite (applicable only to remote access ZTNA instance)
- Specifying an AAA Server

- Specifying an SSL Port Number
- Specifying the Transport Protocol (applicable only to remote access ZTNA instance)
- Configuring a ZTNA Tunnel Route (applicable only to remote access ZTNA instance)
- Configuring Anti-Replay (applicable only to remote access ZTNA instance)
- Configuring Packet Fragmentation (applicable only to remote access ZTNA instance)
- Configuring Forced Timeout (applicable only to intranet access ZTNA instance)
- Configuring Idle Time (applicable only to remote access ZTNA instance)
- Configuring forced logoff schedule
- Configuring Multi-logon
- Configuring Multi-Gateway Address
- Configuring URL Redirection
- Enabling/Disabling the Browser Download Function
- Binding Remote Access ZTNA Instance to a Tunnel Interface (applicable only to remote access ZTNA instance)
- Authentication with USB Key Certificate

Enabling/Disabling ZTNA Instance

When a ZTNA instance is enabled and fully configured, the client can connect normally. If a client is already connected to ZTNA, when the ZTNA instance is disabled, the connected client users will be disconnected.

To enable or disable a ZTNA instance, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

Enable: **enable**

Disable: **disable**

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Configuring ZTNA Service** > **Configuring ZTNA Instance** topic in *StoneOS CLI User Guide*. FR 36857

Supporting to Export NAT444 Logs (only User Allocation Port Log and User Release Port Log) to the IPFIX Server

WebUI

Log

……

Destination of Exported Logs

Log messages can be sent to the following destinations:

- Console - The default output destination. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.
- File - By default, the logs are sent to the specified USB destination in form of a file.
- Syslog Server - Includes Syslog server and and IPFIX server. The system can send all types of logs to UNIX or Windows Syslog Server; or send NAT444 logs (only user allocation port logs and user release port logs) to the IPFIX server.
- Email - Sends logs to a specified email account.
- Local database - Sends logs to the local database of the device.

Log Configuration

You can create Syslog server, set up log email address, add IPFIX servers and configure sending sourceport.

Configuring a Syslog Server

In the **Syslog Server Configuration** tab, you can create, edit, or delete the Syslog server that is used for receiving logs. In addition, you can configure the sending sourceport number and log encoding.

Creating a Syslog Server

To create a Syslog server, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **Syslog Server Configuration** tab.
3. Click **New**.

Option	Description
Name	Specifies the name of the Syslog server, which needs to be 1 to 127 characters in length.
Hostname	Specifies the IP address or host name of the Syslog server.
Log Format	Specifies the log format of Syslog Server log server, including Default, SGCC S5000 and SGCC S6000. Select the format according to the Syslog server type. • Default - Syslog Server log Server can only receive the Hillstone log format. • S5000 - Syslog Server log Server can only receive SGCC-S5000 log format, such as the log Server's of State Grid Corporation of China.

Option	Description
	• S6000 - Syslog Server log Server can only receive SGCC-6000 log format, such as the monitoring Server's of State Grid Corporation of China.
Binding	Specifies the source IP address to receive logs. • Virtual Router: Select **Virtual Router** and then select a virtual router form the drop-down list. If a virtual router is selected, the device will determine the source IP address by searching the reachable routes in the virtual router. • Source Interface: Select **Source Interface** and then select a source interface from the drop-down list. The device will use the IP address of the interface as the source IP to send logs to the syslog server. If management IP address is configured on the interface, the management IP address will be preferred.
Protocol	Specifies the protocol type of the syslog server. The Secure-TCP uses the TLS encryption protocol. If "Secure-TCP" is selected, you can select **Do not validate the server certificate** option, and system can transfer logs normally and do not need any certifications.
Port	Specifies the port number of the syslog server.
Hostname Standard	By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, i.e. **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**. With this option checked, the logs sent to the Syslog Server displays the host-

Option	Description
	name and does not display the device SN, the format is: **<Device Number*8+log severity> date/timehostname log ID Hillstone Networks#log type@module: descriptions**.
Description	Enter a description for the syslog server as needed, which can be up to 255 characters in length.
Log Type	Specifies the log types the syslog server will receive.

4. Click **OK** to save the settings.

Notes: You can add at most 15 Syslog servers.

Configuring Sending Souceport Number

The system supports to specify the sending sourceport number used to send log messages to the Syslog Server. When the sending sourceport number is specified, the system will use the specified sending sourceport to send log messages to the Syslog Server. If the sending sourceport number is not specified, the system will use the random sourceport to send log messages to the Syslog Server by default.

To configure sending souceport number, take the following steps:

1. Click **Monitor > Log > Log Configuration** and select the Syslog Server Configuration tab.
2. Click the **Sending Sourceport Configuration** button to open the Sending Sourceport Configuration page.
3. Enter the specified sourceport number. The range is from 1024 to 65535. If you want to cancel the configuration of the current sourceport number, delete the value.
4. Click **OK**.

Notes:

- The binary logs sent to the Syslog Server is not influenced by the sending sourceport configuration. The binary logs are sent by UDP protocol using 5566 sourceport.
- When SNAT is enabled, the system will randomly select port as the sending source-port according to the port resources of network addresses translated by NAT.

Configuring Log Encoding

The default encoding format for the log information that is output to the Syslog server is utf-8, and the user can start GBK encoding as needed. After the GBK encoding format is opened, the log encoding format that is output to the Syslog server will be GBK encoding. To enable the GBK encoding :

1. Select **Monitor > Log > Log Configuration**.
2. Click **Syslog Server Configuration** tab.
3. Click the **Log Encoding Configuration** button in the upper right corner to open the Log Encoding Configuration page.
4. Click the button to enable the GBK Encoding.
5. .Click **OK** to save the settings.

Configuring an IPFIX Server

IPFIX (IP Flow Information Export) is a standard protocol for network monitoring and data exchange, used for collecting and transmitting network traffic information. IPFIX is a standardized version of the NetFlow V9 protocol, defined by the IETF (Internet Engineering Task Force), aimed at providing a standardized method for capturing traffic data in a network. This data typically includes flow statistics such as source and destination IP addresses, port numbers, protocol types, etc. As a result, IPFIX is widely used in scenarios such as network management and optimization, security monitoring, traffic analysis, and billing systems.

To meet customer needs in CGNAT (Carrier-Grade NAT, also known as NAT444) use cases, the firewall device support to configure the IPFIX server to export collected NAT444 logs in the corresponding template format to the specified IPFIX server. The NAT444 log template is a built-in system template that is periodically updated based on the configured template refresh interval, ensuring that the IPFIX server can correctly parse and retrieve NAT444 log data.

In NAT444 address translation, the system generates five NAT444 logs: user allocation port log, user release port log, port exhaustion alarm log, NAT444 session start log, and NAT444 session end log. Among these, only the user allocation port log and user release port log can be sent to the IPFIX server.

Notes: A maximum of three IPFIX servers can be configured.

To configure the IPFIX server, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration** > **IPFIX Server Configuration**.
2. Click **New**.

Option	Description
Name	Specifies the name of the IPFIX server, which can be 1 to 127 characters in length.
Hostname	Specifies the IP address or host name of the IPFIX server.
Binding	You can specify the source IP address for the IPFIX server to receive log information by selecting a virtual router or source interface: • Virtual Router: Select the virtual router to which the IPFIX server belongs from the **Virtual Router** drop-down list. • Source Interface: Select the source interface from the **Source Interface** drop-down list for the device to send log

Option	Description
	information. The device will use the IP address of the specified interface as the source IP to send log information to the IPFIX server. If the interface has a management IP address, it will use the management IP address first.
UDP Port	Enter the UDP port number of the IPFIX server, which is the destination port of the IPFIX server. The range is 1-65535, with a default of 9996.
Template Refresh Time	Specifies the refresh interval for the system's built-in NAT444 log template. Valid values: 1 to 3600 minutes. Default value: 30 minutes. Once specified, the system will periodically refresh the NAT444 log template based on the set interval, ensuring that the IPFIX server can correctly parse and retrieve the NAT444 log data.
Log Type	Select the type of log information the IPFIX server will receive. Currently, only the NAT log type is supported.

3. Click **OK**.

On the **IPFIX Server Configuration** tab, you can also perform the following operations:

- Edit: In the IPFIX server list, select the checkbox to the left of the server name and click **Edit** to modify the configuration information of the IPFIX server.
- Delete: In the IPFIX server list, select the checkbox to the left of the server name and click **Delete** to delete the selected IPFIX server.

Facility Configuration

The system supports to configure the facility generating log information. When the log information is sent to the Syslog server, the Facility field in the Syslog server will display the facility. You can

globally configure the facility generating log information, or separately specify the facility generating event logs and traffic logs. In addition, the separately specified facility takes precedence over the globally configured facility. If not configured, the Facility field defaults to "local7".

To configure a facility, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**.
2. In the **Facility Configuration** tab, configure the following options:

Option	Description
Global Configuration (required)	Select the facility that generates all types of logs from the drop-down list. Default value: local7. This is the global configuration, which can take effect for all types of logs.
event	Select the facility that generates event logs from the drop-down list. If not specified, the globally configured facility is used.
traffic	Select the facility that generates traffic logs from the drop-down list. If not specified, the globally configured facility is used.

3. Click **OK**.

Managing Logs

Option Descriptions of Various Log Types

This section describes the options when you set the properties of each log types.

Event Log

Option	Description
Enable	Click the button to enable the event logging function.
Console	Select the check box to send a syslog to the Console. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Option	Description
Terminal	Select the check box to send a syslog to the terminal. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to send a syslog to the cache. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max Buffer Size - The maximum size of the cached logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send a syslog to the local database. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. Note: AEX-series firewalls installed with hard disks support this function.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export event logs to the syslog server.

Option	Description
	• View Syslog Server - Click to see all existing syslog servers or to add new server. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Email Address	Select the check box to send event logs to the email. • View Email Address: Click to see all existing email addresses or add a new address. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
SMS	Select the check box to send event logs to the SMS. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Network Log

Option	Description
Enable	Click the button to enable the network logging function.
Cache	Select the check box to export network logs to the cache. • Max Buffer Size - The maximum size of the cached network logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes.

Option	Description
	• Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Local DB	Select the check box to send network logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.

Configuration Log

Option	Description
Enable	Click the button to enable the configuration logging function.
Cache	Select the check box to export configuration logs to the cache. • Max Buffer Size - The maximum size of the cached configuration logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send configuration logs to a file. • Max File Size - Specifies the maximum size of the configuration log file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the

Option	Description
	network log file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add new server.
Log Speed Limit	Select the check box to define the maximum efficiency of generating logs. • Maximum Speed - Specified the speed (messages per second).
Local DB	Select the check box to send configuration logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.

Session Log

Option	Description
Enable	Click the button to enable the session logging function. • Record User Name: Select to show the user's name in the session log messages. • Record Host Name: Select to show the host's name in the session log messages.
Cache	Select the check box to export session logs to cache. • Max Buffer Size - The maximum size of the cached session logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Local DB	Select the check box to send session logs to the local database.

Option	Description
	Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to export session logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

PBR Log

Option	Description
Enable	Click the button to enable a PBR logging function. • Record User Name: Select to show the user's name in the PBR log messages. • Record Host Name: Select to show the host's name in the PBR log messages.
Cache	Select the check box to export PBR logs to the cache. • Max Buffer Size - The maximum size of the cached PBR logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export PBR logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to

Option	Description
	add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of plain text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

NAT Log

Option	Description
Enable	Click the button to enable the NAT logging function. • Record Host Name: Select to show the host's name in the NAT log messages.
Cache	Select the check box to export NAT logs to cache. • Max Buffer Size - The maximum size of the cached NAT logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send NAT logs to the local database. Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to export NAT logs to the syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

Option	Description
IPFIX Server	Select the checkbox to export NAT444 logs (only user allocation port logs and user release port logs) to the IPFIX server. • View IPFIX Server - Click to view all existing IPFIX servers in the system.

IoT Log

Option	Description
Enable	Click the button to enable the IoT logging function. • Record Host Name: Select to show the host's name in the IoT log messages.
Cache	Select the check box to export IoT logs to cache. • Max Buffer Size - The maximum size of the cached IoT logs.
Syslog Server	Select the check box to export IoT logs to the Syslog server. • View Syslog Server - Click to see all existing Syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

EPP Log

Option	Description
Enable	Click the button to enable the EPP logging function.
Terminal	Select the check box to send a syslog to the terminal.

Option	Description
	• Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to export EPP logs to cache. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max Buffer Size - The maximum size of the cached logs.
File	Select the check box to send EPP logs to a file. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Specifies the maximum size of the EPP log file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes.
Syslog Server	Select the check box to export EPP logs to the Syslog server. • View Syslog Server - Click to see all existing Syslog servers or to add a new server. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.
Email Address	Select the check box to send EPP logs to the email.

Option	Description
	• View Email Address: Click to see all existing email addresses or add a new address. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

URL Log

Option	Description
Enable	Click the button to enable the URL logging function. • Record Host Name: Select to show the host's name in the URL log messages.
Cache	Select the check box to export URL logs to the cache. • Max Buffer Size - The maximum size of the cached URL logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export URL logs to a Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

File Filter Log

Option	Description
Enable	Click the button to enable the File Filter logging function.

Option	Description
Cache	Select the check box to export File Filter logs to cache. • Max Buffer Size - The maximum size of the cached File Filter logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export File Filter logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

Content Filtering Log

Option	Description
Enable	Click the button to enable the Content Filter logging function.
Cache	Select the check box to export Content Filter logs to cache. • Max Buffer Size - The maximum size of the cached Content Filter logs. The default value may vary for different hardware platforms.
Syslog Server	Select the check box to export Content Filter logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Option	Description
	• Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

Network Behavior Record Log

Option	Description
Enable	Click the button to enable the Network Behavior Record logging function.
Cache	Select the check box to export Network Behavior Record logs to cache. • Max Buffer Size - The maximum size of the cached Network Behavior Record logs. The default value may vary from different hardware platforms.
Syslog Server	Select the check box to export Network Behavior Record logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.

CloudSandBox Log

Option	Description
Enable	Click the button to enable the CloudSandBox logging function.
Cache	Select the check box to export CloudSandBox logs to the cache. • Max Buffer Size - The maximum size of the cached CloudSandBox logs.
Local DB	Select the check box to send cloud sandbox logs to the local database. Note: AEX-series firewalls installed with hard disks support this function.
File	Select to export CloudSandBox logs as a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Syslog Server	Select the check box to export CloudSandBox logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Threat Log

Option	Description
Enable	Click the button to enable the threat logging function. • Record User Name: Select to show the user's name in the threat

Option	Description
	log messages.
Record User Information	Click the button to enable the Record User Information function for Threat Log. With this function enabled, threat logs will record information about the authenticated user, including AAA server, username, and hostname.
Cache	Select the check box to export threat logs to the cache. • Max buffer size - The maximum size of the cached threat logs. The default value may vary from different hardware platforms. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Local DB	Select the check box to export threat logs to local database. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. Note: AEX-series firewalls installed with hard disks support this function.
File	Select to export threat logs as a file to USB. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Exported log file maximum size. • Save logs to USB - Select a USB device and enter a name as the log file name. • SSD Log - Select the check box to store logs on the hard disk. Only SG-6000-X9180 supports this function.
Terminal	Select to send logs to terminals.

Option	Description
Syslog Server	Select the check box to export threat logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - the distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different Syslog servers, which will relieve the pressure of a single Syslog server. The algorithm can be Round Robin or Src IP Hash.
Email address	Select the check box to export logs to the specified email address. • Viewing Email Address: Click to see or add email address.
Database	Select the checkbox to save logs in the local device. Only several platforms support this parameters. • Disk Space - Enter a number as the percentage of a storage the logs will take. For example, if you enter 30, the threat logs will take at most 30% of the total disk size. • Disk Space Limit - If **Auto Overwrite** is selected, the logs which exceed the disk space will overwrite the old logs automatically. If **Stop Storing** is selected, system will stop storing new logs when the logs exceed the disk space.

Share Access Log

Option	Description
Enable	Click the button to enable the Share Access logging function.
Console	Select to export Share Access logs to the console.

Option	Description
Cache	Select the check box to export Share Access logs to the cache. • Max buffer size - The maximum size of the cached Share Access logs.
Syslog Server	Select the check box to export Share Access logs to the Syslog server. • View Syslog Server - Click to see all existing syslog servers or to add a new server.

Endpoint Tag Log

Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Console	Select to export Share Access logs to the console.
Cache	Select the check box to send endpoint tag logs to the memory buffer. • Max Buffer Size - Specify the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Local DB	Select the check box to send endpoint tag logs to the local database. Note: AX-series firewalls installed with hard disks support this function.
Syslog Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "View Log Server" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Syslog Server.

Endpoint Tag Log

The system support management of endpoint tag logs by using the endpoint tag log function. To configure and manage endpoint tag logs, take the following steps:

1. Select **Monitor** > **Log** > **Endpoint Tag Log** or select **ZTNA** > **Endpoint Tag Log**.

    - Time: indicates the endpoint tag log's generation time.
    - Type: indicates the endpoint tag log type, including login, logout, abnormal logout, endpoint tag update and application resource update.
    - User Name: indicates the user name.
    - User IP(v4): indicates the user IPv4 address.
    - User IP(v6): indicates the user IPv6 address.
    - AAA Server: indicates the AAA server to which the user belongs.
    - Endpoint Name: indicates the endpoint name.
    - Endpoint IP: indicates the endpoint IP address.
    - OS: indicates the operating system of the endpoint.
    - Endpoint Tags: indicates the endpoint tag associated with the user.
    - ZTNA Server: indicates the ZTNA service name that the user accesses.
    - Allowed Application Resources: indicates the application resources that the user are allowed to access.
    - Denied Application Resources: indicates the application resources that the user are not allowed to access.

2. Click **Configure** and enter the **Endpoint Tag Log** page.

Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Cache	Select the check box to send endpoint tag logs to the memory buffer.
Max Buffer Size	When configuring the system to send endpoint tag logs to the memory buffer, you can define the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Syslog Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "View Syslog Server" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Syslog Server.

3. Click **Filter** to view endpoint tag logs that match the specified filtering conditions.
4. Click **Clear** to clear all endpoint tag logs.

   Note: This option is not supported for devices that support sending log information to the local database.
5. Click **Export** to export all endpoint tag logs to a local file.

For more information, refer to the **Monitor** > **Logging** topic in *StoneOS WebUI User Guide*. FR 40679

General Features

……

Exporting Logs

The system supports multiple log types and you can export logs to different destinations. You are allowed to export logs to the following destinations. You can specify the destination as needed.

- Console - Export logs to the Console.
- Terminal- Export logs to Telnet or SSH terminal。
- Cache - Export logs to cache.
- File - Export logs to a file.
- Log Server (Syslog Server) - Export logs to UNIX or Windows Syslog Server.
- Log Server (IPFIX Server) - Export NAT444 logs (only user allocation port logs and user release port logs) to IPFIX Server.
- Email Address- Export logs to the specified email address.
- Database - Export logs to the local database, which resides in storage devices, including SD memory cards and USB flash drives and expansion hard drives.
- SMS - Export logs to specified mobile phone as an SMS.

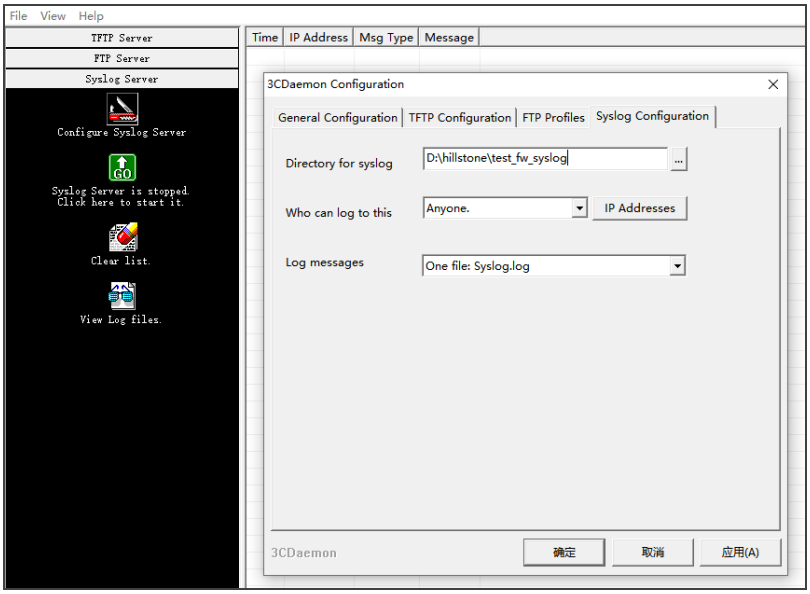
Application Scenario

A user needs to view the NAT logs of the firewall deployed at the Intranet exit and the NAT logs of the firewall should be exported to the Syslog server in plaintext.

Configuration Steps

Step 1: Configuring the Syslog Server on PC

1. Install the Syslog server software on the PC that needs to receive logs. Take 3CDaemon as an example.
2. When the installation is completed, open 3CDaemon.
3. Click **Syslog Server** and then click **Configure Syslog Server**.
4. In the **3CDaemon Configuration** dialogue box, configure the directory for storing the Syslog file, allowed log senders, and the log file name.

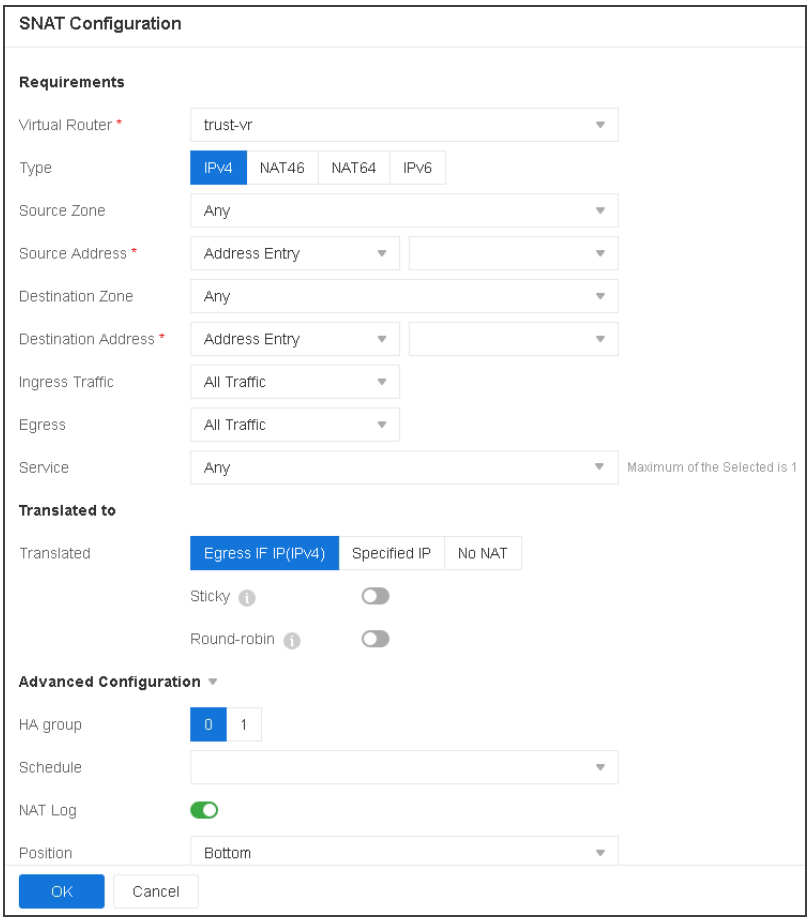


Step 2: Configuring the Export of NAT Logs

To enable the NAT log function of the NAT rule, take the following steps:

1. Select **Policy > NAT > SNAT/DNAT**。
2. Enable NAT Log for each NAT rule. Take the SNAT rule as an example. On the **SNAT Configuration** page, go to **Advanced Configuration** section, and click the enable button behind

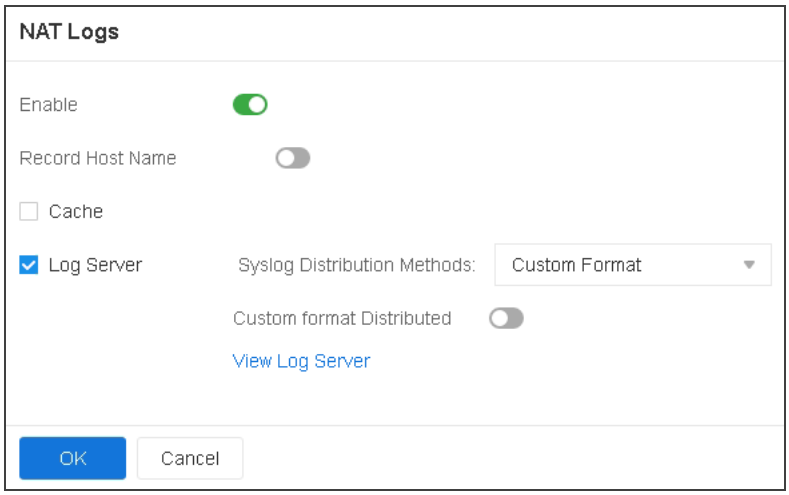
NAT Log.



To enable the NAT log function of the device, take the following steps:

1. Select **Monitor** > **Log** > **NAT Log**.

2. Click **Configure** to go to the **NAT Logs** panel.



Option	Value
Enable	Click the button to enable the NAT log function.
Syslog Server	Click the check box of **Syslog Server** and select **Custom Format** from the **Syslog Distribution Methods** drop-down list.

3. Click **OK**.

   You can also go to Monitor > Log > Log Management. Click the button behind NAT Log and click to make corresponding configuration.



To configure the Syslog server, take the following steps:

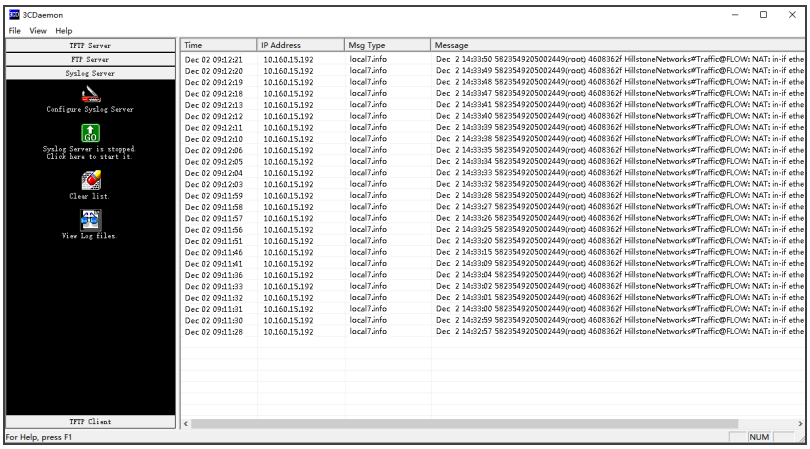
1. Select **Monitor** > **Log** > **Log Configuration** > **Syslog Server Configuration**.
2. On the **Syslog Server Configuration** tab, click **New**.

Option	Value
Hostname	Enter the IP address of the PC where the log server is located.
Binding	Virtual Router
Protocol	UDP (the default syslog protocol)
Port	514 (the default syslog port)
Log Type	Select **NAT Log**.

3. Click **OK**.

Step 3: Viewing NAT Logs in the Syslog Server

- Access the Syslog server. You can see that the Syslog server has received NAT logs.



- Access the directory for saving log files and you can view the saved log files.

For more information, refer to the **Getting Started Guide** > **General Features** > **Exporting Logs** in *StoneOS WebUI User Guide*. FR 40679

CLI

Configuring the IPFIX Server

IPFIX (IP Flow Information Export) is a standard protocol for network monitoring and data exchange, used for collecting and transmitting network traffic information. IPFIX is a standardized version of the NetFlow V9 protocol, defined by the IETF (Internet Engineering Task Force), aimed at providing a standardized method for capturing traffic data in a network. This data typically includes flow statistics such as source and destination IP addresses, port numbers, protocol types, etc. As a result, IPFIX is widely used in scenarios such as network management and optimization, security monitoring, traffic analysis, and billing systems.

To meet customer needs in CGNAT (Carrier-Grade NAT, also known as NAT444) use cases, the firewall device support to configure the IPFIX server to export collected NAT444 logs in the corresponding template format to the specified IPFIX server. The NAT444 log template is a built-in system template that is periodically updated based on the configured template refresh interval, ensuring that the IPFIX server can correctly parse and retrieve NAT444 log data.

In NAT444 address translation, the system generates five NAT444 logs: user allocation port log, user release port log, port exhaustion alarm log, NAT444 session start log, and NAT444 session end log. Among these, only the user allocation port log and user release port log can be sent to the IPFIX server.

Notes: A maximum of three IPFIX servers can be configured.

To export log information to the IPFIX server, you need to complete the following configurations:

- Creating the IPFIX Server
- Configuring the IPFIX Server Parameters
- Specifying the Template Refresh Time
- Specifying the Output Log Type
- View IPFIX Server Configuration Information

Creating the IPFIX Server

All configurations for the IPFIX Server need to be completed in IPFIX Server configuration mode. To create the IPFIX Server and enter the IPFIX Server configuration mode, use the following command in global configuration mode:

logging ipfix-server*server-name*

- *server-name* – Specifies the name of the IPFIX Server. Valid values: 1 to 127 characters.

After executing this command, the system creates an IPFIX Server with the specified name and enters the IPFIX Server configuration mode. If the specified name already exists, the system directly enters the IPFIX Server configuration mode.

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

no logging ipfix-server*server-name*

Configuring the IPFIX Server Parameters

After creating the IPFIX Server, the user needs to configure the IPFIX Server's IP address or host name, UDP port, binding method, and virtual router. In IPFIX Server configuration mode, use the following commands:

server { **ip***ip-address* | **hostname***hostname*} **udp***udp-port-number***bindtype** { **vrouter***vr-name* | **source-interface***interface-name*}

- **ip***ip-address* | **hostname***hostname* – Specifies the IP address or host name of the IPFIX Server.
- **udp***udp-port-number* - Specifies the UDP port number of the IPFIX Server, which is the destination port of the IPFIX server. Valid values: 1 to 65535. Default value: 9996.
- **bindtype** { **vrouter***vr-name* | **source-interface***interface-name*} - Specifies the VRouter to which the IPFIX Server belongs or the source interface used to send log information. **vrouter***vr-name* specifies the name of the VRouter, **source-interface***interface-name* specifies the source interface for sending log information. The device will use the IP address of the specified interface as the source IP to send log information to the IPFIX server. If the interface has a management IP address, it will use the management IP address first.

To delete all configurations of the specified IPFIX Server, in IPFIX Server configuration mode, use the following command:

no server

Notes: After executing the no server command, the UDP port configuration is restored to the default value of 9996.

Specifying the Template Refresh Time

Specifying the refresh interval for the system's built-in NAT444 log template. Then, the system will periodically refresh the NAT444 log template based on the set interval to ensure that the IPFIX server can correctly parse and retrieve the NAT444 log data.

To specify the template refresh time, in IPFIX Server configuration mode, use the following command:

refresh-time*time-value*

- *time-value* – Specifying the template refresh interval. Valid values: 1 to 3600 minutes. Default value: 30 minutes.

To restore the system default template refresh time, in IPFIX Server configuration mode, use the following command:

no refresh-time

Specifying the Output Log Type

Specify the type of log to export to the IPFIX server. Currently, only the NAT log type is supported. To do this, in IPFIX Server configuration mode, use the following command:

log-enable nat

To delete the specified log type, in IPFIX Server configuration mode, use the following command:

no log-enable nat

Viewing IPFIX Server Configuration Information

You can view the IPFIX server configuration information in any mode using the following command:

show logging ipfix-server

Example:

```
hostname# show logging ipfix-server
servername hostname bindname protocol port logtype refreshtime
---------------------------------------------------------------------------------------
ipfix 2.2.2.2 trust-vr UDP 5400 nat 30
```

……

Sending and Filtering Event Logs

You can specify the output destination for the event logs as needed, and filter the output logs based on the severity.

To send event logs to the console, remote terminal, syslog server, mobile phone, hard-disk card or enable email notification, and filter the output logs, in the global configuration mode, use the following command:

logging event to {**console** | **remote** | **syslog**| **sms** | **email** | **localdb** } [**severity***severity-level*]

- **console** – Sends the event logs to the console.
- **remote** – Sends the event logs to the remote terminal.
- **syslog** – Sends the event logs to the Syslog Server.
- **sms** – Sends the event logs whose severity is Critical or is higher than Critical to the mobile phone by using SMS.
- **email** – Sends the event logs to the Email.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
- **severity***severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.

To disable the function, in the global configuration mode, use the following command:

no logging event to {**console** | **remote** | **syslog** | **sms** |**email** | **localdb**}

To send the event logs to the memory buffer and filter the logs, in the global configuration mode, use the following command:

logging event to buffer [**severity***severity-level*] [**size***buffer-size*]

- **severity***severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **size***buffer-size* – Specifies the buffer size. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to buffer**.

To write the event logs to a file and filter the logs, in the global configuration mode, use the following command:

logging event to file [**severity***severity-level*] [**name** [**usb0** | **usb1**] *file-name*] [**size***file-size*]

- **severity***severity-level* – Specifies the severity of the output event logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only write event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size***file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 10485764 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging event to file**.

Sending Threat Logs

You can specify the output destination for the threat logs as needed. To send threat logs to the console, remote terminal, syslog server, hard-disk or enable email notification, in the global configuration mode, use the following command:

logging threat to {**console** | **remote** | **syslog** [**custom-format** [**distributed** [**round-robin** | **src-ip-hash**]]] | **email** | **localdb** } [**severity***severity-level*]

- **console** – Sends the threat logs to the console.
- **remote** – Sends the threat logs to the remote terminal.
- **syslog** – Sends the threat logs to the Syslog Server.
- **custom-format** – Sends the log messages in plaintext. By default, the system sends the log messages in plaintext.
- **distributed** – Sends the log messages to multiple syslog servers in the distribution mode.
- **src-ip-hash** | **round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **email** – Sends the threat logs to the Email.
- **localdb** – Sends the logs to the local database(hard-disk card). Only several platforms support the parameters.
- **severity***severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only write event logs of Notifications, Warnings and Errors severities.

To disable the function, in the global configuration mode, use the following command:

no logging threat to {**console** | **remote** | **syslog**| **email**| **localdb** } [**severity***severity-level*]

To send the threat logs to the memory buffer, in the global configuration mode, use the following command:

logging threat to buffer [**severity***severity-level*] [**size***buffer-size*]

- **severity***severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **size***buffer-size* – Specifies the buffer size. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to buffer**.

To write the threat logs to a file, in the global configuration mode, use the following command:

logging threat to file [**severity***severity-level*] [**name** [**usb0** | **usb1**] file-name] [size file-size]

- **severity***severity-level* – Specifies the severity of the output threat logs to filter the logs. Only the logs of the specified severity or higher severities will be sent, i.e., the number should be equal to or smaller than the specified number. For example, if the specified severity is Notifications, then system will only send event logs of Notifications, Warnings and Errors severities.
- **name** [**usb0** | **usb1**] *file-name* – Specifies the USB disk and file that are used to save the logs.
- **size***file-size* – Specifies the size of the file (on the USB disk or Flash disk) to which the logs are written to. The value range is 4096 to 1048576 bytes. The default value is 1048576.

To disable the function, in the global configuration mode, use the command **no logging threat to file**.

Sending Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. You can send traffic logs to the console, syslog server, memory buffer, IPFIX server (only NAT logs can be exported to the IPFIX server) and local SSD (Web surfing logs cannot be sent to SSD). You can select the output destination according to your requirements.

To send the traffic logs to the console , buffer or syslog server, use the following command in the global configuration mode:

logging traffic {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** [**size***buffer-size*] }

To export NAT traffic logs to the IPFIX server, in global configuration mode, use the following command:

logging trafficnattoipfix-server

To send session logs and NAT logs to the local SSD, in the global configuration mode, use the following command:

logging traffic {**session** | **nat**} **to localdb**}

- **session** | **nat** | **urlfilter** – Specifies the log type that you want to output.
- **console** | **syslog** | **buffer** – Specifies the output destination. You can output the logs to the console ,buffer or syslog server. For more information about how to configure the Syslog Server, see Configuring the Syslog Server.
- **ipfix-server** - Specifies to export NAT logs (NAT444) to the IPFIX server. For more information about how to configure the IPFIX Server, see Configuring the IPFIX Server.
- **localdb** – Specifies the output destination of session logs and NAT logs as the SSD on the device. Web surfing logs cannot be sent to the local SSD. Only CloudEdge, SSD-equipped A-series (except A2200, A1800, and A1600) and X-series devices support this function.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

In the global configuration mode, use the following command to disable the output function: **no logging traffic** {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** }, **no logging trafficnattoipfix-server** or **no logging traffic** {**session** | **nat** } **to localdb**.

Sending Data Security Logs

You can specify the output destination for the data security logs (file filter logs, content filter logs, network behavior record logs) as needed. To send data security logs (file filter logs, content filter logs, network behavior record logs)to the console, remote terminal, syslog server, local database, or enable email notification, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog**[**binary-format** [**distributed** [**src-ip-hash** | **round-robin**]] | **custom-format**]] }

- **console** – Sends the data security logs to the console.
- **syslog** – Sends the data security logs to the Syslog Server.
- **binary-format** – Sends the logs in binary format.
- **distributed** – Sends the logs to multiple servers in the distribution mode.
- **src-ip-hash | round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and**round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.
- **custom-format** – Sends the logs in plaintext. By default, the system sends the logs in plaintext.

To disable the function, in the global configuration mode, use the following command:

no logging data-security [**dlp** | **cf** | **nbr**] **to** {**console** | **syslog** }

To send the data security logs (file filter logs, content filter logs, network behavior record logs) to the memory buffer, in the global configuration mode, use the following command:

logging data-security [**dlp** | **cf** | **nbr**] **to buffer** [**size***buffer-size*]

- **size***buffer-size* – Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 524288.

To disable the function, in the global configuration mode, use the command **no logging data-security [dlp | cf | nbr] to buffer**.

Sending IoT Logs

IoT logs can be sent to the console, buffer and syslog server. You can specify the output destination for IoT logs as needed. Before you specify the output destination, in the global configuration mode, you need to enable the IoT logs function with the following commands:

logging iot-monitor on

In the global configuration mode, use **no logging iot-monitor on** to disable the IoT logs function.

To send IoT logs to console, buffer and syslog server, in the global configuration mode, use the following command:

logging iot-monitor to {console | buffer [size*buffer-size***] | syslog [custom-format [distributed [src-ip-hash | round-robin]]]}**

- **console** – Sends IoT logs to the specified console.
- **syslog** – Sends IoT logs to the specified syslog server. For how to configure the syslog server, refer to Configuring Syslog Server.
- **custom-format** – Sends IoT logs in the plain text. By default, system sends logs in the plain text.
- **distributed** – Distributes IoT logs in the plain text to several syslog servers.
- **src-ip-hash | round-robin** – Specifies the algorithm, including **src-ip-hash** and **round-robin** (the default algorithm).

In the global configuration mode, use the following command to disable the function.

no logging iot-monitor to {console | buffer | syslog}

Configuring the Output Log Format

StoneOS logs follow a fixed pattern of information layout. By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, i.e. **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

Output example of logs in the default format: <188> Apr 11 02:48:22 25083xxxxxx05643(root) 42340401 HillstoneNetworks#Event@MGMT: Admin user "hillstone" cleared Debug log\n\000

Based on the log standard defined by RFC 3164/5424:

- Standard format: **<Device Number*8+log severity> date/timehostname log ID HillstoneNetworks#log type@module: descriptions**
- Non-standard format: **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

You can configure the output log format as needed. In the the global configuration mode, use the following command:

- Display the four digit year: **logging syslog 4digit-year-timestamp**

  The output format is: **<Device Number*8+log severity> four digit year-date/time time zoneSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**

  Sample output: <188> 2024-04-11T02:49:23.380569Z 25083xxxxxx05643(root) 421c041f HillstoneNetworks#Event@MGMT: Admin user "hillstone" logout through SSH, the IP is X.X.X.X, and the corresponding login time is 2024-04-11 02:43:25.\n

- Display the hostname and the log severity: **logging syslog additional-information**

  The output format is: **<Device Number*8+log severity> date/timeSN(VSYS name)[h:hostname][p:log severity] log ID HillstoneNetworks#log type@module: descriptions**

  Sample output: <186> Apr 11 02:50:46 25083xxxxxx05643(root)[h:SG-6000][p:2] 42080a0d HillstoneNetworks#Event@MGMT: hillstone save system configuration via SSH.\n\000

- Display the hostname and not display the device SN.

    1. In global configuration mode, enter the configuration mode of the specified Syslog server: **logging syslog-server***server-name*

    2. In configuration mode of the specified Syslog server, enter **hostname standard**
       The output format is: **<Device Number*8+log severity> date/timehostname log ID HillstoneNetworks#log type@module: descriptions**
       Sample output: <189> Apr 11 02:46:32 SG-6000 43240501 Hill-stoneNetworks#Event@NET: Static entry is created, 1.1.1.1, 1111.1111.1111, trust-vr\n\000

To cancel the displaying of four digit year /hostname/ log severity, and restore the default log format in the the global configuration mode, use the following command:

- Cancel display the four digit year: **no logging syslog 4digit-year-timestamp**
- Cancel display the hostname and the log severity: **no logging syslog additional-information**
- Display the device SN and cancel display the hostname: In configuration mode of the specified Syslog server, enter **no hostname standard**

Specifying a Facility

The Facility field is used to identify the device generating the log information. When the log information is sent to the Syslog server, the Facility field will be displayed in the Syslog server. The system supports global configuration of the Facility field for log information, and also supports separately specifying the Facility field for event logs and traffic logs. In addition, the separately specified Facility field takes precedence over the globally configured Facility field. If not configured, the Facility field defaults to "local7".

Globally Configuring the Facility Field of Log Messages

The system supports to globally configure the Facility field of log messages. This configuration can take effect for all types of logs. To globally configure the Facility field of log messages, in global

configuration mode, use the following command:

logging facility local*x*

• **local***x* – Specifies the Facility field of log information. The value range of x is an integer from 0 to 7. The default value is 7.

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

Separately Specifying the Facility Field of Event Logs and Traffic Logs

To separately specify the Facility field of event logs and traffic logs, in global configuration mode, use the following command:

logging {**event** | **traffic**} **facility local***x*

• **local***x* – Specifies the Facility field of event logs and traffic logs. The value range of x is an integer from 0 to 7.

To delete the specified Facility field, in global configuration mode, use the command **no logging** {**event** | **traffic**} **facility**.

Viewing the Facility Field of Event Logs and Traffic Logs

To view the Facility field of log messages, in any mode, use the following command:

show logging facility

The following result is returned:

```
hostname#show logging facility
Event：local0
Traffic：local2
```

Viewing Log Configurations

To view the log configurations, in any mode, use the following commands:

- Show the system log configuration:**show logging**
- Show the syslog server configuration: **show logging syslog-server**
- Show the email address configuration:**show logging email**
- Show the log statistics:**show logging statistics**
- Show the SMTP server configuration: **show smtp**
- Show if the hostname and username are displayed : **show logging content**
- Show if the hostname and username are displayed in the logs: **show logging content**
- Show the SMS configuration: **show logging sms**

Sending Traffic Logs to Syslog Servers

When there are lots of log messages generated by Hillstone devices, a single Syslog server may fail to deal with all the messages. To address this problem, Hillstone devices support the distributed sending function. With this function configured, Hillstone devices can send the log messages to multiple Syslog servers according to a certain algorithm to reduce the pressure to a single Syslog server.

> **Notes:** Only the traffic and data security log messages can be sent in the distributed way. And only the threat logs can be sent in plaintext and in the distributed way.

To configure the distributed sending function, in the global configuration mode, use the following command:

logging {traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr]} to syslog [binary-format [distributed [src-ip-hash | round-robin]] | custom-format]

- **traffic {session | nat | urlfilter} | data-security [dlp | cf | nbr]** – Specifies the log type that will be sent.

- **syslog** – Sends the logs to Syslog servers.
- **binary-format** – Sends the traffic logs in the binary format.
- **distributed** – Sends the traffic logs to multiple Syslog servers according to the algorithm specified.
- **src-ip-hash** | **round-robin** – Specifies the algorithm used to choose Syslog servers. **src-ip-hash**, choose the Syslog server according to the source IP address; **round-robin**, choose the Syslog server by the round-robin algorithm, and this is the default algorithm used by the system.
- **custom-format** – Sends logs in the plaintext format. By default, the system will send the traffic logs in the plaintext format.

To remove the traffic log sending configuration, in the global configuration mode, use the following command:

no logging {**traffic** {**session** | **nat** | **urlfilter**} | **data-security** [**dlp** | **cf** | **nbr**]} **to syslog**

To send the threat logs in the plaintext format and in the distributed way, use the following command in the global configuration mode:

logging threat to syslog [**custom-format** [**distributed** [**src-ip-hash** | **round-robin**]]]

- **custom-format** – Sends the logs in the plaintext format. By default, the system sends the logs in the plaintext format.
- **syslog** – Sends the logs to the syslog server.
- **distributed** – Sends the logs to the syslog server in the distributed way.
- **src-ip-hash** | **round-robin** – Specifies the server selection algorithm.**src-ip-hash**indicates the source-hashing algorithm and **round-robin**indicates the round-robin scheduling algorithm. The round-robin scheduling algorithm is the default algorithm.

In the global configuration mode, use the following command to cancel the output of the threat logs:

no logging threat to syslog

For more information, refer to the **Monitor** > **Logs** topic in *StoneOS CLI User Guide*. FR 40679

Supporting to Create SSL VPN and ZTNA Dual Stack Instances

WebUI

SSL VPN

SSL VPN

The device provides an SSL based remote access solution. Remote users can access the intranet resource safely through the provided SSL VPN.

SSL VPN consists of two parts: SSL VPN server and SSL VPN client. The device configured as the SSL VPN server provides the following functions:

- Accept client connections.
- Allocate IP addresses, DNS server addresses, and WIN server addresses to SSL VPN clients.
- Authenticate and authorize clients.
- Perform host checking to client.
- Decrypting and forwarding encrypted packet from the client.

By default, the concurrent online client number may vary on different platform series. You can expand the supported number by purchasing the corresponding license.

After successfully connecting to the SSL VPN server, the SSL VPN client secures your communication with the server. The following SSL VPN clients are available:

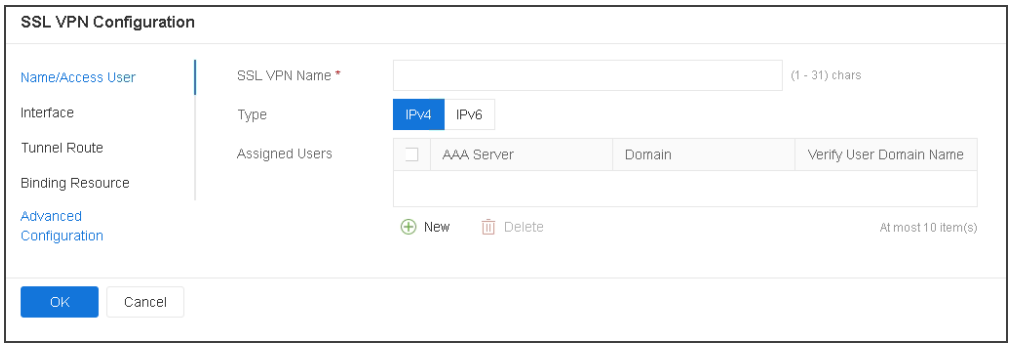
- Hillstone Secure Connect Client for Windows
- Hillstone Secure Connect Client for Android

- Hillstone Secure Connect Client for iOS
- Hillstone Secure Connect Client for macOS
- Hillstone Secure Connect Client for Linux
- Hillstone Secure Connect Client for ChineseOS

Configuring an SSL VPN

To configure an SSL VPN, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. In the SSL VPN page, click **New**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
SSL VPN Name	Type the name of the SSL VPN instance.The length is 1 to 64 characters.
Type	Select IPv4, IPv6, or Dual Stack to specify the service type of the SSL VPN instance. The IPv6 and Dual Stack options are available only when the version is IPv6. **Related Concept:**Dual stack is a network technology that allows both IPv4 and IPv6 protocol stacks to run simultaneously on a network device, enabling seamless switching and com-

Option	Description
	munication between IPv4 and IPv6 networks.
Assigned Users (at most 10 items)	
AAA Server	Select an AAA server from the **AAA Server** drop-down list. You can click **View AAA Server** to view the detailed information of this AAA server. If you select an OAuth2 server, the client supports OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server.The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, system will verify the username and its domain name. **Note**: The OAuth2 server does not support user domain name verification.
Add	Click **Add** to add the assigned users. You can repeat to add more items.

In the Interface tab, configure the corresponding options.

Access Interface	
Egress Interface	Select the interface from the drop-down list as the SSL VPN server interface. This interface is used to listen to the request from the SSL VPN client. At most 8 interfaces can be selected.
Service Port	Specifies the SSL VPN service port number.The value range is 1 to 65535.
Tunnel Interface	
Tunnel Interface	Specifies the tunnel interface used to bind to the SSL VPN tunnel. Tunnel interface transmits traffic to/from SSL VPN tunnel. • Select a tunnel interface from the drop-down list, and

Access Interface	
	then click **Edit** to edit the selected tunnel interface. • Click **New** in the drop-down list to create a new interface.
Address Pool	
IPv4 Address Pool	Specifies the SSL VPN address pool. • Select an address pool from the drop-down list, and then click **Edit** to edit the selected address pool. • Click **New** in the drop-down list to create a new address pool.
IPv6 Address Pool	• When configuring IPv4 SSL VPN, you need to specify the IPv4 SSL VPN address pool. • When configuring IPv6 SSL VPN, you need to specify the IPv6 SSL VPN address pool. • When configuring dual stack SSL VPN, you need to specify both IPv4 and IPv6 SSL VPN address pools.

In the Tunnel Route tab, configure the following options.

Tunnel Route
• When configuring IPv4 SSL VPN, you need to specify the IPv4 tunnel route so that you can access IPv4 intranet resources. • When configuring IPv6 SSL VPN, you need to specify the IPv6 tunnel route so that you can access IPv6 intranet resources.

Tunnel Route	
• When configuring dual stack SSL VPN, you need to specify both the IPv4 and IPv6 tunnel routes so that you can access IPv4 and IPv6 intranet resources.	
After the SSL VPN client receives the specified network segment, the client will generate the route to the specified destination network segment.	
New	Click **New** to add this route. You can repeat to add more items.
IP	Type the destination IP address.
Mask	Type the netmask of the destination IP address.
Metric	Type the metric value.
Type	Sets the user type to **User Group** or **Role**.
User Group/Role	When the type is set to **User Group**, select the AAA server to which the user group belongs and the user group name from the drop-down list. Only users in this user group can access the specified network segment in the tunnel route. You can also click ⊕ and create a user group in the **User Group Configuration** panel. For more information, see Creating a User Group. When the type is set to **Role**, select the role name from the drop-down list. Only users corresponding to this role can access the specified network segment in the tunnel route. You can also click ⊕ and create a role in the **Role Configuration** panel. For more information, see Creating a Role.
Delete	Click **Delete** to delete the selected route.

Tunnel Route	
Add Default Route	Click **Add Default Route** to add a default route with both the IP address and netmask being all 0.

Enable Dedicated SSL VPN Tunnel

Click the button to enable the dedicated SSL VPN tunnel function. This way, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to SSL VPN.

Notes:

- The client versions that support the dedicated SSL VPN tunnel function include: the latest version of the SSL VPN client for Windows, the latest version of the SSL VPN client for macOS, and the latest version of the SSL VPN client for Linux.
- The dedicated SSL VPN tunnel function cannot be used together with the domain route function.
- After you enable the dedicated SSL VPN tunnel function, we recommend that you do not configure a default route in the tunnel routing.

Enable Domain Route

Specifies the destination domain name that you want to access through SSL VPN tunnel.

After clicking the **Enable** button, system will distribute the specified domain names to the VPN client, and the client will generate the route to the specified destination according to the resolving results from the DNS.

Tunnel Route	
Notes: The domain route function cannot be used together with the dedicated SSL VPN tunnel function.	
Maximum	The maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value ranges from 1 to 10000. The default value is 1000.
New	Click **New** to add the domain name to the list and you can add up to 64 domain names.
Domain	Specifies the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. **com** and **.com** are not supported.
Delete	Click **Delete** to delete the selected domain name.

In the Binding Resource tab, configure the binding relationship between user groups, roles and resources.

Binding Resource	
New	Click **New** to add binding entries for resources and user groups, roles to the list below. You can repeat to add more items.
Name	Select an existing resource name from the drop-down list. The range is 1 to 63 characters.
Type	Select the binding type from the drop-down list. It can be a type of user group or role.
Resource List	Select an existing resource name from the drop-down list. The range is 1 to 63 characters.

Binding Resource	
User Group/role	Select an existing user group/role from the drop-down list. Click ⊕ to add a user group or a role. Select the AAA servers where user groups reside from the drop-down list. Currently, only the local authentication server and the RADIUS server are available. **Note**: • A user group/role can be bound with multiple resources, and a resource can also be bound with multiple user groups/roles. • Only 256 binding entries can be configured in an SSL VPN instance.
AAA Server	Select the AAA servers where user groups reside from the drop-down list. Currently, only the local authentication server and the RADIUS server are available.
Delete	Click **Delete** to delete the selected item.

3. If necessary, click **Advanced Configuration** to configure the advanced functions, including parameters, client, host security, SMS authentication, and optimized path.

   In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. **Any** indicates one of TLSv1, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If tlsv1.2 or any is specified to the SSL protocol in SSL VPN server, you need to convert the certificate that you are going

Security Kit	
	to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via SSL VPN client, so that the SSL VPN server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 –in oldcert.pfx –out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports tlsv1.2 protocol. **openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"** 3. Import the newly generated .pfx format certificate into your browser or USB Key. After the above operation, you have to log into SSL VPN server with SSL VPN client whose version is 1.4.6.1239 or later.
Trust Domain	Specifies the trust domain. When the GMSSLv1.0 protocol is

Security Kit	
	used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must config this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the SSL VPN tunnel. The default value is AES. **NULL** indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm.
Hash	Specifies the hash algorithm of the SSL VPN tunnel. The default value is MD5. **NULL** indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm.
Compression	Specifies the compression algorithm of the SSL VPN tunnel. By default, no compression algorithm is used.
Client Connection	
Allow Download Client from Browser	Select the check box of the client type to specify the allowed type of SSL VPN client. By default, you are allowed to access the system with five types of SSL VPN clients, which are SSL VPN client for Windows, SSL VPN client for Android, SSL VPN client for iOS, SSL VPN client for macOS, and SSL VPN client for Linux. You can configure to access the system only via the specified types of SSL VPN clients as needed.
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client. The value range is 1 minute to 25 hours.

Security Kit	
	The default value is 30 minutes.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list. When the schedule takes effect, the system forces online SSL VPN users to log out based on the periodic schedule or the time-frame. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • SSL VPN users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple Login	This function permits one client to sign in more than one place simultaneously. Select the **Enable** check box to enable the function.
Multiple Login Times	Type the number of simultaneous login with the same user name into the **Multiple Login Times** box. The value range is 0 to 99,999,999. The value of 0 indicates no limitation. The default value is 0.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.
DF-Bit	Specifies whether to permit packet fragmentation on the device forwarding the packets. The actions include: • Set - Forbids packet fragmentation. • Copy - Copies the DF value from the destination of the

Security Kit	
	packet. It is the default value. • Clear - Permits packet fragmentation.
Port (UDP)	Specifies the UDP port number for the SSL VPN connection. The value range is 1 to 65535.
Port (TCP)	Specifies the TCP port number for the SSL VPN connection. The value range is 1 to 65535.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Select one or more client types. By default, the system allows all of the 6 types of SSL VPN clients to access: the SSL VPN client for Windows, the SSL VPN client for Android, the SSL VPN client for iOS, the SSL VPN client for macOS, the SSL VPN client for Linux, and the SSL VPN client for ChineseOS. You can configure a specified allowed type of SSL VPN client as required.
Change Password URL	Specifies the URL address that can redirect to the specified URL page from the client to modify the password. The length is 0 to 255 characters.
Forgot Password URL	Specifies the URL address that can redirect to the specified URL page from the client to reset the password. The length is 0 to 255 characters. **Notes**: This configuration takes effect only after Change Password function is enabled on the local server.
Redirect URL	This function redirects the client to the specified redirected URL after a successful authentication. Type the redirected URL into the box. The value range is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are sup-

Client Configuration	
	ported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.-abc.-com/oa/-login.do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+user-name=$GBUSER&password=$PWD, e.g., http://www.-abc.-com/oa/-login.do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.-abc.com
Title	Specifies the description for the redirect URL. The value range is 0 to 31 characters. This title will appear as a client menu item.
Delete privacy data after dis-connection	Select **Enable** to delete the corresponding privacy data after the client's disconnection.
Digital Certificate Authentication	
Authentic-	Click **Enable** to enable this function. There are two options

Client Configuration	
ation	available: • Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username and password. The USB Key certificate users also need to type the USB Key password. • Digital Certificate only - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificater users also need to type the USB Key password. No username or user's password is required. When **Digital Certificate only** is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY	When USB Key authentication is enabled, you can download

Client Configuration	
Download URL	the UKey driver from this URL. The length is 0 to 63 characters.
Trust Domain Subject&Username Checking CN Matching OU Matching	To configure the trust domain and the subject & username checking function: 1. From the Trust domain drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU** box to determine whether matches them. 3. Click **Add**. The configured settings will be displayed in the list below. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Two-Step Verification** to enable the function. Two-Step Verification means that when an SSL VPN user logs

Option	Description
	in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS Authentication, Token Authentication or Email Authentication after the username and password is entered. The user must enter the random verification code received in order to log into SSL VPN and access intranet resources.
Type	Specifies the type of Two-Step Verification, including SMS Authentication, Token Authentication and Email Authentication: • SMS Authentication: Click **SMS Modem** or **SMS Gateway** to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Enter prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Authentication	Select the **SMS Authentication** to enable the function. And select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from drop-down list. For more information about SMS Gateway, see SMS Gateway.
Lifetime of SMS Veri-	Specifies the lifetime of the SMS authentication code. The range is 1 to 10 minutes. The default value is 10.

Option	Description
fication Code	
Sender Name	Specifies a message sender name to display in the message content. The range is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8. Note: If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the range of the length of the SMS verification code is 4 to 6.
SMS Template	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters. Note: If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the content of text messages must be " $ VRFYCODE".
Sign Name	If an ALIYUNSMS service provider name is specified for the "SMS Gateway Name" option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the SMS of Alibaba Cloud.
Template Code	If an ALIYUNSMS service provider name is specified for

Option	Description
	the "SMS Gateway Name" option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.
Email Authentication	
Mail Server	Specifies the existing Email server which the Email address that used to send the verification code is configured on. The range is 1 to 31 characters. For more information about the configuration of Mail Server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code. The range is 1 to 10 minutes. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code, SSL VPN server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users to configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8. The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not

Option	Description
	request this, please ignore it.".

In the Host Compliance Check/Binding tab, configure the corresponding options.

Host Compliance Check	
Creates a host compliance check rule to perform the host compliance check function. Before creating a host compliance check rule, you must first configure the host compliance check profile in Configuring a Host Compliance Check Profile.	
Role	Specifies the role to which the host compliance check rule will be applied. Select the role from the **Role** drop-down list. **Default** indicates the rule will take effect to all the roles.
Host Compliance Check	Specifies the compliance check profile. Select the profile from the **Host Compliance Check** drop-down list.
Exception handling method	Specifies the exception handling method. • Guest Role: Select the guest role from the **Guest Role** drop-down list. The user will get the access permission of the guest role when the host checking fails. If —— is selected, system will disconnect the connection when the host compliance check fails. • Redirect URL: Click the **Redirect URL** radio button, and then type the URL into the textbox. When the host checking fails, the browser jump to the specified URL and guide the user to download the software required for host security detection and

Host Compliance Check	
	disconnect the client. If this option is not configured, the client will be disconnected.
Guest Role	Select the guest role from the **Guest Role** drop-down list. The user will get the access permission of the guest role when the host checking fails. If **Null** is selected, system will disconnect the connection when the host compliance check fails.
Periodic Check	Specifies the host compliance check period. System will check the status of the host automatically according to the host compliance check profile in each period.
Add	Click **Add**. The configured settings will be displayed in the table below.
Delete	To delete an item, select the item you want to delete from the list, and then click **Delete**.
Host Binding	
Enable Host Binding	Click **Enable** to enable is this function. By default, one user can only log in one host. You can change the login status by configuring the following options. • Allow one user to login through multiple hosts. • Allow multiple users to login on one host. • Automatically add the user-host ID entry into the binding list at the first login. **Note**: To use the host binding function, you still have to configure it in the host binding configuration page. For more information about host binding, see Host Binding.

In the Optimized Path tab, configure the corresponding options.

Option	Description
Optimal path detection can automatically detect which ISP service is better, giving remote users a better user experience.	
No Check	Do not detect.
Client	The client selects the optimal path automatically by sending UDP probe packets.
Server	When the client connects to the server directly without any NAT device, this is the detection process: 1. The server recognizes the ISP type of the client according to the client's source address. 2. The server sends all of the sorted IP addresses of the egress interfaces to the client. 3. The client selects the optimal path. When the client connects to the server through a NAT device, this is the detection process: 1. The server recognizes the ISP type of the client according to the client's source address. 2. The server sends all of the sorted NAT IP addresses of the external interfaces to the client. 3. The client selects the optimal path.
NAT Mapping Address and Port	If necessary, in the NAT mapping address and port section, specify the mapped public IPs and ports of the server referenced in the DNAT rules of the DNT device. When the client connects to the server through the DNAT

Option	Description
	device, the NAT device will translate the destination address of the client to the server's egress interface address. Type the IP address of the NAT device's external interface and the HTTPS port number (You are not recommended to specify the HTTPS port as 443, because 443 is the default HTTPS port of WebUI management). You can configure up to 4 IPs (which can be IPv4 or IPv6 address).

In the Cluster IP Config tab, configure the corresponding options.

Option	Description
In the network environment that is in HA Peer mode, configure valid SSL VPN on both devices. When the primary device or its relevant links fails, the SSL VPN client can reconnect to the other primary device. You need to specify a reconnection address list. The SSL VPN client will attempt reconnection based on the priority of the addresses in the list. If reconnection fails, the client will cycle through the addresses in the list until a successful connection is made. You can specify up to four reconnection addresses, which are prioritized in the order they are listed (Server1 to Server4).	
Cluster IP/Port	Specifies the server address (which can be IPv4 address, IPv6 address, or domain name) and port number used for SSL VPN connection.

4. Click **Done** to save the settings.

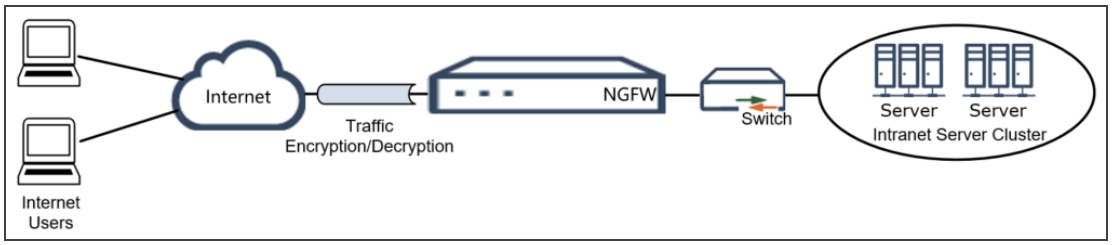
For more information, refer to the **VPN** > **SSL VPN** > **Configuring SSL VPN** in *StoneOS WebUI User Guide*. FR 41605

ZTNA Typical Scenarios

The typical scenarios of ZTNA include remote access and intranet access.

Remote Access

With the popularity of mobile office, the demand for remote access to intranet resources is growing. To meet this demand and ensure the security of intranet resources, Hillstone provides ZTNA remote access solution. This solution can control access traffic based on remote user identity, status of endpoint device, and access time. It uses fine-grained control policies to enable access to specific authorized applications, and continuously monitors changes in endpoint status to flexibly adjust the scope of authorized applications that users can access.



The user login process for the ZTNA remote access solution is as follows:

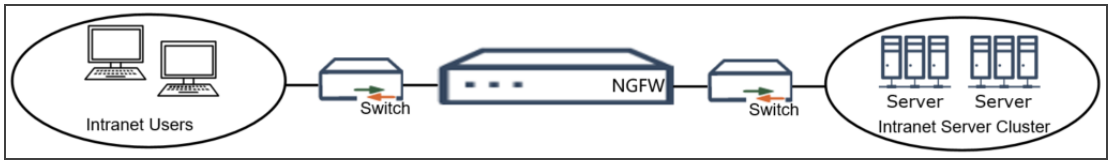
1. The ZTNA user enters the server address, port, authentication mode (username/password, username/password + digital certificate, digital certificate only, and third-party application login) on the client, and requests verification. If second-factor authentication is configured, the user needs to complete it.
2. After authentication is passed, the server sends a command to collect endpoint information to the client, assigns a private IP to the client, and establishes a secure tunnel between the server and the client.
3. The client executes the command to collect host information, such as the OS version, whether firewall is installed, antivirus software, browser security level, whether certain processes are running, etc., and reports them to the server.
4. The server parses the host information, obtains endpoint tags, and sends the username and endpoint tags to the authentication module to request the creation of an authenticated user.
5. The authentication module creates an authenticated user, associates it with endpoint tags, and obtains user group information.

6. Based on the username, user group, and endpoint tags, the server matches the ZTNA policy to determine the list of application resources that the client is allowed to access.

7. The ZTNA client pops up the Portal page, displaying the application resources that the user is allowed and not allowed to access, as well as the names and URLs of the application resources.

Intranet Access

The traditional network security concept assumes that the enterprise intranet is generally secure, and security threats mainly come from the outside. However, many significant security threats often occur within the intranet, such as employees inadvertently downloading malicious software while browsing the internet, posing serious security risks to the entire intranet. In addition, unauthorized access and unauthorized visits within the intranet may lead to business damage and information leakage. To address this issue, Hillstone provides the ZTNA intranet access solution. This solution can control traffic based on the identity of intranet users, status of endpoint device, and access time. It uses fine-grained control policies to enable access to specific authorized applications, and continuously monitors changes in endpoint status to flexibly adjust the scope of authorized applications that users can access.



Compared with the remote access solution, the devices in ZTNA intranet access solution do not need to encrypt and decrypt traffic, so no tunnel needs to be established. The user login process for the ZTNA intranet access solution is as follows:

1. The ZTNA user enters the server address, port, authentication mode (username/password, username/password + digital certificate, digital certificate only, and third-party application login) on the client, and requests verification. If second-factor authentication is configured, the user needs to complete it.

2. After authentication is passed, the server sends a command to collect endpoint information to the client.
3. The client executes the command to collect host information, such as the OS version, whether firewall is installed, antivirus software, browser security level, whether certain processes are running, etc., and reports them to the server.
4. The server parses the host information, obtains endpoint tags, and sends the username and endpoint tags to the authentication module to request the creation of an authenticated user.
5. The authentication module creates an authenticated user, associates it with endpoint tags, and obtains user group information.
6. Based on the username, user group, and endpoint tags, the server matches the ZTNA policy to determine the list of application resources that the client is allowed to access.
7. The ZTNA client pops up the Portal page, displaying the application resources that the user is allowed and not allowed to access, as well as the names and URLs of the application resources.

Configuring the ZTNA Server

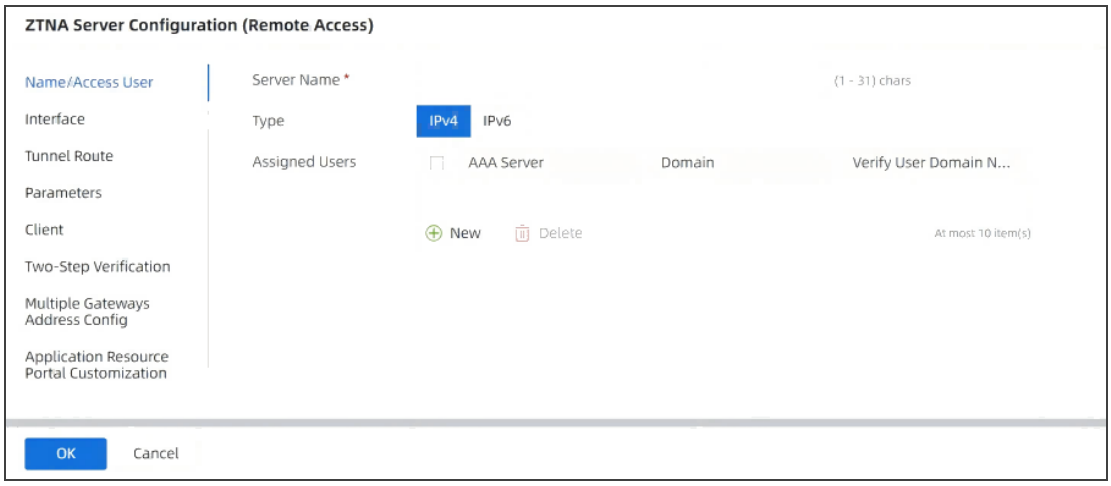
The configurations of the ZTNA server on the WebUI include:

- Configuring ZTNA Gateway
- Endpoint Tags
- Managing Endpoint Items
- Application Resource/Application Resource Group
- Address Pool
- ZTNA Policy

- ZTNA Portal
- Single Packet Authorization (SPA)

Configuring ZTNA Remote Access

1. Select **ZTNA** > **Gateway**.
2. Click **New** > **Remote Access**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
Server Name	Type the name of the ZTNA instance. The length is 1 to 31 characters.
Type	Select IPv4, IPv6, or Dual Stack to specify the service type of the ZTNA instance. The IPv6 and Dual Stack options are available only when the version is IPv6. **Related Concept:**Dual stack is a network technology that allows both IPv4 and IPv6 protocol stacks to run simultaneously on a network device, enabling seamless switching and communication between IPv4 and IPv6 networks.
Assigned Users (at most 10 items)	
AAA Server	Click **New** and select a AAA server from the **AAA Server** drop-down list. Or, you can click **New** in the drop-down list to create an AAA server. If you select an OAuth2 server, the client supports OAuth2 authentication. **Note**: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server. The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, the system will verify the user name and its domain name. **Note**: The OAuth2 server does not support user domain name verification.

In the Interface tab, configure the corresponding options.

Option	Description
Egress Interface	Specifies the interface used to listen to the request from ZTNA clients. Select the interface from the drop-down list. Or, click **New** in the drop-down list to create an interface. At most 8 interfaces can be selected.
Service Port	Specifies the ZTNA service port number. The value range is 1 to 65535.
Tunnel Interface	Specifies the tunnel interface for the ZTNA instance. Select a tunnel interface from the drop-down list. Or, click **New** in the drop-down list to create a tunnel interface.
IPv4 Address Pool	Specifies the ZTNA address pool. Select an address pool from the drop-down list. Or, click **New** in the drop-down list to create a new address pool. • When configuring IPv4 ZTNA, you need to specify the IPv4 ZTNA address pool. • When configuring IPv6 ZTNA, you need to specify the IPv6 ZTNA address pool. • When configuring dual stack ZTNA, you need to specify both the IPv4 and IPv6 ZTNA address pools.
IPv6 Address Pool	

In the Tunnel Route tab, configure the following options.

Tunnel Route	
• When configuring IPv4 ZTNA, you need to specify the IPv4 tunnel route so that you can access IPv4 intranet resources. • When configuring IPv6 ZTNA, you need to specify the IPv6 tunnel route so that you can access IPv6 intranet resources. • When configuring dual stack ZTNA, you need to specify both the IPv4 and IPv6 tunnel routes so that you can access IPv4 and IPv6 intranet resources.	
A tunnel route created based on a network segment will be distributed to the ZTNA client. ZTNA client uses it to generate the route to the specified destination.	
New	Click **New** to add a route.
IP	Type the destination IP address.
Netmask	Type the netmask of the destination IP address.
Metric	Type the metric value. The value range is 1 to 9999.
Type	Sets the user type to **User Group** or **Role**.
User Group/Role	When the type is set to **User Group**, select the AAA server to which the user group belongs and the user group name from the drop-down list. Only users in this user group can access the specified network segment in the tunnel route. You can also click ⊕ and create a user group in the **User Group Configuration** panel. For more information, see Creating a User Group. When the type is set to **Role**, select the role name from the drop-down list. Only users corresponding to this role can access the specified network segment in the tunnel route. You can also click ⊕

Tunnel Route	
	and create a role in the **Role Configuration** panel. For more information, see Creating a Role.
Delete	Click **Delete** to delete the selected route.
Add Default Route	Click **Add Default Route** to add a default route with both the IP address and netmask being all 0.
Enable Dedicated ZTNA Tunnel	
Click the button to enable the dedicated ZTNA tunnel function. This way, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to ZTNA. **Notes:** • The client versions that support the dedicated ZTNA tunnel function include: the latest version of the ZTNA client for Windows, the latest version of the ZTNA client for macOS, the latest version of the ZTNA client for Linux, and the latest version of the ZTNA client for ChineseOS. • The dedicated ZTNA tunnel function cannot be used together with the domain route function. • After you enable the dedicated ZTNA tunnel function, we recommend that you do not configure a default route in the tunnel routing.	
Enable Domain Route	
After clicking the **Enable** button, the system will distribute the specified domain	

Tunnel Route	
names to the ZTNA client, and the client will generate the route to the specified destination according to the resolving results from the DNS. **Notes:** The domain route function cannot be used together with the dedicated ZTNA tunnel function.	
Maximum	Specifies the maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value range is 1 to 10000. The default value is 1000.
New	Click **New** to add the domain name to the list and you can add up to 64 domain names.
Domain	Specifies the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot. Both wildcards and a single top level domain, e.g. com and .com are not supported.
Delete	Click **Delete** to delete the selected domain name.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. The option **any** indicates one of TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If **TLSv1.2** or **any** is specified in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the TLSv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 – in oldcert.pfx – out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports TLSv1.2 protocol. **openssl pkcs12 – export – in cert.pem – out newcert.pfx – CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"**

	3. Import the newly generated .pfx format certificate into your browser or USB Key.
Trust Domain	Specifies the PKI trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation. The default value is trust_domain_default.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must configure this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the ZTNA tunnel. **NULL** indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm. The default value is AES.
Hash	Specifies the hash algorithm of the ZTNA tunnel. **NULL** indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm. The default value is MD5.
Compression	Specifies the compression algorithm of the ZTNA tunnel. By default, no compression algorithm is used.
Client Connection	
Allow Download Client from Browser	Select the check box of the client type to specify the allowed type of ZTNA client. By default, you are allowed to access the system with five types of ZTNA clients, which are ZTNA client for Windows, ZTNA client for Android, ZTNA client for iOS, ZTNA cli-

	ent for macOS, and ZTNA client for Linux. You can configure to access the system only via the specified types of ZTNA clients as needed.
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client.The value range is 1 minute to 25 hours. The default value is 30 minutes.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list. When the schedule takes effect, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • ZTNA users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple login	Click **Enable** to permit a user to log in from more than one place simultaneously.
Multiple login times	Specifies the number of simultaneous login with the same username. The value range is 0 to 99,999,999. The value 0 indicates that the number of simultaneous login times is not limited. The default value is 0.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.

DF-Bit	Specifies whether to permit packet fragmentation on the device forwarding the packets. The actions include: • Set - Forbids packet fragmentation. • Copy - Copies the DF value from the destination of the packet. It is the default value. • Clear - Permits packet fragmentation.
Port (UDP)	Specifies the UDP port number for the ZTNA connection. The value range is 1 to 65535.
Port (TCP)	Specifies the TCP port number for the ZTNA connection. The value range is 1 to 65535.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Specifies the ZTNA client types that are allowed to access. By default, the six types of ZTNA clients are allowed to access: Windows, macOS, Linux, ChineseOS, iOS, and Android. You can select one or more client types as required.
Change Password URL	Specifies the URL address where the user will be redirected to modify the password. The length is 0 to 255 characters.
Forgot Password URL	Specifies the URL address where the user will be redirected to reset the password. The length is 0 to 255 characters.
Redirect URL	This function redirects the client to the specified URL address after a successful authentication. The length is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding

	fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.- abc.- com/oa/- login.- do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+user-name=$GBUSER&password=$PWD, e.g., http://www.- 443 Chapter 7 VPN abc.- com/oa/- login.- do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.abc.com
Title	Specifies description for the redirect URL. The length is 0 to 31 characters. This title will appear as a client menu item.
Client Certificate Authentication	
Authentication	Enable this function to request client certificate authentication. There are two options available: • Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username and password. The USB Key certificate users also need to type the USB Key password. • Digital Certificate only - To pass the authentication,

	you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificate users also need to type the USB Key password. No username or user's password is required. When **Digital Certificate only** is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length 0 to 63 characters.
Trust Domain Subject&Username Checking CN Matching OU Matching	To configure the trust domain and the subject & username check function: 1. From the **Trust domain** drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed.

	2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU Matching** box to determine whether matches them. 3. You can click **New** to add more items. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Enable** to enable two-step verification. It means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS authentication, token authentication or email authentication after the username and password are entered. The user must enter the random verification code received in order to log in and access intranet resources.
Type	Specifies the verification type, including **SMS Authentication**, **Token Authentication** and **Email Authentication**: • SMS Authentication: Click **SMS Modem** or **SMS Gateway**

Option	Description
	to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Click **Token Authentication** and enter the prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Auth Type	Select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from the drop-down list. For more information about the SMS gateway, see SMS Gateway.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code, in minutes. The value range is 1 to 10. The default value is 10. If the user does not enter the SMS authentication code within the specified time and does not apply for a new code, ZTNA server will disconnect the user.
Sender Name	Specifies a message sender name to display in the message content. The length is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.

Option	Description
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8.
SMS Temple	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.
Sign Name	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the ALIYUNSMS.
Template Code	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the ALIYUNSMS.
Email Authentication	
Mail Server	Select an existing mail server from the drop-down list. Or, click **New** to create a mail server. For more information about the configuration of a mail server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code, in minutes. The value range is 1 to 10. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code,

Option	Description
	ZTNA server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8 . The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".
Multiple Gateways Address Config	
When the ZTNA service is enabled for multiple devices in the network, you can add the service addresses (egress interface addresses or domain names) of these devices to the gateway address list. When the client establishes a ZTNA connection with the device, it can select the address with the best link quality from the list to establish the connection. When the device is configured with a gateway address list, the client can enable gateway detection function to select the desired ZTNA gateway for connection.	
Name	Click **New** to add a gateway address configuration in the gateway address list. Enter the gateway name. The range is 1 to 31 char-

Option	Description
	acters. Up to 24 gateways can be configured. When you configure multiple gateways, the ZTNA configurations on the multiple gateways need to be the same as those on the master ZTNA gateway.
Gateway Address	Specifies the IPv4 address, IPv6 address, or domain name of multiple gateways. The range for a domain is 255 characters and the maximum length between the two periods (.) cannot exceed 63 characters.

2. Click **OK** to save the settings.

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Configuring ZTNA Gateway** > **Configuring ZTNA Remote Access** topic in *StoneOS WebUI User Guide*. FR 41605

Monitor

Select **ZTNA** > **Monitor** > **Summary** to enter the ZTNA monitor page.

……

Viewing and Managing Online Users

To manage and view the status information of all ZTNA online users, take the following steps:

1. Select **ZTNA** > **Monitor** > **User Status**.
    a. Login Time: indicates the login time of the online user;
    b. User Name: indicates the user name of the online user;
    c. AAA Server: indicates the AAA server name to which the online user belongs;
    d. ZTNA Server: indicates the ZTNA service name that the online user accesses;
    e. User IP(v4): indicates the IPv4 address of the online user that the ZTNA server assigns;

f. User IP(v6): indicates the IPv6 address of the online user that the ZTNA server assigns;

g. Endpoint Name: indicates the user endpoint name;

h. Endpoint IP: indicates the user endpoint IP address, i.e. the public IP address of the user;

i. OS: indicates the operating system of the user endpoint;

j. Endpoint Tag: indicates the endpoint tag associated with the online user;

k. Client Version Number: indicates that the version number of the ZTNA client used by the online user.

l. Allowed Application Resources: indicates the application resources that the online user is granted access;

m. Denied Application Resources: indicates the application resources that the online user is not granted access;

n. Upstream Speed: indicates the upstream speed of the online user;

o. Downstream Speed: indicates the downstream speed of the online user.

2. Click **Filter** to add filter conditions to view the detailed information of ZTNA online users that meet the filter conditions.

3. By selecting one or more users and clicking **Force Log Off**, you can force disconnecting a user with the ZTNA server.

Note: To view upstream and downstream speed statistics, make sure the ZTNA monitor function is enabled.

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Monitor** topic in *StoneOS WebUI User Guide*. FR 41605

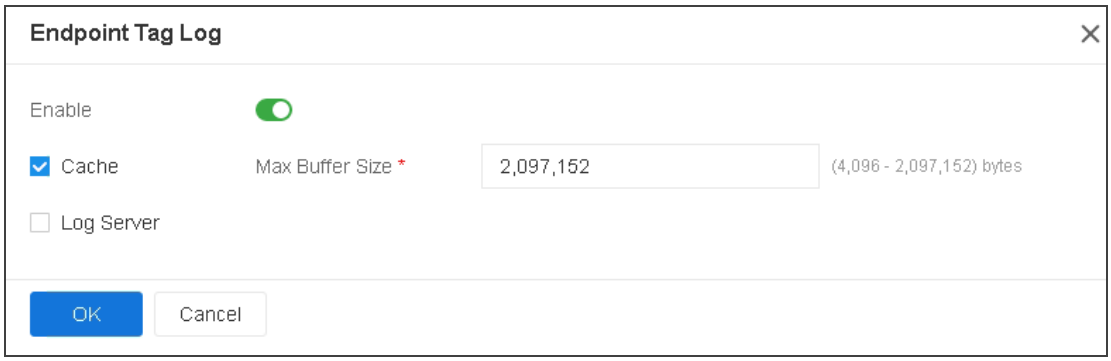
Endpoint Tag Log

The system support management of endpoint tag logs by using the endpoint tag log function. To configure and manage endpoint tag logs, take the following steps:

1. Select **Monitor** > **Log** > **Endpoint Tag Log** or select **ZTNA** > **Endpoint Tag Log**.

    - Time: indicates the endpoint tag log's generation time.
    - Type: indicates the endpoint tag log type, including login, logout, abnormal logout, endpoint tag update and application resource update.
    - User Name: indicates the user name.
    - User IP(v4): indicates the user IPv4 address.
    - User IP(v6): indicates the user IPv6 address.
    - AAA Server: indicates the AAA server to which the user belongs.
    - Endpoint Name: indicates the endpoint name.
    - Endpoint IP: indicates the endpoint IP address.
    - OS: indicates the operating system of the endpoint.
    - Endpoint Tags: indicates the endpoint tag associated with the user.
    - ZTNA Server: indicates the ZTNA service name that the user accesses.
    - Allowed Application Resources: indicates the application resources that the user are allowed to access.
    - Denied Application Resources: indicates the application resources that the user are not allowed to access.

2. Click **Configure** and enter the **Endpoint Tag Log** page.



Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Cache	Select the check box to send endpoint tag logs to the memory buffer.
Max Buffer Size	When configuring the system to send endpoint tag logs to the memory buffer, you can define the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Syslog Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "View Syslog Server" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Syslog Server.

3. Click **Filter** to view endpoint tag logs that match the specified filtering conditions.

4. Click **Clear** to clear all endpoint tag logs.

   Note: This option is not supported for devices that support sending log information to the local database.

5. Click **Export** to export all endpoint tag logs to a local file.

For more information, refer to the **Zero Trust Network Access (ZTNA) > Endpoint Tag Log** topic in *StoneOS WebUI User Guide*. FR 41605

Secure Connect Client Management

End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.
- To download and install Hillstone Secure Connect client for ChineseOS, search for "Hillstone Secure Connect" in the APP Store that comes with ChineseOS.

By default, the two addresses on the device and on the official website of Hillstone Networks use the same download source, and the downloaded Secure Connect client is also the same.

Hillstone Secure Connect Client for Windows

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for Windows v5.4.0 and later.

The SSL VPN/ZTNA client for Windows is Hillstone Secure Connect. It can run in the following operating systems:

- Windows7 SP1/Windows8.1/Windows10/Windows11
- Windows server 2008 R2/Windows server 2012/Windows server 2012 R2/Windows server 2016/Windows server 2019/Windows server 2022

The encrypted data can be transmitted between the client and the device after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC on which the client is running.
- Show the connecting status, statistics, interface information, and route information.
- Show log messages.
- Upgrade the client software.
- Resolve the resource list information received from the server.
- Collect and report endpoint device status information.

System supports IPv4 and IPv6 Secure Connect Windows clients.

This section mainly describes how to download, install, start, uninstall the Secure Connect Windows client, and gives instructions on how to use its GUI and menu. The device side supports the following authentication methods:

- Username/Password
- Username/Password + Digital Certificate (including USB Key certificate and file certificate)
- Digital Certificate (including USB Key certificate and file certificate) only
- Third-party Application Login (OAuth2 authentication)

Downloading and Installing the Client

Take either of the following methods to download and install the Secure Connect Windows client:

- Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.

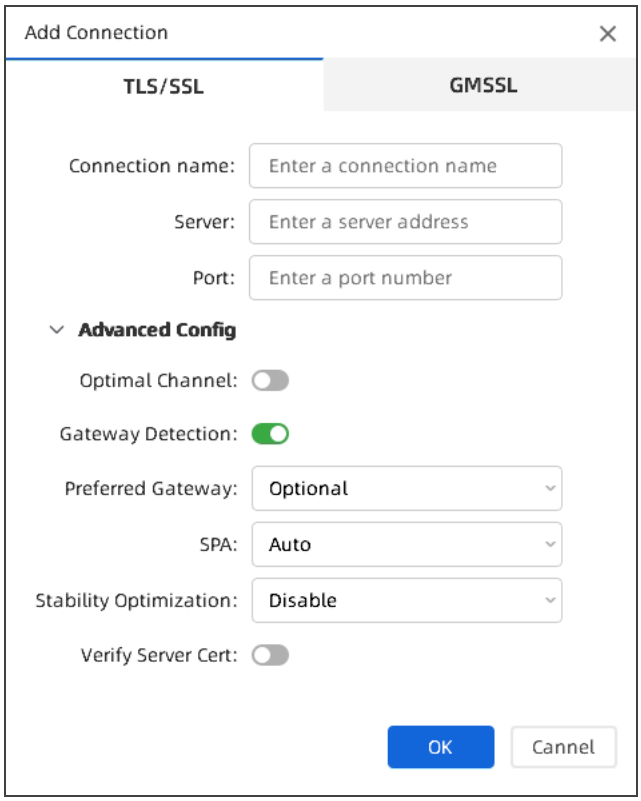
A virtual network adapter will be installed on your PC together with the Secure Connect Windows client. It is used to transmit encrypted data between the device and the client.

Starting Up and Connecting

After the Secure Connect Windows client is installed successfully, take the following steps to start and log in the client:

1. Double-click the shortcut of Hillstone Secure Connect on your desktop, or from the Start menu, choose **All Programs > Hillstone Secure Connect > Hillstone Secure Connect**. The client main page is displayed.

2. Click **Add Connection**. The following dialog box is displayed.



Enter the connection information.

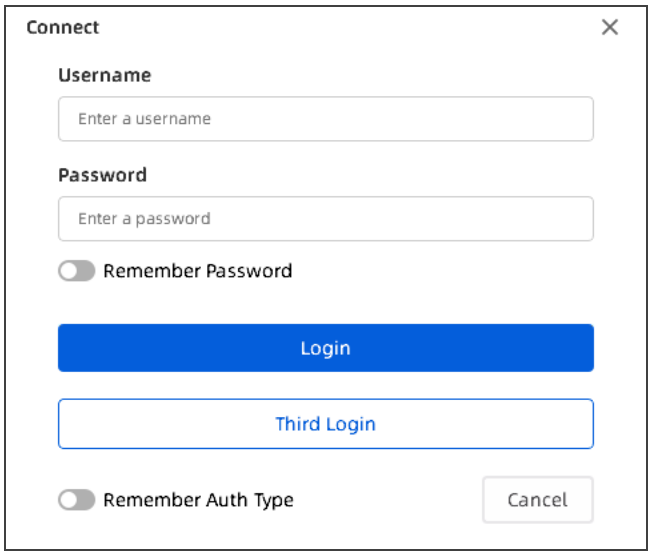
Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Advanced Config: By default, advanced configurations are hidden. You can click › to expand this section and configure the following options.	

Option	Description
Optimal Channel	Set whether to enable optimal path detection function. This function is used for the SSL VPN access function. When the optimal path detection is enabled on both the server and the client, clients connected from different ISP lines can automatically choose the fastest route to connect to the device of SSL VPN. By default, this function is disabled.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.

Option	Description
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. On the Connect dialog box, select an authentication type. The client will attempt to establish a connection to the device.
   The authentication type includes username/password, username/password+certificate, certificate, and third-party application login. If the access user on the device selects an OAuth2 server, OAuth2 authentication will be used as the third-party application login. In this case, you will be redirected to the OAuth2 authentication process: click the OAuth2 authentication icon, enter the OAuth2 authentication page, the browser will return the authentication result after the OAuth2 authorization and authentication complete, and a login status will be returned to the client.



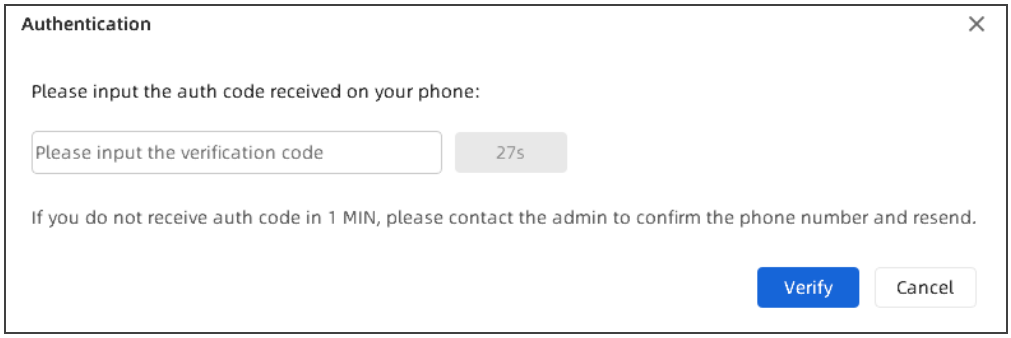
Option	Description
Username	Enter the name of the login user. When Auth type is specified as "Username" or "Username + Certificate", the client user name and password should be entered.

Option	Description
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Certificate	When the authentication type is "Username + Certificate" or "Certificate", click this option to enter the dialog box for selecting a certificate. The selected certificate will be sent to the device for authentication.
Select Digital Certificate	Options in the "Select Digital Certificate" dialog box are described as follows: • Default System Certificate: Click this radio button to allow the device to use the Hillstone UKey certificate as the system default certificate. This is the default setting. • USBKey Certificate: Click this radio button and select a USB-Key certificate from the current certificate list. The USB Key should be inserted into the USB interface of the PC in advance. You can use the USB Key deployment tool named SelectUSBKey to set the third-party certificate as the default certificate. For more information, refer to Third-Party USB Key. • File Certificate: Click this radio button and select a file certificate from the current certificate list. The file certificate should be imported into the PC in advance. • Certificate list: Display the existing certificate in the system. Click **Refresh** icon to update the list.

Option	Description
GMSSL certificate	Options in the "GMSSL certificate" dialog box are described as follows: • Device Name: Select the current USB Token device name in the drop-down list. The USB Token device should be inserted into the USB interface of the PC in advance. • Application Name: The application is a structure that contains a container, a device authentication key, and a file. Select the specified application name in the drop-down list. • Container Name: The container is the unique storage space in the USB Token device to save the key. It is used to store the encryption key pair, the encryption certificate corresponding to the encryption key pair, the signature key pair, and the signature certificate corresponding to the signature key pair. Select the name of the specified container in the drop-down list. • Signature certificate: Display the name of the SM2 signature certificate in the specified container. • Encryption certificate: Display the name of the SM2 encryption certificate in the specified container.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/Password + Digital certificate" or "Only Digital certificate".
Remember	After this option is enabled, you do not need to enter the PIN at

Option	Description
PIN	the next-time connection.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Remember Auth Type	after this option is selected, this authentication type will be directly used upon next connection. By default, this option is selected. If you disable this function, you need to select an authentication type again upon next connection. **Note**: When the authentication type on the device changes, if the remembered authentication type is not included in the changed authentication type, you will be prompted that the authentication type is different from that on the device upon your next connection. In this case, you need to select an authentication type again.

5. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog (as shown below) and click **Verify**. If you have not received the authentication code within one minute, you can re-apply by clicking **Resend**.



6. If token authentication is enabled on the device side, the token Authentication dialog will appear. You need to pass the token authentication.

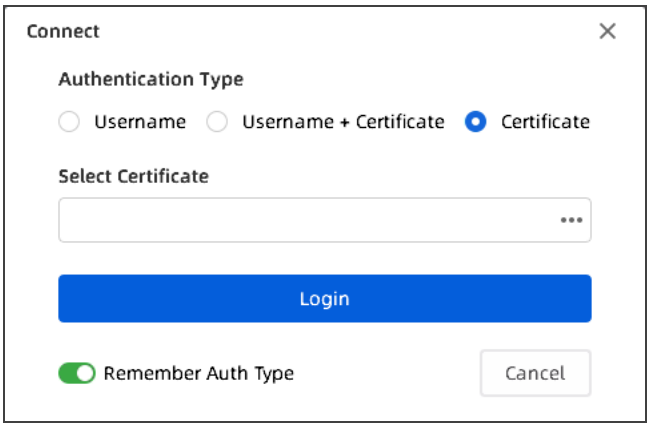
- After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
- You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

7. If Email authentication is enabled on the device side, the Email Authentication dialog will appear. You need to pass the Email authentication.
    - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
    - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

- If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.
- After "OAuth2 authentication is successful" is displayed on the browser, you may not successfully log in to the SSL VPN/ZTNA client. There may be scenarios where the IP address is occupied. Please check the reason for failure on the client.

- If secondary authentication is enabled on the device and OAuth2 authentication is supported, secondary authentication will not be performed when the client uses the third-party application login for connection.
- When you select the third-party application login, if you do not perform authentication operation after the browser pops up, the client will prompt authentication timeout after 10 minutes.
- To roll back the client to an earlier version, you need to uninstall the current version before installing the earlier version. You cannot directly overwrite the existing version. Otherwise, an error about the connection configuration will appear and the connection will fail.
- When the client automatically reconnects, you need to perform OAuth2 authentication again.
- When you connect to the device (R10F4 and later F versions, R11 and later versions) that supports OAuth2 authentication, the client page returns the authentication type configured on the device. For example, if the device is configured with username/password and OAuth2 authentication, the **Connect** page on the client displays the "Username/Password" and "Third Login" authentication types.
- When you connect to the device (version that is earlier than R10F4) that does not support the OAuth2 authentication, the **Connect** page on the client displays three authentication types by default. For example, if the device is configured with the certificate authentication only, you need to select Certificate on the Connect page so that the connection can be successful, as

shown below:



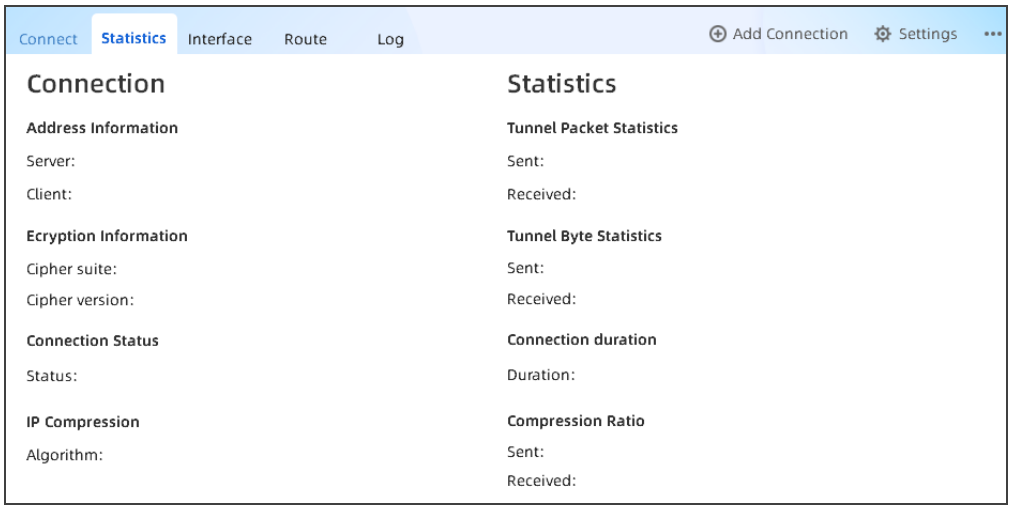
Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the icon ( ) will be displayed in the notification area. And the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the icon to edit the entry; and the icon to delete the entry.

Viewing Connection and Statistics Information

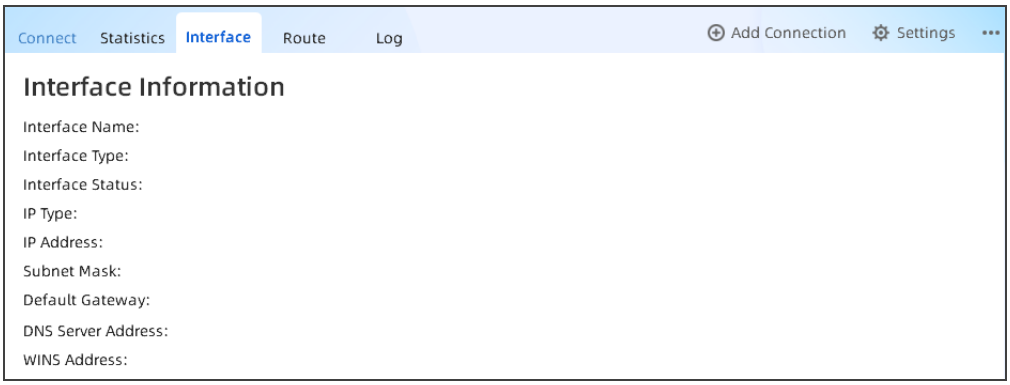
On the client main page, click the **Statistics** tab to view connection and statistics information.



Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.
Received	The number of received packets through the encryption tunnel.
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** > **IPv4 Route** or **Route** > **IPv6 Route** tab to view IPv4 or IPv6 routing information.



Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Address	The IPv4 address (allocated by the server) of the interface used to send encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Server Address	The address of the DNS server used by the client, which is an IPv4 address.
IPv4 WINS Address	The address of the WINS server used by the client, which is an IPv4 address.

Option	Description
When the user on the client is connected to the IPv6 or dual stack server, the following information is displayed:	
IPv6 Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

Hillstone Secure Connect Client for Android

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for Android v5.2.0 and later.

The SSL VPN/ZTNA client for Android is Hillstone Secure Connect. It can run in Android 8.x/Android 9.x/Android 10.x/Android 11.x/Android 12.x/Android 13.x/HongmengOS 2.0. The functions of Secure Connect Android client contain the following items:

- Obtain the interface information of the Android OS.
- Display the connection status with the device, traffic statistics, interface information, and routing information.
- Display the log information of the application.
- Collect and report endpoint status information.

Downloading and Installing the Client

To download and install the Secure Connect Android client, take the following steps:

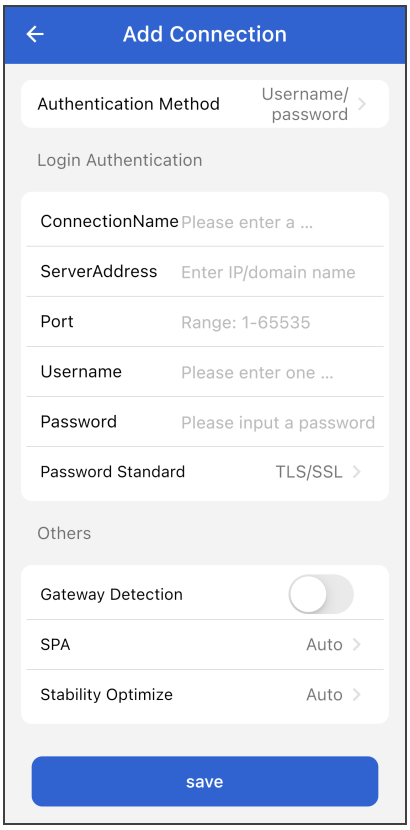
1. Visit https://www.hillstonenet.com/more/services/product-downloads/ to download the installation file of the client, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. Use the Android device to scan the QR code of the Secure Connect Android client.
3. Open the URL and download the Hillstone-Secure-Connect-Versione_Number.apk file.
4. After downloading successfully, find this file in the Android device.
5. Click it and the installation starts.
6. Read the permission requirement.
7. Click **Install**.

Starting Up and Connecting

After the Secure Connect Windows client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.

2. In the "Home" tab, click "+" and enter the "Add Connection" page.



Enter the connection information.

Option	Description
Authentication Method	Select the authentication method. "User name/password", "User name/password + Digital Certificate" and "Digital Certificate" are supported.
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Username	Enter the name of the login user. When authentication method is

Option	Description
	specified as "User name/password" or "User name/password + Digital Certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/password + Digital certificate" or "Digital certificate".
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Select Certificate	Select the digital certificate that has been imported into the Android device in advance.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client

Option	Description
	will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
Single Packet Authentication	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires

Option	Description
	single packet authorization and knocks on the default knock port number.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.

If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS authentication, token authentication or email authentication is enabled, you need to enter the corresponding authentication code to complete the authentication.

After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit a login entry, click the icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Network	The IPv4 address (allocated by the server) of the interface used to send

Option	Description
Address	encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Address	The address of the DNS server used by the client, which is an IPv4 address.
When the user on the client is connected to the IPv6 or dual stack server, the following information is displayed:	
IPv6 Network Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

Hillstone Secure Connect Client for iOS

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for iOS v5.2.0 and later.

The SSL VPN/ZTNA client for iOS is Hillstone Secure Client. It supports iOS 12.x/iOS 13.x/iOS 14.x/iOS 15.x/iOS 16.x versions. The Secure Connect iOS client mainly has the following functions:

- Simplify the tunnel creation process between the iOS device and the Hillstone device
- Display the connection status between the iOS device and the Hillstone device

- Display the log information
- Collect and report endpoint device status information.

Downloading and Installing the Client

You can take either of the following methods to download and install the Secure Connect iOS client:

- Search Hillstone Secure Client(beta) in the App Store.
- Visit https://www.hillstonenet.com/more/services/product-downloads/, locate the QR code for iOS client, use the iOS device to scan the code and then jump to App Store for downloading and installation.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance

Starting Up and Connecting

After the client is installed successfully, for the first time login, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.
2. In the "Home" tab, click "+" and enter the "Add Connection" page.

   Enter the connection information.

Option	Description
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.

Option	Description
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection

Option	Description
	fails, the ZTNA client will switch to connect the gateway with the best link quality.
Single Packet Authentication	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires single packet authorization and knocks on the default knock port number.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.

If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after

the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS, token or email authentication is enabled, type the corresponding code to complete the authentication.
6. After login, the iOS device will start the VPN configuration deployment automatically. In the **Would Like to Add VPN Configurations** page, click **Allow**.
7. Enter your passcode. The passcode is the one for unlocking your iOS screen. With the correct passcode entered, the iOS device starts to install the profile.
8. After the installation is complete, start **Settings** of the iOS device and navigate to **VPN**.
9. Select the configured connection name and click the **Connect** button.
10. After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Notes: For subsequent logins, you do not need to perform the VPN configuration deployment steps. You can log in the client and start the connection directly.

Editing and Deleting Login Entry

To edit a login entry, click the  icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Network	The IPv4 address (allocated by the server) of the interface used to send

Option	Description
Address	encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Address	The address of the DNS server used by the client, which is an IPv4 address.
When the user on the client is connected to the IPv6 or dual stack server, the following information is displayed:	
IPv6 Network Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

Hillstone Secure Connect Client for macOS

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for macOS v5.4.0 and later.

The SSL VPN/ZTNA client for macOS is Hillstone Secure Connect. It can run in macOS 10.13/macOS 10.14/macOS 10.15/macOS 11.0/macOS 12.0/macOS 13.0 versions. The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Establish the encrypted connection with the SSL VPN/ZTNA server.
- Show the connection status, traffic statistics, and route information.

- Show log messages.
- Collect and report endpoint device status information.

Downloading and Installing the Client

To download and install the Secure Connect macOS client, take the following steps:

1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/ or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, double-click it. In the pop-up, drag the Secure Connect macOS client to the **Applications** folder to perform the installation.



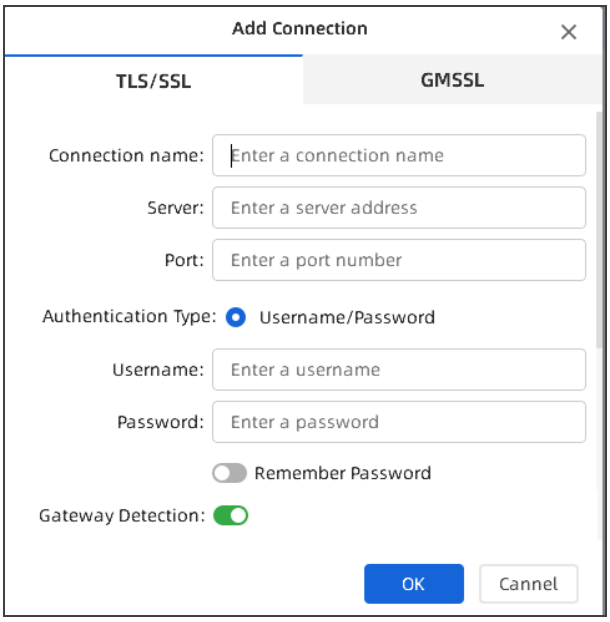
Notes: To open the installation file, you must have the administrator permission and select **Anywhere in System Preferences > Security & Privacy > General > Allow apps downloaded from**.

Starting Up and Connecting

After the Secure Connect macOS client is installed successfully, take the following steps to start and log in the client:

1. Select **Launchpad > Hillstone Secure Connect**. The client starts.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Authentication Type	The authentication type is username/password.
Username	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication

Option	Description
	server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number,

Option	Description
	ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is

different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous step to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.

5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

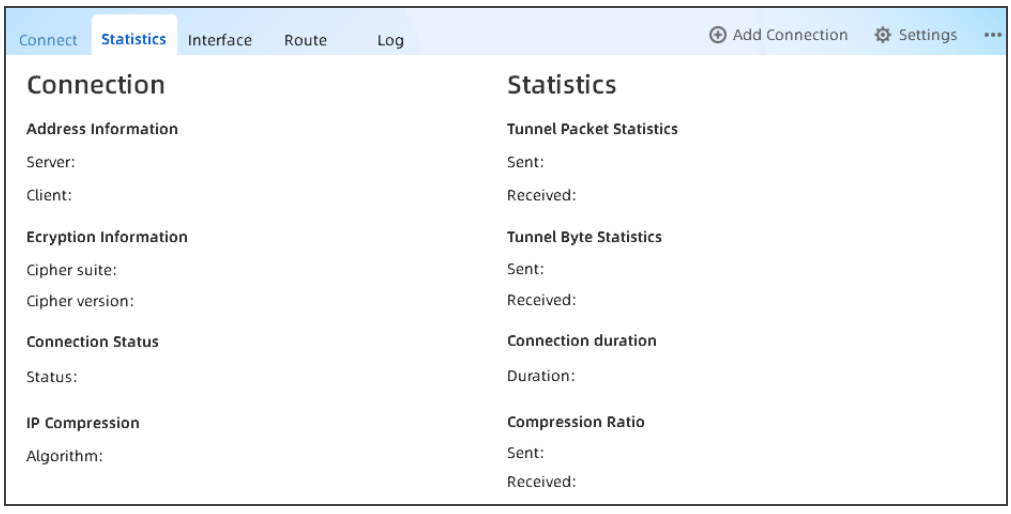
Finishing the above steps, the client will connect to the server automatically.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

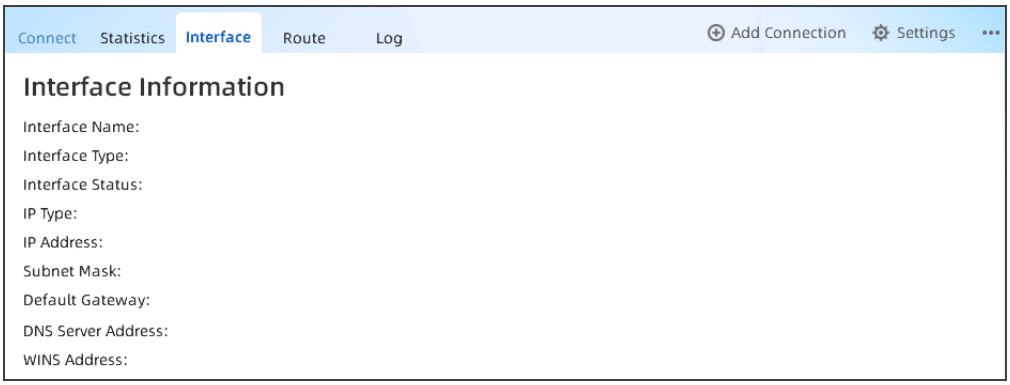
On the client main page, click the **Statistics** tab to view connection and statistics information.



Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packets	
Send	The number of sent packets through the encryption tunnel.
Received	The number of received packets through the encryption tunnel.
Tunnel Bytes	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** > **IPv4 Route** or **Route** > **IPv6 Route** tab to view IPv4 or IPv6 routing information.



Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Address	The IPv4 address (allocated by the server) of the interface used to send encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Server Address	The address of the DNS server used by the client, which is an IPv4 address.
IPv4 WINS Address	The address of the WINS server used by the client, which is an IPv4 address.
When the user on the client is connected to the IPv6 or dual stack server, the following	

Option	Description
information is displayed:	
IPv6 Network Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

Hillstone Secure Connect Client for Linux

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for Linux v5.4.0 and later.

The SSL VPN/ZTNA client for Linux is Hillstone Secure Connect. It can run in the following operation systems:

- CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5
- Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04
- Ubuntu Kylin 18.04/20.04

The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC in which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint status information.

Take CentOS 7.6 as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other three Linux systems can refer to 64-bit Ubuntu Kylin16.04 desktop.

Downloading and Installing the Client

To download and install the Secure Connect Linux client, take the following steps:

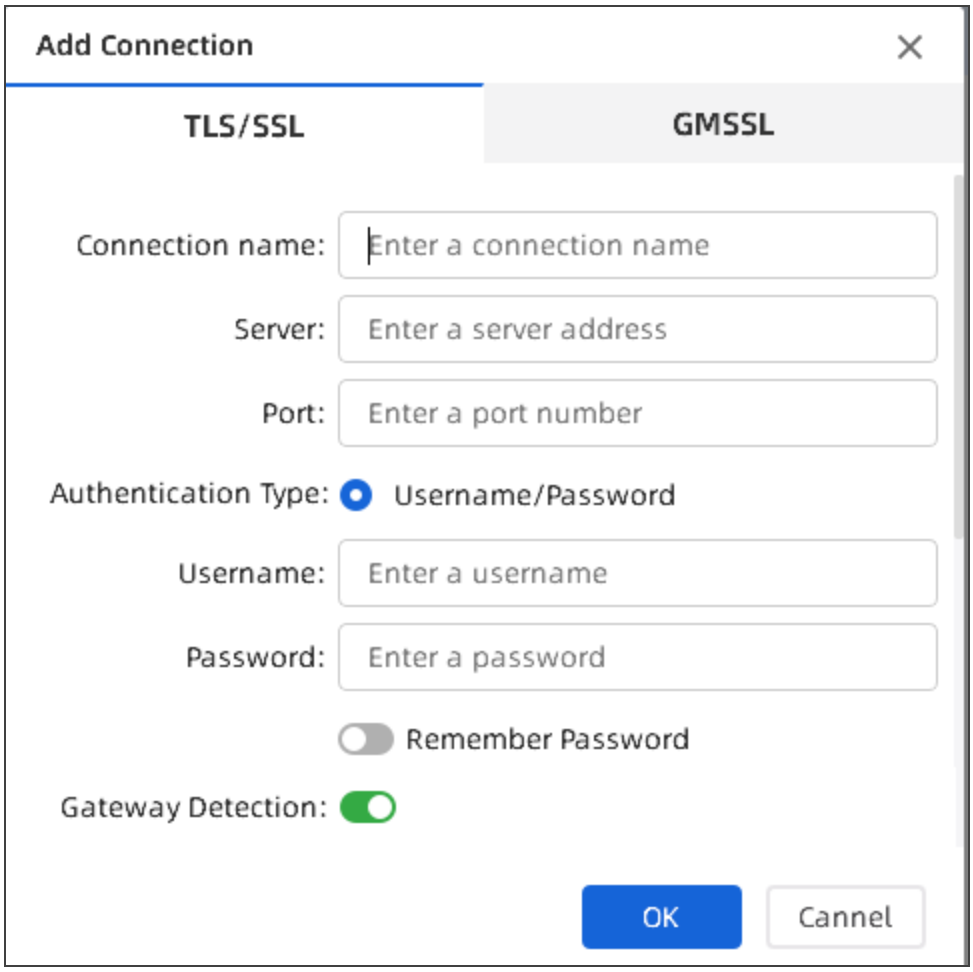
1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, right-click the client icon and select **Properties** to go to the properties page. In the properties page, click **Permissions** tab and check **Allow executing files as program**, then close it.
3. Double-click the client icon and follow the setup wizard to complete the installation.

Starting Up and Connecting

After the Secure Connect Linux client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on your desktop. The client main page is displayed.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.

Option	Description
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is enabled, you do not need to enter the user's password at the next-time connection.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the

Option	Description
	best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please

Option	Description
	refer to General Configuration.

If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.
5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

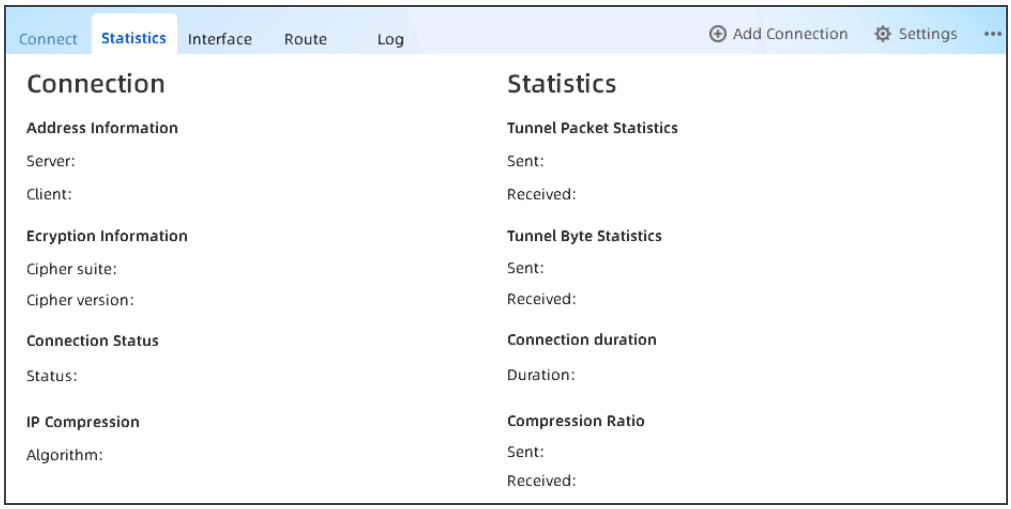
After the client connects to the SSL VPN/ZTNA server, the encrypted data can be transmitted between the client and the server now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

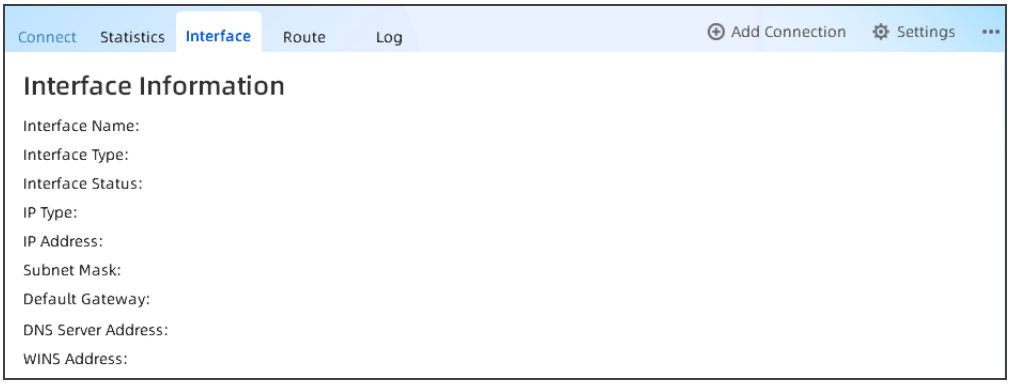


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compression	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.
Received	The number of received packets through the encryption tunnel.

Address Information: Shows the IP addresses	
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Receive	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** > **IPv4 Route** or **Route** > **IPv6 Route** tab to view IPv4 or IPv6 routing information.



Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.

Option	Description
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Address	The IPv4 address (allocated by the device) of the interface used to send encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Server Address	The address of the DNS server used by the client, which is an IPv4 address.
IPv4 WINS Address	The address of the WINS server used by the client, which is an IPv4 address.
When the user on the client is connected to the IPv6 or dual stack server, the following information is displayed:	
IPv6 Network Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

Hillstone Secure Connect Client for ChineseOS

Dual stack SSL VPN/ZTNA instances can be connected to Secure Connect Client for ChineseOS v5.4.0 and later.

The SSL VPN/ZTNA client for ChineseOS is Hillstone Secure Connect. It can run in the following operation systems:

- UOS 20 (CPU HiSilicon Kirin)
- Kylin V10 (CPU Zhaoxin)
- UOS 20 (CPU Feiteng)
- Kylin V10 (CPU HiSilicon Kirin)
- Kylin V10 (CPU Loongson)
- UOS 20 (CPU Loongson)

Hillstone Secure Connect Client for ChineseOS will be supported in Kylin V10 (CPU Feiteng) and UOS 20 (CPU Zhaoxin) later.

The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC in which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint status information.

This section mainly describes how to download, install, start, uninstall Secure Connect Client for ChineseOS, and gives instructions on how to use its GUI and menu. The device side supports the following authentication methods:

- Username/Password
- Username/Password + Certificate
- Certificate
- Third-party Application Login (OAuth2 Authentication)

Take UOS 20 as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other ChineseOS systems is similar.

Downloading and Installing the Client

To download and install the Secure Connect ChineseOS client, take the following steps:

1. Visit the APP Store that comes with ChineseOS and search for the Hillstone Secure Connect client.
2. Click **Install** to install the client. After the client is installed, the **Open** button is displayed. You can click **Open** to start up the client.

Starting Up and Connecting

After the Secure Connect ChineseOS client is installed successfully, take the following steps to start and log in the client:

1. In the **Start** menu, click **Hillstone Secure Connect**. You can also right-click **Hillstone Secure Connect** to add a shortcut or fix the client to taskbar.
2. Click **Add**.

   Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.

Option	Description
Advanced Config: By default, advanced configurations are hidden. You can click › to expand this section and configure the following options.	
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA server has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA server has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single

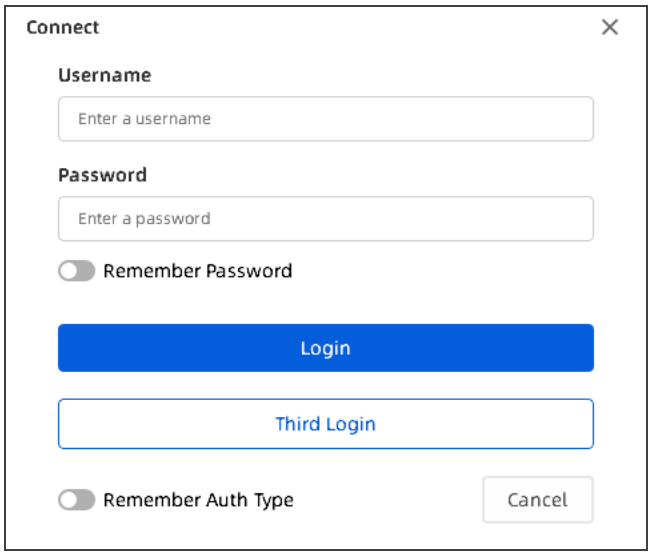
Option	Description
	packet authorization before establishing a connection to the ZTNA server. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA server, the ZTNA server will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA server, clients consider that the ZTNA server requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. On the Connect dialog box, select an authentication type and log in.

The client will attempt to establish a connection to the device.

The authentication type includes username/password, username/password+certificate, certificate, and third-party application login. If the access user on the device selects an OAuth2 server, OAuth2 authentication will be used as the third-party application login. In this case, you will be redirected to the OAuth2 authentication process: click the OAuth2 authentication icon, enter the OAuth2 authentication page, the browser will return the authentication result after the OAuth2 authorization and authentication are completed, and a login status will be returned to the client.



Option	Description
Username	Enter the name of the login user. When Auth type is specified as "Username" or "Username + Certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Certificate	When the authentication type is "Username + Certificate" or

Option	Description
	"Certificate", click this option to enter the dialog box for selecting a certificate. The selected certificate will be sent to the device for authentication.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Remember Auth Type	after this option is selected, this authentication type will be directly used upon next connection. By default, this option is selected. If you disable this function, you need to select an authentication type again upon next connection. **Note**: When the authentication type on the device changes, if the remembered authentication type is not included in the changed authentication type, you will be prompted that the authentication type is different from that on the device upon your next connection. In this case, you need to select an authentication type again.

5. If SMS authentication, token authentication, or Email authentication is enabled, type the corresponding authentication code to pass the secondary authentication.

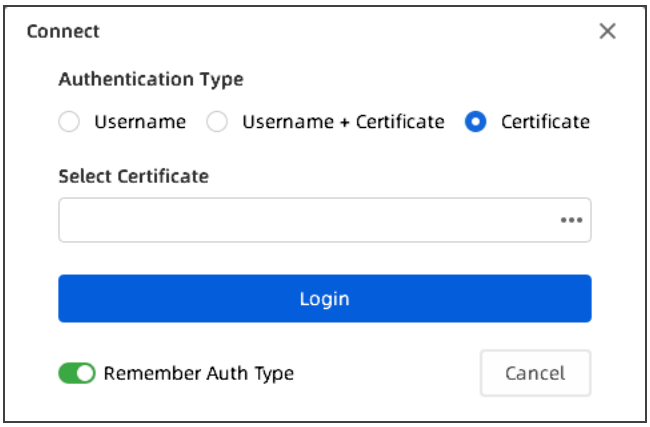
6. Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the encrypted communication between the client and server can be implemented now.

    - If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about

password control function, refer to Configuring a Local AAA Server.

- After "OAuth2 authentication is successful" is displayed on the browser, you may not successfully log in to the SSL VPN/ZTNA client. There may be scenarios where the IP address is occupied. Please check the reason for failure on the client.
- If secondary authentication is enabled on the device and OAuth2 authentication is supported, secondary authentication will not be performed when the client uses the third-party application login for connection.
- When you select the third-party application login, if you do not perform authentication operation after the browser pops up, the client will prompt authentication timeout after 10 minutes.
- To roll back the client to an earlier version, you need to uninstall the current version before installing the earlier version. You cannot directly overwrite the existing version. Otherwise, an error about the connection configuration will appear and the connection will fail.
- When the client automatically reconnects, you need to perform OAuth2 authentication again.
- When the client is connected to the device (R10F4 and later F versions, R11 and later versions) that supports OAuth2 authentication, the client page returns the authentication type configured on the device. For example, if the device is configured with username/password and OAuth2 authentication, the **Connect** page on the client displays the "Username/Password" and "Third Login" authentication types.
- When the client is connected to the device (version that is earlier than R10F4) that does not support the OAuth2 authentication, the **Connect** page on the client displays three authentication types by default. For example, if the device is configured with the certificate authentication only, you need to select Certificate on the Connect page so that

the connection can be successful, as shown below:

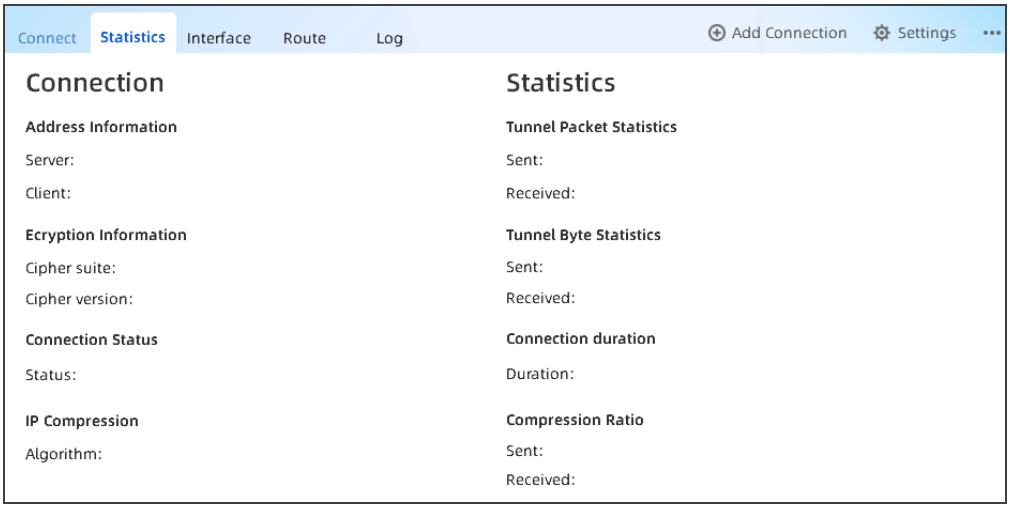


Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the icon to edit the entry; and the icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

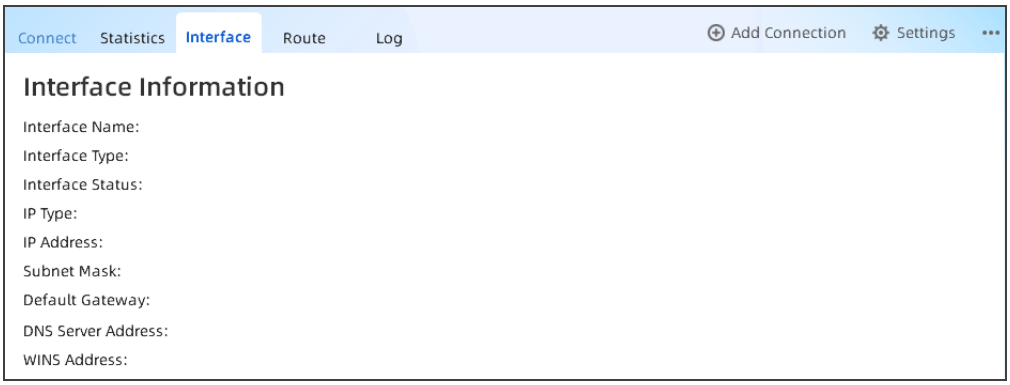


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.

Address Information: Shows the IP addresses	
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.
Received	The number of received packets through the encryption tunnel.
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** > **IPv4 Route** or **Route** > **IPv6 Route** tab to view IPv4 or IPv6 routing information.



Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
When the user on the client is connected to the IPv4 or dual stack server, the following information is displayed:	
IPv4 Address	The IPv4 address (allocated by the server) of the interface used to send encrypted data.
IPv4 Subnet Mask	The IPv4 subnet mask of the interface used to send encrypted data.
IPv4 DNS Server Address	The address of the DNS server used by the client, which is an IPv4 address.
IPv4 WINS Address	The address of the WINS server used by the client, which is an IPv4 address.

Option	Description
When the user on the client is connected to the IPv6 or dual stack server, the following information is displayed:	
IPv6 Network Address	The IPv6 address (allocated by the server) of the interface used to send encrypted data.
IPv6 Prefix Length	The IPv6 prefix length of the interface used to send encrypted data.
IPv6 DNS Server Address	The address of the DNS server used by the client, which is an IPv6 address.

For more information, refer to the **VPN > SSL VPN > Secure Connect Client** or **Zero Trust Network Access (ZTNA) > ZTNA Client** topic in *StoneOS WebUI User Guide*. FR 41605

CLI

Configuring SSL VPN Server

This section describes the following configurations about SSL VPN server:

- Configuring an IPv4 Access Address Pool
- Configuring an IPv6 Access Address Pool
- Configuring Resources List
- Configuring a UDP Port
- Configuring an SSL VPN Instance
- Binding the SSL VPN Instance to a Tunnel Interface
- Authentication Using UKey Certificate
- Two-Step Verification

- Host Binding
- Host Check
- Optimal Path Detection
- Force Disconnecting an SSL VPN Client
- Allowing Password Change by Local Users
- Configuring Change Password URL of the Client
- Configuring Forgot Password URL of the Client
- Configuring SSL Cipher Suite
- Exporting and Importing a User-list File
- Control the Access by Using the Radius Server
- Configuring the Allowed Client Types
- General Configuration

Configuring an SSL VPN Instance

To create an SSL VPN instance, in the global configuration mode, use the following command:

tunnel scvpn *instance-name*

- *instance-name* – Specifies a name for the SSL VPN instance.

This command creates an SSL VPN instance and leads you into the SSL VPN instance configuration mode; if the instance exists, you will enter the SSL VPN instance configuration mode directly.

To delete an SSL VPN instance, in the SSL VPN instance configuration mode, use the following command:

no tunnel scvpn*instance-name*

This section describes how to configure an SSL VPN instance, including:

- Specifying the service type
- Specifying an access address pool
- Specifying a server interface
  ……
- Configuring an SSL VPN tunnel route
  ……
- Using SSL VPN in HA peer mode
  ……

Specifying the Service Type

By default, the service type of SSL VPN instanse is IPv4. You can specify the service type of the SSL VPN instance, including IPv4, IPv6, or dual stack. The IPv6 and dual stack types are available only when the system version is IPv6. In the SSL VPN instance configuration mode, use the following command:

service-type {**ipv4** | **ipv6** |**dual-stack**}

- **ipv4** | **ipv6** | **dual-stack** – Specifies the service type of the SSL VPN instance, including IPv4, IPv6, or dual stack.

  Related Concept:

  Dual stack is a network technology that allows both IPv4 and IPv6 protocol stacks to run simultaneously on a network device, enabling seamless switching and communication between IPv4 and IPv6 networks.

Specifying a Server Interface

The client uses HTTPS protocol to access to the server. To specify the SSL VPN interface of the server, in the SSL VPN instance configuration mode, use the following command:

interface*interface-name*

- *interface-name* – Specifies the name of the interface for the SSL VPN client to connect.

To cancel the SSL VPN interface, in the SSL VPN instance configuration mode, use the following command:

no interface *interface-name*

Configuring an SSL VPN Tunnel Route

To reach the destination network segment or destination domain name through SSL VPN tunnel, you need to specify them by configuring the SSL VPN tunnel route.

- The specified destination network segment will be distributed to the VPN client, then the client uses it to generate the route to the specified destination.
- The specified destination domain name will be distributed to the VPN client, and the client will generate the route to the specified destination according to the resolving results from DNS.

Notes: When you configure dual stack SSL VPN, you need to specify both the IPv4 and IPv6 SSL VPN tunnel routes.

Configuring an IPv4 Tunnel Route to the Specified Network Segment

You can only specify the IPv4 or dual stack SSL VPN tunnel route for the IPv4 SSL VPN instance. To reach the destination network segment through SSL VPN tunnel, in the SSL VPN instance configuration mode, use the following command:

split-tunnel-route*ip-address/netmask* [**metric***metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination network segment.

- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

To delete a route, in the SSL VPN instance configuration mode, use the following command:

no split-tunnel-route*ip-address/netmask* [**metric***metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

Configuring an IPv6 Tunnel Route to the Specified Network Segment

You can only specify the IPv6 or dual stack SSL VPN tunnel route for the IPv6 SSL VPN instance. To reach the destination network segment through SSL VPN tunnel, in the SSL VPN instance configuration mode, use the following command:

split-tunnel-route-ipv6*ipv6-address/prefix* [**metric***metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ipv6-address/prefix* – Specifies the IPv6 address and network mask of the destination network segment.
- **metric** *metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.

- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

To delete a route, in the SSL VPN instance configuration mode, use the following command:

no split-tunnel-route-ipv6*ipv6-address/prefix* [**metric***metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

Using SSL VPN in HA Peer Mode

In the network environment using HA peer mode, configure SSL VPN in both Hillstone devices. When one device or its relevant links are down, the SSL VPN client can re-connect to the other device. You need to configure the reconnection address table. The SSL VPN client will re-connect to the SSL VPN server according to the priority of the reconnection address. If the SSL VPN client fails to re-connect to the server, it will try every address in the reconnection address table until it can connect to the server. You can at most specify four reconnection address, , which are prioritized in the order they are listed (Server1 to Server4).

To configure the reconnection address table, use the following command in the SSL VPN instance configuration mode:

cluster {**server1** |**server2** | **server3** | **server4**} *address* [**port***port-number*]

- {**server1** |**server2** | **server3** | **server4**} *address* – Specifies the IPv4 address, IPv6 address, or domain name of the SSL VPN server.

- **port***port-number* – Specifies the port number that the SSL VPN server used. The default port is 4433.

To delete the reconnection address table, use the following command in the SSL VPN instance configuration mode:

no cluster [**server1** | **server2** | **server3** | **server4**]

- **no cluster** - Delete all reconnection addresses.
- **server1** | **server2** | **server3** | **server4** - Delete the specified reconnection address.

When using this new function, note the following matters:

- If you select the **Auto Reconnect** option in the SSL VPN client and use the **client-auto-connect count** command to set the reconnection times as unlimited, the SSL VPN client will only re-connect to the originally configured server, and will not re-connect to the server specified in the reconnection address table. If you set the reconnection times as X, the SSL VPN client will re-connect to the server in the table after X times of failed attempts to the originally configured server.
- If you does not select the **Auto Reconnect** option in the SSL VPN client, the SSL VPN client will directly re-connect to the server you specified in the reconnection address table
- When using the firmware that supports the using of SSL VPN in HA peer mode, the SSL VPN whose version is lower than 1.4.4.1207 can connect to the SSL VPN server if the server has no reconnection address table configured. StoneOS will inform the users to update the SSL VPN client. If the server has configured the reconnection address table, the SSL VPN whose version is lower than 1.4.4.1207 cannot connect to SSL VPN server. You need to uninstall the client and login to the SSL VPN Web Login page to download the new version of the SSL VPN client. Then install the new version. The new version is compatible with the firmware that does not support this new function.

Selecting an Optimal Path

To specify an interface as SSL VPN tunnel egress interface, in the SSL VPN instance configuration mode, use the following command:

interface *interface-name*

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

Repeat this command to specify more interfaces (up to two) as the tunnel egress interface.

To cancel the specified tunnel interface, in the SSL VPN instance configuration mode, use the following command:

no interface*interface-name*

To configure the optimal path selection, in the SSL VPN instance configuration mode, use the following command:

link-select { **mode** {**client-detect** | **server-detect**} | {**addr1** | **addr2** | **addr3** | **addr4**} *address* [**port***port-number*]}

- **mode** {**client-detect** | **server-detect**} - Specifies the mode of the optimal link detection. **client-detect** indicates that the client detects the optimal link and **server-detect** indicates that the server detects the optimal link. By default, the client selects link spontaneously.
- {**addr1** | **addr2** | **addr3** | **addr4**} *address* - Specifies the Internet interface IP address of DNAT device. The system allows up to four IP addresses, which can be IPv4 or IPv6 address.
- **port** *port-number* – Specifies the HTTPS port number of the DNAT Internet interface. The value range is 1 to 65535. The default value is 4433. To avoid collision with WebUI HTTPS port number, you are not recommended to use port 443.

To cancel optimal link selection, in the SSL VPN instance configuration mode, use the following command:

no link-select [**addr1** | **addr2** | **addr3** | **addr4**]

- **no link-select** - Delete all configurations about optimal link selection.
- **addr1** | **addr2** | **addr3** | **addr4** - Delete the Internet interface IP address of the specified DNAT device.

SSL VPN optimal link selection also provides multi-link redundancy, which enables the server to switch links when one link disconnects so as to guarantee the connection stability between server and client (traffic flow may be interrupted during switching).

For more information, refer to the **VPN** > **SSL VPN** topic in *StoneOS CLI User Guide*. FR 41605

Configuring ZTNA Instance

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

tunnel ztna *instance-name* [**intranet** | **remote**]

- *instance-name* - Specifies a name for the ZTNA instance. The length is 1 to 31 characters.
- **intranet** | **remote** - Specifies the ZTNA instance type, which can be **intranet** or **remote**. By default, **remote** is selected.

This command creates a ZTNA instance with the specified name and leads you into the corresponding ZTNA instance configuration mode, including intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode; if the instance exists, you will enter this ZTNA instance configuration mode directly.

To delete a ZTNA instance, in the ZTNA instance configuration mode, use the following command:

no tunnel ztna *instance-name* {**intranet** | **remote**}

> **Notes:** The number of ZTNA gateways that can be created varies based on different platforms.

In intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, you can configure the following:

- Enabling/Disabling ZTNA Instance
- Specifying the Service Type
- Specifying an Access Address Pool (applicable only to remote access ZTNA instance)
- Specifying a Server Interface
  ……
- Configuring a ZTNA Tunnel Route (applicable only to remote access ZTNA instance)
  ……
- Configuring Multi-Gateway Address
  ……

Specifying the Service Type

You can specify the service type of ZTNA instance, which can be IPv4, IPv6, or dual stack. The dual stack type can be configured only for remote access ZTNA instance. The IPv6 and dual stack types are available only when the system version is IPv6. By default, the service type of ZTNA instance is IPv4. To specify the service type of the ZTNA instance, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

service-type {**ipv4** | **ipv6** | **dual-stack**}

- **ipv4** | **ipv6** | **dual-stack** − Specifies the service type of the ZTNA instance, including IPv4 or IPv6.

  Related Concept:

  Dual stack is a network technology that allows both IPv4 and IPv6 protocol stacks to run simultaneously on a network device, enabling seamless switching and communication between IPv4 and IPv6 networks.

Specifying a Server Interface

The client uses HTTPS protocol to access the server. Each ZTNA instance can be configured with 8 interfaces. To specify the ZTNA interface of the server, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

interface *interface-name*

- *interface-name* – Specifies the name of the interface for the ZTNA client to connect.

To cancel the ZTNA interface, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no interface *interface-name*

Configuring a ZTNA Tunnel Route

This configuration is applicable only to remote access ZTNA instance. To reach the destination IPv4/IPv6 network segment or destination domain name through the ZTNA tunnel, you need to specify them by configuring the IPv4/IPv6 ZTNA tunnel route.

- The specified destination network segment will be distributed to the ZTNA client, then the client uses it to generate the route to the specified destination.
- The specified destination domain name will be distributed to the ZTNA client, and the client will generate the route to the specified destination according to the resolving results from DNS.

Notes: When you configuring dual stack ZTNA, you need to specify both the IPv4 and IPv6 tunnel routes.

Configuring a ZTNA Tunnel Route to the Specified IPv4 Network Segment

You can only specify the IPv4 or dual stack ZTNA tunnel route for the IPv4 ZTNA instance. To reach the destination IPv4 network segment through a ZTNA tunnel, in remote access ZTNA instance configuration mode, use the following command:

split-tunnel-route*ip-address/netmask* [**metric***metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ip-address/netmask* – Specifies the IP address and network mask of the destination network segment.
- **metric***metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

You can add multiple IPv4 tunnel routes as required.

To delete an IPv4 tunnel route, in remote access ZTNA instance configuration mode, use the following command:

no split-tunnel-route*ip-address/netmask* [**metric***metric-number*]

Configuring a ZTNA Tunnel Route to the Specified IPv6 Network Segment

You can only specify the IPv6 or dual stack ZTNA tunnel route for the IPv6 ZTNA instance. To reach the destination IPv6 network segment through a ZTNA tunnel, in remote access ZTNA instance configuration mode, use the following command:

split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*] [**user-group** *aaa-server_name group_name* | **role** *role_name*]

- *ipv6-address/prefix* – Specifies the IPv6 address and prefix length of the destination network segment.
- **metric***metric-number* – Specifies a metric value for the route. The value range is 1 to 9999. The default value is 35.
- **user-group** *aaa-server_name group_name* – Specifies the AAA serer to which the user group belongs and the user group name. Only users in this user group can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a user group. For more information, see User Group Configuration (System Management > System User Management > User Group Configuration).
- **role** *role_name*] – Specifies the role name. Only users corresponding to this role can access the specified network segment in the tunnel route. Note: Before you specify this parameter, you need to create a role. For more information, see Role Configuration (System Management > System User Management > Role Configuration).

You can add multiple IPv6 tunnel routes as required.

To delete an IPv6 tunnel route, in remote access ZTNA instance configuration mode, use the following command:

no split-tunnel-route-ipv6 *ipv6-address/prefix* [**metric** *metric-number*]

Configuring Multi-Gateway Address

ZTNA supports configuration of multiple backup gateways for clients to select which to connect. When the ZTNA server is configured with backup gateways, ZTNA users can enable gateway detection on clients to select the connected ZTNA gateway.

After gateway detection is enabled, ZTNA client will attempt to obtain the backup gateway list from the gateway that the user is logging in, detect the link quality of all backup gateways and then establish the ZTNA connection with the one that has the best link quality. After the connection is established, ZTNA client will detect and update the link quality every 30 minutes. When a connection or login failure occurs, ZTNA client will switch to connect the backup gateway that has the best link quality.

To configure a backup gateway, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

gateway *gateway-name* {**ipv4***ipv4-address* | **ipv6***ipv6-address*| **domain** *string*}

- *gateway-name* - Specifies the backup gateway name. The range is 1 to 31 characters.
- **ipv4***ipv4-address*- Specifies the IPv4 address of the backup gateway.
- **ipv6***ipv6-address*- Specifies the IPv6 address of the backup gateway.
- *string* - Specifies the domain name of the backup gateway. The range is 1 to 255 characters, and the length between two dots (.) cannot exceed 63 characters.

Repeat this command to configure multiple backup gateways.

To delete the specified backup gateway, in intranet access ZTNA instance configuration mode or remote access ZTNA instance configuration mode, use the following command:

no gateway *gateway-name*

Notes: ZTNA configurations on the backup gateways need to be consistent with those on the master backup gateway.

For more information, refer to the **Zero Trust Network Access (ZTNA)** > **Configuring ZTNA Service** in *StoneOS CLI User Guide*. FR 41605

Supporting the Signature Database of IoT Devices

CLI

Configuration Procedure of IoT Monitor Function

To use the IoT monitor function, you need to configure the following:

1. **Update the signature database of IoT devices**

    a. Update the signature database of IoT devices——Upgrade the signature database of IoT devices to improve the capability of identifying IoT devices.

2. Select an IoT asset identification type:

    a. **Local asset identification**:

    Note: The built-in type for local asset identification is available only for A-series fire-walls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

        1. Configure Docker——Deploy the asset identification system into the device system

        2. Enable the local asset identification function

        3. Configure the local asset identification function

    b. **Local asset identification——External Docker**:

        - Deploy the asset identification system on the virtual machine

3. **IoT Asset Identification**

    a. Configuring the identification list——Specify the address list of IoT asset devices that you want to identify.

    b. Configuring the zone——Enable the IoT Monitor function within a zone and bind the identification list.

4. **IoT Monitor Management**

    a. Configuring the region——Add the regionof the corresponding region for IoT devices.

b. Viewing IoT monitor——View the manufacturer, type, online devices, and various detailed statistics of all identified IoT devices.

c. Viewing IoT logs.

5. IoT Policy Control

a. Configuring the device object——Specify classification dimensions for IoT devices, such as manufacturer, type, device model, operating system, etc. The system will then map the identified IoT device information to corresponding device objects.

b. Configuring the policy rule——Configure the policy rule based on device objects.

6. IoT Threat Governance

a. Combined with the threat protection function, endpoint protection function, and data security function, IoT devices detected with security threats can be correspondingly governed.

b. Uploading IoT data to iSource——You can implement further threat event response and handling such as asset management and policy/blocking deployment by using iSoutce.

c. Uploading IoT data to the Hillstone cloud platform——Upload IoT report data and asset data to the cloud platform for unified analysis, statistics, and management.

Notes: The IoT monitor function is controlled by license. Make sure that the current device supports the IoT monitor function and is installed with the IoT license.

IoT Device Signature Database

Introduction of IoT Device Signature Database

The IoT device signature database is crucial for identifying various IoT devices. Its continuous updates ensure ongoing accuracy in device identification. The IoT device signature database supports both online and local updates. Hillstone provides two default update servers for the signature database: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can modify the signature database update configurations as needed.

Notes: Non-root VSYS does not support IoT signature database updates.

IoT Device Signature Database Update Configuration

The IoT device signature database update configurations include:

- Configuring the update mode
- Configuring the update transmission protocol
- Configuring the update server
- Specifying an HTTP proxy server
- Specifying the update schedule
- Updating immediately
- Importing the IoT device signature database file
- Viewing IoT device signature database information
- Viewing update configurations of the IoT device signature database

Configuring the Update Mode

The system supports both manual and automatic update modes. To configure the update mode, in global configuration mode, use the following command:

iot update mode {**auto** | **manual**}

- **auto** – Specifies automatic updates for the IoT signature database (default mode).
- **manual** – Specifies manual updates for the IoT signature database.

To restore the default update mode, in global configuration mode, use the following command:

no iot update mode

Configuring the Update Transmission Protocol

The system supports to update the IoT signature database via HTTP and HTTPS, with HTTPS as the default. To configure HTTP as the update protocol, in global configuration mode, use the following command:

iot update protocol HTTP

To restore the default HTTPS mode, in global configuration mode, use the following command:

no iot update protocol HTTP

Configuring the Update Server

The system provides two default IoT device signature database update servers: update1.hillstonenet.com and update2.hillstonenet.com. You can configure up to three additional update servers. To configure an update server, in global configuration mode, use the following command:

iot update {**server1** | **server2** | **server3**} {*ip-address* | *domain-name*} [**vrouter***vrouter-name*] [**src-interface***src-interface-name*]

- **server1 | server2 | server3** – Specifies the server to configure (supports both IPv4 and IPv6). The default for **server1** is update1.hillstonenet.com and for **server2** is update2.hillstonenet.com.

- *ip-address* | *domain-name* – Specifies the name of the update server, either as an IP address (*ip-address*) or domain name (*domain-name*) (e.g., update1.hillstonenet.com).
- **vrouter***vrouter-name* - Specifies the VRouter to which the update server belongs (default: **trust-vr**).
- **src-interface***src-interface-name* – Specifies the name of the source interface, which needs to be an interface within the VRouter. This way, the IoT device signature database will access the update server via this source interface. If not specified, the MGT interface is used by default.

To remove the configuration for a specified update server, in global configuration mode, use the following command:

no iot update {**server1** | **server2** | **server3**}

Specifying an HTTP Proxy Server

When the device needs to access the internet via an HTTP proxy, you need to configure the proxy server's IP address and port to ensure successful updates of the IoT device signature database.

To configure the proxy server, in global configuration mode, use the following command:

iot update proxy-server {**main** | **backup**} *ip-addressport-number*

- **proxy-server** {**main** | **backup**} – Use **main** to specify the main proxy server and use **backup** to specify the backup proxy server.
- *ip-address port-number* – Specifies the IP address and port number of the proxy server.

To remove the proxy server configuration, use the following command:

no iot update proxy-server {**main** | **backup**}

Specifying the Update Schedule

By default, the system updates the IoT device signature database daily in automatic mode at random times to avoid server overload. You can specify the update frequency and time as needed. To configure the update schedule, in global configuration mode, use the following command:

iot update schedule {**daily** | **weekly** {**mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun**} | **monthly** *date*} [*HH:MM*]

- **daily** – Sets daily updates.
- **weekly {mon | tue | wed | thu | fri | sat | sun}** – Sets weekly updates, with the specified day (**mon | tue | wed | thu | fri | sat | sun**).
- **monthly** *date* - Sets monthly updates, with the specified date *date* (1-31). If the specified date does not exist in a given month (e.g., February 30), the update will not occur that month.
- *HH:MM* – Specifies the update time (e.g., 09:00).

Updating Immediately

Regardless of whether the update mode is manual or automatic, you can trigger an immediate update at any time. To perform an immediate update, in any mode, use the following command:

exec iot update [**full**]

- **exec iot update** – Updates only the differing parts of the current IoT device signature database and the latest released IoT device signature database from the update server.
- **full** – Forces an upgrade of the current IoT device signature database.

Importing the IoT Device Signature Database File

In some cases, your device may not be able to connect to the update server to update the IoT device signature database. To fix this issue, the system provides the function of importing the IoT device signature database file, allowing you to import the IoT device signature database file into the device via FTP, FTPS, SFTP, or TFTP servers, thus updating the device's IoT device signature database. To import the IoT device signature database file, in execution mode, use the following command:

import iot signature from {{**ftp | ftps |sftp**} **server***A.B.C.D | X:X:X:X::X***user***user-name***password***password*[**vrouter***vrouter-name*] | **tftp server***ip-address* [**vrouter***vrouter-name*]} *file-name*

- **ftp | ftps |sftp** - Specifies the type of server.
- *A.B.C.D | X:X:X:X::X* – Specifies the IP address of the FTP, FTPS, SFTP, or TFTP server.
- **user***user-name***password***password* – Specifies the username and password for the FTP/FTPS/SFTP server.
- **vrouter***vrouter-name* – Specifies the VRouter to which the FTP, FTPS, SFTP, or TFTP server belongs. Default value: trust-vr.
- *file-name* – Specifies the name of the IoT device signature database file to be imported.

Viewing IoT Device Signature Database Information

You can view the IoT device signature database information at any time using the corresponding show command, which includes the version and release date of the IoT device signature database. To view IoT device signature database information, in any mode, use the following command:

show iot info

Example:

```
hostname# show av-file-engine info
Signature vendor: Hillstone Networks
Current version: 1.0.72
Release date: 2024/08/27 11:05:40
```

Viewing Update Configurations of the IoT Device Signature Database

You can view the IoT device signature database update information at any time using the corresponding show command, which includes information on the update server, update mode, update frequency and time, and the update status of the IoT device signature database. To view IoT

device signature database update configuration information, in any mode, use the following command:

show iot update

Example:

```
hostname# show av-file-engine update
IoT signature update options:
protocol: HTTPS
server1: 10.XX.XX.100, 443, trust-vr
server2: 10.XX.XX.100, 443, trust-vr
server3:
proxy server status: disable
main proxy server:
backup proxy server:
mode: auto
schedule: daily 01:25
current status: normal
last update result: latest signature, needn't update
last update time: Tue Sep 10 01:25:59 2024
```

For more information, refer to the **Threat Prevention** > **IoT Monitor** topic in *StoneOS CLI User Guide*. FR 42382

WebUI

Configuration Procedure of IoT Monitor Function

To use the IoT monitor function, you need to configure the following:

1. Update the signature database of IoT devices

    a. Update the signature database of IoT devices——Upgrade the signature database of IoT devices to improve the capability of identifying IoT devices.

2. IoT Asset Identification

    a. Select an IoT asset identification type:

        - Local asset identification: built-in——use the Docker management function to deploy the asset identification system into the device system; external——install the asset identification program on the virtual machine and use the asset identification system deployed on the virtual machine.

    b. Configuring IoT global configuration——Specify the asset identification method and the corresponding detailed configuration.

    c. Configuring the identification list——Specify the address list of IoT asset devices that you want to identify.

    d. Configuring the endpoint type——Enable/disable the function of automatically synchronizing endpoints to the repository.

    e. Configuring the zone——Enable the IoT Monitor function within a zone and bind the identification list.

3. IoT Monitor Management

    a. Configuring the region——Add the region of the corresponding area for IoT devices.

    b. Viewing IoT monitor——View the manufacturer, type, online devices, and various detailed statistics of all identified IoT devices.

    c. Viewing IoT logs

4. **IoT Policy Control**

    a. Configuring the device object——Specify classification dimensions for IoT devices, such as manufacturer, type, device model, operating system, etc. The system will then map the identified IoT device information to corresponding device objects.

    b. Configuring the policy rule——Configure the policy rule based on device objects.

5. **IoT Threat Governance**

    a. Combined with the threat protection function, endpoint protection function, and data security function, IoT devices detected with security threats can be correspondingly governed.

    b. Uploading IoT data to iSource——You can implement further threat event response and handling such as asset management and policy/blocking deployment by using iSoutce.

    c. Uploading IoT data to the Hillstone cloud platform——Upload IoT report data and asset data to the cloud platform for unified analysis, statistics, and management.

Notes: The IoT monitor function is controlled by license. Make sure that the current device supports the IoT monitor function and is installed with the IoT license.

For more information, refer to the **Threat Prevention** > **IoT Monitor** topic in *StoneOS WebUI User Guide*. FR 42382

Upgrading System

The firmware upgrade wizard helps you:

- Upgrade system to a new version or roll back system to a previous version.
- Upgrade the format of earlier-version data such as logs, monitoring data, and reports in the database or delete the data.
- Update the Share Access signature database, Application signature database, URL signature database, Antivirus signature database, Antivirus intelligence file engine database, IPS signature database, Sandbox Whitelist Database, IP reputation database, Risk mitigation rule signature database, Abnormal behavior mode database, Malware behavior mode database, botnet prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database.
- Update the Trusted Root Certificate Database.

Updating Signature Database

The signature databases that can be installed include Encrypted traffic detection database,Share Access signature database,Application signature database, URL signature database, Antivirus signature database, antivirus intelligence file engine database, Sandbox Whitelist Database, IPS signature database, IP reputation database, SSL proxy domain whitelist signature database, Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database. Except Encrypted traffic detection database,SSL proxy domain whitelist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, you can only view other signature databases when the system is installed with the corresponding licenses. The system support the following two methods to upgrade signature databases: remote update via HTTP and HTTPS; local update via downloading update package through the default signature database update server.Except the SSL proxy domain whitelist signature database or ISP Information Database, you can only view signature databases installed with licenses.

The system supports to download each signature database over IPv6.

Notes:

The following devices support to upgrade antivirus intelligence file engine database.

- A-series: Except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200.
- K-series: SG-6000-K2680, SG-6000-K2380, and SG-6000-K6280-GS.SG-6000-K6580, and SG-6000-K9180.
- X-series: SG-6000-X25803, SG-6000-X25812, and SG-6000-X9180-GS.
- CloudEdge: Only CloudEdge that is deployed on X86-based server.

To update signature database, take the following steps:

1. Select **System** > **Upgrade Management** > **Signature Database Update**.
2. In the **Signature Database Update** page, configure the following.

Option	Description
Current Version	Show the current version number.
Latest Version	Show the latest version number. **Note:** The latest version of the ISP information database can be displayed only when the current version exists. The latest version of other signature databases can be displayed only when the corresponding signature database licenses are activated and the current version exists.
Update Entire Signature	In the IPS signature database module, you can update the current IPS signature database to the IPS entire signature database. By default, this option is disabled. Click  to update the IPS entire signature database. This operation may cause the throughput performance of the device to

Option	Description
	drop by up to 20%. It is recommended that you configure it based on the actual load of the device. Click  to cancel updating the IPS entire signature database. This operation reduces the current number of signatures in the IPS signature database and may affect the details of threat events that have been generated. **Notes:** The following devices support this option: • A-series: SG-6000-A200/A200G4B /A200W/A1000/A1100
Remote Update	Encrypted traffic detection database, Application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database. • Protocol: Select the update method of the signature database, including HTTP and HTTPS. Click **Restore Default** to restore the default HTTPS transmission method. • Update Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. The IPv4 and IPv6 address are supported for configuring the update server address.

Option	Description
	Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers according to your need. In **Update Server**, specify the server IP or domain name and Virtual Router. • Update Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally. In **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button of **Auto Update** and specify the auto update time. Click **Ok** to save your changes. • Update Now: Click **Ok And Online Update** to update the signature database right now.
Local Update	Download the update package from the default feature update server for local update. • Download the upgrade packages of the encrypted traffic detection database, application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database, SSL proxy

Option	Description
	domain whitelist signature database, , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, IP geography database, and IoT device signature database from https://update1.hillstonenet.com and https://update2.hillstonenet.com. • Click **Browse** and select the signature file in your local PC, and then click **Upload**. **Notes:** 1. Before StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Botnet C&C Detection Package" link of the default update server. From StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Encrypt Botnet C&C Detection Package" link of the default update server. 2. If a large number of devices (with the same version and model) need local update, contact Hillstone's support team to acquire bulk update solutions.

For more information, refer to the **System** > **Upgrading System** topic in *StoneOS WebUI User Guide*. FR 42382

Online Packet Capture Supports to Capture only Packets from Newly Established Sessions

CLI

Configuring Packet Capture Task

Including configuration capture tasks, capture rules, start/stop capture, export capture files, clear capture files.

packet-capture task

Create an online packet capture task and enter the packet capture task configuration mode. Use the no form of the command to delete the specified online packet capture task.

Command:

packet-capture task*task-name*

no packet-capture task*task-name*

Description:

task-name - Specifies the name of the online packet capture task and enter the packet capture task configuration mode.

Default values:

None

Mode:

Global configuration mode

Guidance:

At most 5 packets capture tasks can be configured within each VSYS.

Example:

hostname(config)# **packet-capture task task1**

include-self-traffic

Enable the Contain Self-traffic function so that captured packets contain traffic sent and received by the device itself. Use the no form of the command to disable this function.

Command:

include-self-traffic

no include-self-traffic

Description:

None

Default values:

Enable

Mode:

Packet capture task configuration mode

Guidance:

You can configure this function when the packet capture mode is session mode.

Example:

hostname(config-pkt-task)# **include-self-traffic**

only-new-session

Enable capturing only packets from newly established sessions.

［Command］

only-new-session [**pak-num-per-session***number*]

no only-new-session

［Description］

pak-num-per-session*number* - Specifies the number of data packets that can be captured for each newly established session. This count starts from the time the session is established. Default value: 20. Valid values: 1 to 255. For example, if you specify the number of data packets to capture for

each newly established session as 100, the system will capture the first 100 data packets for each newly established session.

［Default values］

Disable

［Mode］

Packet capture task configuration mode

［Guidance］

You can configure this function when the packet capture mode is session mode.

［Example］

hostname(config-pkt-task)# **only-new-session pak-num-per-session 100**

For more information, refer to the **Monitor** > **Diagnostic Tool** topic in *StoneOS CLI User Guide*.

FR 42386

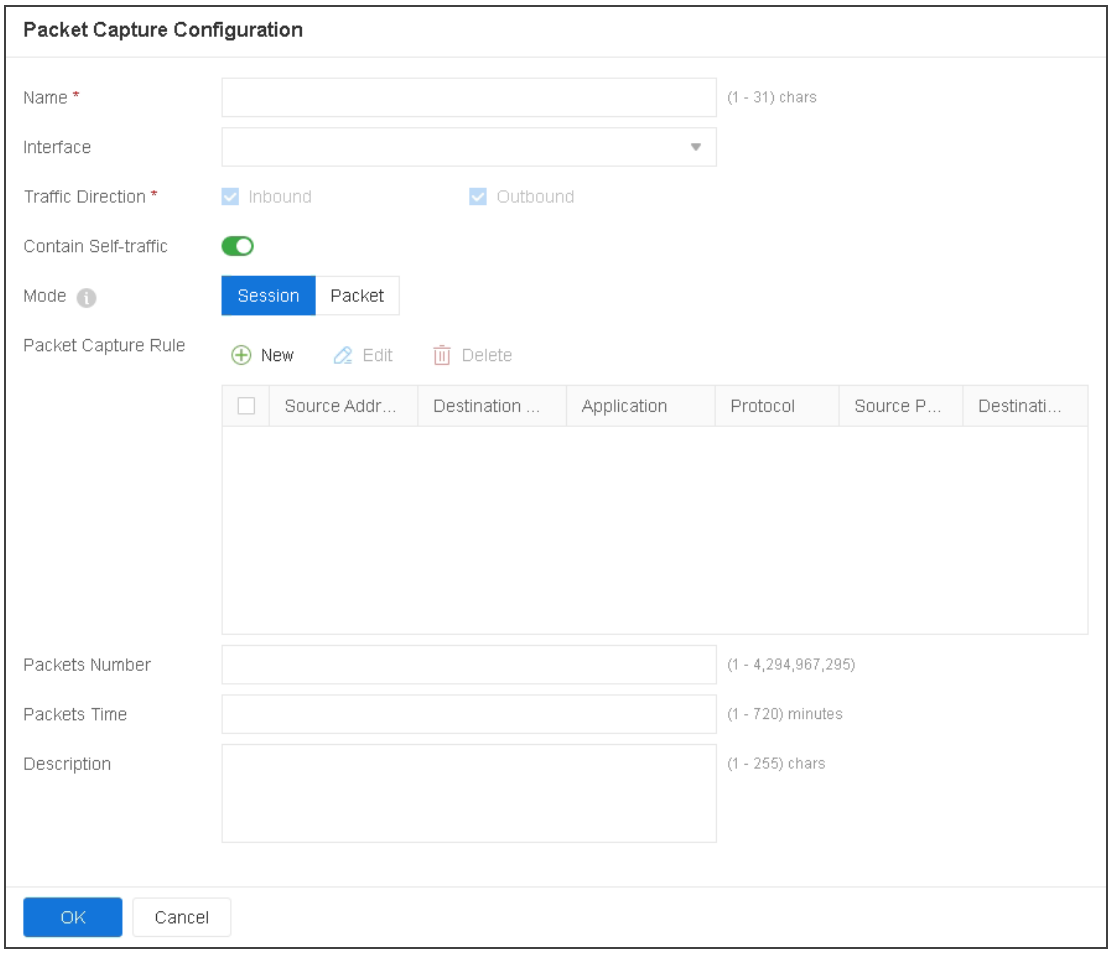
WebUI

Configuring Packet Capture Tools

To capture packets, take the following steps:

1. Select **System > Diagnostic Center > Packet Capture Tool**.

2. Click **New**.



Option	Description
Name	Enter the name of the packets capture entry.
Interface	Select the interface used for the online packet capture task from the drop-down list.
Traffic Direction	Specifies the traffic direction of the interface. Valid values: Inbound and Outbound. By default, both Inbound and Outbound are selected.

Option	Description
	• Inbound: The online packet capture task captures packets that flow from the specified interface into the device. If fails, the packets may be blocked by the firewall or not flow into the firewall. If no packets flow into the firewall, you can troubleshoot the upstream link or upstream device as needed. • Outbound: The online packet capture task captures packets that flow out from the specified interface. If succeeds, you can troubleshoot the downstream link or downstream device as needed. • Inbound+Outbound: You can select both inbound and outbound and determine the actual traffic direction of the interface based on captured packets.
Mode	Specifies the mode of capturing packets, including the session mode and packet mode. By default, the session mode is selected. • Session: In this mode, the system can efficiently capture packets that have established sessions and meet the packet capture rule. ◦ Contain Self-traffic: Turn on the switch to enable the Contain Self-traffic function. This way, captured packets contain traffic sent and received by the device itself. By default, this function is enabled.

Option	Description
	◦ Only New Session: Turn on the switch to enable the Capture only Packets from Newly Established Sessions. By default, this function is disabled. After you enable this function, you can specify the number of data packets that can be captured for each newly established session in the **Pcap Num Per Session** field. This count starts from the time the session is established. Default value: 20. Valid values: 1 to 255. For example, if you specify the number of data packets to capture for each newly established session as 100, the system will capture the first 100 data packets for each newly established session. ◦ Packet Capture Rule: Click **New**, and configure the packet capture rules in the **Packet Capture Rules** page. For the configuration method, refer to Create a Packet Capture Rule. Select the check box of the packet capture rule in the list and click the **Edit** button to edit the configuration of the packet capture rule again. Select the check box of the packet capture rule in the list and click the **Delete** button to delete the packet capture rule. • Packet: When the system resources are sufficient, in this mode, the system can capture packets of all traffic.

Option	Description
	Notes: • In session mode, you cannot capture packets of hardware fast forward. • In packet mode, you cannot capture packets of hardware fast forward and IOM card fast forward.
Packets Number	Specifies the total number of packets that can be captured for the packet capture task. Valid values: 1 to 4294967295. During the effective period (packets time) of the packet capture task, if the number of packets captured reaches the configured number, the system automatically stops capturing packets.
Packets Time	Enter the packets time in the text box. The range is 1-720 minutes.
Description	Enter the entry description in the text box.

3. Click **OK**.



4. For each task, click **Start** button in the Capture Packets column to start capturing packets, and **Start** button will change to **Capturing**. Click the **Status** to view the current size/number of packets captured.

5. To stop capturing packets, click **Capturing** button in the Capture Packets column.

6. After you stop capturing packets or the capturing is completed, click **Download** at the top-right corner of the Capture Grid List to save the captured packets to a specified location.
7. You can select one or more file entries, and click **Export** at the top right corner of the list to export the package files. The exported grab package files are in compressed format.
8. To clear packet capture data, select a packet capture task and click the **Clear Data** button. All files captured under this task will be cleared.

Notes:

- At most 5 online packet capture tasks can be created.
- An online packet capture task cannot capture packets based on the tunnel interface and MGT0 interface.
- We recommend that the packet you capture at a time does not exceed 500 MB because a larger packet may fail to be exported caused by timeout.
- At most 5 packet capture tasks can be configured within each VSYS.
- You can start only one packet capture task within a single VSYS each time, and start a packet capture task within multiple VSYSes at the same time.
- When you delete a non-root VSYS, the packet capture tasks and packet capture files within the VSYS are deleted at the same time.

For more information, refer to the **Diagnosis Center** > **Packet Capture Tool** topic in *StoneOS WebUI User Guide*. FR 42386

Configuring Local Asset Identification

The local asset identification function is to identify IoT devices by using the asset identification module deployed in the device.

Enabling/Disabling the Local Asset Identification Function

By default, the local asset identification function is disabled. To enable or disable the function, in global configuration mode, use the following command:

- Enable: **iot-monitor docker-detect enable**
- Disable: **no iot-monitor docker-detect**

Configuring the Local Asset Identification Function

Local asset identification is divided into built-in and external types.

- Built-in: Use the built-in asset identification module. Before you select this type, configure the Docker management functon of the system to deploy the asset identification system within the firewall.
- External: Use the asset identification system deployed on the virtual machine. Before you select this type, deploy the asset identification system in the virtual machine.

Notes: The built-in type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

To configure the local asset identification function, in global configuration mode, use the following command:

iot-monitor docker-detect {**local-docker** | **external-docker ip** *ip-address*} **port** *port-number* **vrouter** *vr-name*

- **local-docker** - Specifies to use the built-in asset identification module. The default IP address is 127.0.0.1, which requires no configuration or modification.

- **external-docker ip** *ip-address* - Specifies to use the asset identification system deployed on the virtual machine, and specifies the IP address of the virtual machine.
- **port** *port-number* - Specifies the port number of the asset identification module. When you use **local-docker**, this port number is the host port number of Docker. Please make sure this port number is consistent with the host port number specified in Docker. Valid values: 1-65535.
- **vrouter** *vr-name* - Specifies the name of the VRouter to which the virtual machine belongs from the drop-down list.

To cancel the configuration of the local asset identification function, in global configuration mode, use the following command:

no iot-monitor docker-detect local-docker

Viewing the Configuration about the IoT Asset Identification Function

To view the configuration about the IoT asset identification function, in any mode, use the following command:

show iot-monitor detect-config

Example:

SG-6000(config)# **show iot-monitor detect-config**

IoT-monitor cloud-detect status: enable

IoT-monitor docker-detect module environment: external iot docker

IoT-monitor docker-detect module ip: 10.182.192.187

IoT-monitor docker-detect module port: 36000

IoT-monitor docker-detect module vrouter: trust-vr

```
IoT-monitor docker-detect action status: Disable
IoT-monitor docker-detect connect status: Disabled
-------------------------------------------------------------------------------------------
-------
```

Configuring the Interval of Re-identifying IoT Devices

By default, the device system re-identifies IoT devices at an interval of 20 minutes (1,200 seconds). You can adjust this interval based on your requirements. To do this, in global configuration mode, use the following command:

iot-monitor identify-renew interval *interval-value*

- *interval-value* - Specifies the interval of re-identification. Valid values: 10 to 1200 seconds. Default value: 1200 seconds.

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

no iot-monitor identify-renew interval

For more information, refer to the **Threat Prevention** > **IoT Monitor** topic in *StoneOS CLI User Guide*. FR 42384

The Ingress Interface of DNS Proxy Rule Can be Set to Any

CLI

Creating a DNS Proxy Rule

To create a DNS proxy rule or enter the DNS Proxy rule configuration mode, in the global configuration mode, use the following command:

dns-proxy rule [**id***id*]

- **id***id* – Specifies the ID of the DNS proxy rule. If not specified, the system will automatically assign an ID to the DNS proxy rule. The ID must be unique in the entire system.

To delete the DNS proxy rule, in the global configuration mode, use the command **no dns-proxy rule id** *id*.

Configuring the Filtering Condition of a DNS Proxy rule

The filtering conditions of a DNS Proxy rule include the ingress interface, source address, destination address and DNS domain name of DNS request. You should configure these four conditions simultaneously, and then system will filter the DNS requests after configuration. Only if the DNS request meets the above four conditions can it is considered a successful match.

Specifying Ingress Interface

You can specify the ingress interface of DNS requests in the rule to filter DNS request messages. Once specified, the system will process the ingress traffic based on the behavior specified in the rule. To add a DNS ingress interface, in DNS proxy rule configuration mode, use the following command:

> **Notes:** The ingress interface cannot be configured as a management interface, HA interface, loopback interface, , Vif interface, or other VSYS interface.

ingress-interface [*interface-name* | **Any**]

- *interface-name* | **Any** - Specifies the ingress interface for DNS requests, which can be an interface (*interface-name*) or **Any**, with the default set to **Any**.
    - If specified as an interface (*interface-name*), the system will process the ingress traffic based on the behavior specified in the DNS proxy rules. You can configure this command multiple times to specify multiple DNS ingress interfaces.

- If specified as **Any**, the system will process the traffic from any interface based on the behavior specified in the DNS proxy rule. This configuration is applicable to the following scenarios: In a network environment with multiple segments, where each segment is connected to the firewall via different interfaces and requires to direct user traffic to the appropriate DNS server for resolution by using DNS proxy, you can configure the ingress interface of the DNS proxy rule as 'Any'. This allows the same rule to be reused across interfaces of different segments, which avoids to create and maintain separate DNS proxy rule for interface of each segment, thereby simplifying the configuration.

In DNS proxy rule configuration mode, use the **no ingress-interface** [**Any** | *interface-name*] command to delete the ingress interface of DNS traffic.

Specifying Source Address

You can specify the source address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. To add or delete the source address of DNS request, in DNS proxy rule configuration mode, use the following command:

- Add the source address of the address entry type: **src-addr** { *addr-name* | **any**}
- Delete the source address of the address entry type: **no src-addr** { *addr-name*| **any**}
- Add the source address of the IP member type: **src-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the source address of the IP member type: **no src-ip** {*ip/netmask* | *ip-address netmask*}
- Add the source address of the IP range type: **src-range***min-ip max-ip*
- Delete the source address of the IP range type: **no src-range***min-ip max-ip*

Specifying Destination Address

You can specify the destination address of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple destination address filtering conditions.To add or delete

the destination address of request, in DNS proxy rule configuration mode, use the following command:

- Add the destination address of the address entry type: **dst-addr** { *addr-name* | **any**}
- Delete the destination address of the address entry type: **no dst-addr**{ *addr-name* | **any**}
- Add the destination address of the IP member type: **dst-ip** {*ip/netmask* | *ip-address netmask*}
- Delete the destinaion address of the IP member type: **no dst-ip** {*ip/netmask* | *ip-address netmask*}
- Add the destination address of the IP range type: **dst-range***min-ip max-ip*
- Delete the destination address of the IP range type: **no dst-range***min-ip max-ip*

Specifying Domain Name

You can specify the domain name of DNS request in the rule to filter the DNS request message. It is permissible to specify multiple domain name filtering conditions.To add or delete the domain name, in DNS proxy rule configuration mode, use the following command:

domain { **any** | *domain-name* | **host-book***host-book-entry* }

- *domain-name* - Specifies the domain name that will be matched.
- **any** – Specifies as any domain name that will be matched.
- **host-book** *host-book-entry* – Specifies the name of the host entry that will be matched.

In DNS proxy rule configuration mode ,use the following command to delete the domain name that will be matched:

no domain any | *domain-name* | **host-book***host-book-entry*.

Specifying the Action of a DNS Proxy Rule

For the DNS request that meets the filtering conditions, system can proxy, bypass and block the traffic.You can specify the action for a DNS proxy rule, in the DNS proxy rule configuration mode,

using the following command:

action {**proxy** [**rollback**] | **secure-dns** | **bypass** | **block**}

- **proxy** [**rollback**] – Specifies the action of a DNS proxy rule as proxy. The DNS request will be resolved through the proxy server. You can configure the **rollback** property as needed. After **rollback** is configured, when there is no DNS server or DNS server unable to resolve the DNS address, system will bypass the DNS request and forward it to the DNS server originally requested by the message.
- **secure-dns** – Specifies the action of a DNS proxy rule as secure DNS. That is, the DNS request will be proxied and resolved through the DoH server. When the secure DNS function is not enabled or the connection fails, the default action is "proxy". For more information, see Secure DNS.
- **bypass** – Specifies the action of a DNS proxy rule as bypass. That is, the DNS request will be forwarded to the DNS server originally requested by the message.
- **block** – Specifies the action of a DNS proxy rule as block. That is,the DNS request will be discarded.

For more information, refer to the **Firewall** > **DNS** > **Configuring a DNS Proxy** topic in *StoneOS CLI User Guide*. FR 39078

WebUI

Configuring a DNS Proxy

DNS Proxy function take effect by the DNS proxy rules.Generally a proxy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's ingress interface, source address, destination address, and domain name. The action of the DNS proxy rules includes proxy, secure DNS, bypass, and block. When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers, so that the DNS request meeting the filtering condition will be resolved by these DNS proxy servers.

Configuring a DNS Proxy Rule

To create a DNS proxy rule, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **New** in the DNS Proxy section.
3. In the <DNS Proxy Rule Configuration> page, configure the following settings.

Option	Description
Description	Add the description.
Type	Specify the type of a DNS proxy rule, IPv4 or IPv6.
Ingress Interface	Specifies the ingress interface of DNS request in the rule to filter the DNS request message, which can be an interface or Any, with the default set to Any: • If specified as an interface, the system will process the ingress traffic based on the behavior specified in the DNS proxy rules. You can configure this command multiple times to specify multiple DNS ingress interfaces. • If specified as **Any**, the system will process the traffic from any interface based on the behavior specified in the DNS proxy rule. This configuration is applicable to the following scenarios: In a network environment with multiple segments, where each segment is connected to the firewall via different interfaces and requires to direct user traffic to the appropriate DNS server for resolution by using DNS proxy, you can configure the ingress interface of the DNS proxy rule as 'Any'. This allows the same rule to be reused

Option	Description
	across interfaces of different segments, which avoids to create and maintain separate DNS proxy rule for interface of each segment, thereby simplifying the configuration. **Notes:** The ingress interface cannot be configured as a management interface, HA interface, loopback interface, , Vif interface, or other VSYS interface.
Source Address	Specify the source address of DNS request to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. Select the address entry type and then type the address. Click Add to add the selected entry to the pane. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. • You can click ▼ in the search box and enter the name and

Option	Description
	member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **IPv4** type, the default address configuration is any. To restore the configuration to this default one, select the **any** check box. • When selecting the **IPv6** type, the default address configuration is IPv6-any. To restore the configuration to this default one, select the **IPv6-any** check box.
Destination Address	Specify the destination address of DNS request to filter the DNS request message. It is permissible to specify multiple destination address filtering conditions. Select the address entry type and then type the address. Click Add to add the selected entry to the pane.

Option	Description
	1. Select an address type from the **Address** drop-down list. 2. Select or type the destination addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the destination address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if

Option	Description
	you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **IPv4** type, the default address configuration is any. To restore the configuration to this default one, select the **any** check box. • When selecting the **IPv6** type, the default address configuration is IPv6-any. To restore the configuration to this default one, select the **IPv6-any** check box
Domain	Specify the domain name of DNS request to filter the DNS request message. It is permissible to specify multiple domain name filtering conditions. Select the domain entry type and then type the domain. Click **Add** to add the selected entry to the pane. 1. Select an address type from the **Domain** drop-down list. 2. Select or type the domain name. 3. Click **Add** to add the domain to the left pane. 4. After adding the desired domain, click **Close** to complete the domain configuration. You can also perform other operations: • When selecting the **Host Book** type, you can click **Add** to create a new host book entry. • The default domain configuration is any. To restore the con-

Option	Description
	figuration to this default one, select the **any** check box.
Action	Specify the action for a DNS proxy rule. For the DNS request that meets the filtering conditions, system can proxy, secure DNS, bypass, or block the traffic.
DNS Proxy Failed	Specify the action for DNS proxy failed. System can block or bypass the DNS request and then forward it to the DNS server originally requested by the message.
Log	Click the **Enable** button to enable the DNS proxy log function. With this function enabled, the system will generate log information when there is DNS request traffic matching this DNS proxy rule. You can view the DNS proxy log in the Network Log page.
DNS Server	Specifies the DNS proxy server. When the action of the proxy rule is specified as Proxy, you need to configure the DNS proxy servers. You can specify up to six DNS servers for each DNS rule. You can customize the proxy server or specify a DNS server automatically obtained by the system. • When **User-defined** is selected, click **New** under the DNS server list and enter the IP address (IPv4 or IPv6 address) of the server and select the virtual router where the server belongs. You can bind the egress interface and preferred proxy as needed. When multiple DNS servers are configured, the preferred proxy server is given preference to resolve the domain. If no preferred server is specified, the

Option	Description
	system the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin. If there are only regular DNS server, then system will select this kind of DNS servers in a round robin. • When **Use System** is selected, select the virtual router or interface from the **Data Range** drop-down list to obtain the DNS server configured by the system or learned through a protocol, such as DHCP and PPPoE, from the specified virtual router or interface. **Note:** When the DNS server is configured as the IP address of the intranet DNS server, a DNS resolution dead loop may occur. Proceed with caution.
DNS64	If the IPv6 client host receives the DNS query request, it will use DNS64 to resolve the AAAA record (IPv6 address) in the DNS query information. If the resolution is successful, the IPv6 address is directly returned to the client. If the resolution fails, it will use DNS64 to resolve the A record (IPv4 address) in the DNS query information, and return the A record (IPv4 address) to the AAAA record (IPv6 address) to the client. Click the **Enable** button to enable the DNS64 function. By default, the DNS64 function is disabled.
DNS64 Server	The DNS64 server is used to resolve the A record (IPv4 address) in the DNS query information. Each IPv6 DNS proxy rule can

Option	Description
	specify up to 6 DNS64 servers. DNS64 Prefix: Specifies the DNS64 prefix and prefix length. The DNS64 prefix to synthesize the A record (IPv4 address) into an AAAA record (IPv6 address). The synthesized IPv6 address is in the form of "DNS64 prefix + IPv4 address". By default, the DNS64 prefix is "64:ff9b:: /96". At the bottom of the DNS64 server list, click the "+" button, and a table entry will be added. Enter the IP address (IPv4 address) of server and other parameters ,such as the virtual router.

4. Click **OK**.

For more information, refer to the **Network** > **DNS** topic in *StoneOS WebUI User Guide*. FR 39078

When Performing SNAT translation by Using NAT444, the System Can Allocate the Same Range of Port Blocks for both TCP and UDP Traffic from the Same Source IP address

CLI

Configuring NAT444

NAT444 on Hillstone devices is implemented by creating and executing SNAT rules. Compared with traditional SNAT rules, NAT444 SNAT rules are featured with some new parameters. This section mainly describes these new parameters. To configure an SNAT rule for NAT444, in the VRouter configuration mode, use the following command:

snatrule [**id***id*] [**before***id* | **after***id* | **top**] **from***src-address***to***dst-address* [**service***service-name*] [**eif***egress-interface* | **evr***vrouter-name*] **trans-toaddressbook***trans-to-address***mode**

dynamicport [**fixed-block** | **random-block** [**tcp-udp-port-consistent**]] **start***start-port***end***end-port***size***port-block-size* [**max-block-per-user***blocks*] [**log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} [**group** {*group-id* | **both**}] [**description***description*]

- **mode****dynamicport** [**fixed-block** | **random-block**] **start***start-port***end***end-port***size***port-block-size* [**max-block-per-user***blocks*] – All the sessions originating from one source IP will be mapped to one specified IP address in an address entry. The source IP corresponds to one or more port blocks of the mapped IP. If the port resources in the block are exhausted, the translation will fail. For detailed mapping relationship, see the NAT444 SNAT example below.
  - **fixed-block** – Uses the static port block mapping mode . Each source IP address corresponds to a fixed port block of the mapped IP.
  - **random-block** – Uses the dynamic port block mapping mode. Each source IP address can correspond to one or more port blocks and the parameter **max-block-per-user** *blocks* determines how many port blocks that each source IP address can correspond to.
  - **tcp-udp-port-consistent** – Specifies that the same range of port blocks is allocated for TCP and UDP traffic from the same source IP address, simplifying log information. This parameter can only be specified in dynamic port block mapping mode (**random-block**). Once this parameter is specified:
    - When allocating NAT444 port blocks for TCP or UDP traffic from the same source IP address, the system will assign the same range of port blocks for both protocols, and it will only record one port block allocation log. In this log, the transport protocol type (protocol) will be displayed as "255".

- When releasing NAT444 port blocks for TCP or UDP traffic from the same source IP address, the system will only release the port block resources when not any ports of the port blocks corresponding to these two protocols are used, and it will record only one port block release log. In this log, the transport protocol type (protocol) will be displayed as "255".
- For NAT444 port block requests and releases for ICMP or GRE traffic, the system will no longer record related log information.

- **start** *start-port* **end** *end-port* – Specifies the start port and end port of the available port range. The value range is 1024 to 65535.
- **size** *port-block-size* – Specifies the size of the port block. The value range is 64 to 64512, and the value must be the integer multiple of 64.
- **max-block-per-user***blocks* – Specifies the maximum number of port blocks that each user in the intranet can occupy. When using the dynamic port block mapping mode, you can set this parameter. The default value is 1.

- **log** {[**port-block** {**allocate** | **release** | **all**}] [**session** {**allocate** | **release** | **all**}] | **session** {**allocate** | **release** | **all**} | **all**]} – Configures log for NAT444 (generates logs for matched traffic):
  - **port-block** {**allocate** | **release** | **all**} – Generates logs when the system is allocating (**allocate**) or releasing (**release**) port block. **all** indicates generating logs for both of the above events.
  - **session** {**allocate** | **release** | **all**} – Generates logs when the system is creating (**allocate**) or disconnecting (**release**) a NAT session. **all** indicates generating logs for both of the above events.

- **all** – Generates log when the system is either allocating/releasing a port block or creating/disconnecting a NAT session.

group*group-id* | **both** - Specifies the HA group the SNAT rule belongs to. If the parameter is not specified, the SNAT rule being created will belong to HA group0. In the static port block mapping mode (**fixed-block**), the both parameter can be specified. System will divide the port range of the device under the HA Peer mode according to the HA Node ID. That is, the device of each HA Node ID uses half the port range. For example, the device of HA Node ID is 0 uses the first half of the port range, and the device of HA Node ID is 1 uses the second half of the port range.

The following is a NAT444 SNAT example:

Suppose the source IP is src_addr: 192.168.1.0/24, and the translated IP is global_addr: `200.1.2.10~200.1.2.100`

```
hostname(config-vrouter)# snatrule id 1 from src_addr to any trans-to address-book global_addr mode dynamicport fixed-block start 1024 end 65000 size 4096
rule id=1
The mapping relationship is shown as below:
hostname(config-vrouter)# show snat id 1 ports-map
-----------------------------------------------------------------
=================================================================
==================
from translate to start port end port
-----------------------------------------------------------------
192.168.1.0 200.1.2.10 1024 5119
192.168.1.1 200.1.2.10 5120 9215
192.168.1.2 200.1.2.10 9216 13311
……
192.168.1.14 200.1.2.10 58368 62463
```

```
192.168.1.15 200.1.2.11 1024 5119
192.168.1.16 200.1.2.11 5120 9215
192.168.1.17 200.1.2.11 9216 13311
……
```

To configure an SNAT rule that disables NAT444, in the NAT configuration mode, use the following command:

snatrule [**id***id*] [**before***id* | **after***id* | **top**] **from***src-address***to***dst-address* [**eif***egress-interface* | **evr***vrouter-name*] **no-trans** [**group***group-id*]

For more information, refer to the **Firewall** > **NAT** > **NAT444** topic in *StoneOS CLI User Guide*. FR 43547

Log

ID:	0x4424360e
Type:	Traffic
Severity:	Informational
Message:	[NAT444 user alloc port *protocol original_src_ip - translated_src_ip - first_src_port last_src_port*]
Description:	The system allocated a port block based on the NAT444 rule, and logged *protocol*, *original_src_ip*, *translated_src_ip*, *first_src_port* and *last_src_port* of the original packet. **Notes:** If the SNAT translation of NAT444 uses dynamic port block mapping mode (**random-block**) and is configured to allocate the same range of port blocks for TCP and UDP traffic from the same source IP address (**tcp-udp-port-consistent**): • When allocating NAT444 port blocks for TCP

	or UDP traffic from the same source IP address, the system will assign the same range of port blocks for both protocols and record only one port block allocation log. The transport protocol type (protocol) in the log will be displayed as "255". • For NAT444 port block requests for ICMP or GRE traffic, the system will no longer record related log information.
Solution:	N/A

ID:	0x4424360f
Type:	Traffic
Severity:	Informational
Message:	[NAT444 user free port *protocol original_src_ip - translated_src_ip - first_src_port last_src_port*.]
Description:	The system freed an allocated port block, and logged *protocol*, *original_src_ip*, *translated_src_ip*, *first_src_port* and *last_src_port* of the original packet. **Notes:** If the SNAT translation of NAT444 uses dynamic port block mapping mode (**random-block**) and is configured to allocate the same range of port blocks for TCP and UDP traffic from the same source IP address (**tcp-udp-port-consistent**): • When releasing NAT444 port blocks for TCP

	or UDP traffic from the same source IP address, the system will only release the port block resources when not any ports of the port blocks corresponding to these two protocols are used, and it will record only one port block release log. In this log, the transport protocol type (protocol) will be displayed as "255". • For NAT444 port block requests for ICMP or GRE traffic, the system will no longer record related log information.
Solution:	N/A

For more information, refer to *StoneOS Log Messages Reference Guide*. FR 43547

Supporting to Display and Deliver IPS Threat Logs That Carry Attack Payload

CLI

Configuring IPS Threat Logs to Carry Attack Payload

Before you start

- To deliver IPS threat logs that carry attack payload to the log server, you need to configure the log server with the log format set to "Default". For more information, refer to the **Monitor** > **Logs** > **Configuring System Logs** > **Configuring a Syslog Server** section in *StoneOS CLI User Guide*.

By default, the IPS threat logs generated by the system do not carry attack payload, making it difficult for you to perform attack analysis based on IPS threat logs. Therefore, the system allows you

to configure whether IPS threat logs carry attack payload. You can enable this function as needed. Once enabled, the IPS threat logs will carry attack payload, either for display or delivering to the log server. You can analyze these attack payloads to better respond to network security threats.

To configure the IPS threat logs to carry attack payload, in global configuration mode, use the following command:

- Enable: **threat-syslog-send-payload on**
- Disable: **threat-syslog-send-payload off**

Enabling/Disabling Base64 Encoding for Attack Payload

> **Notes:** Disabling this function may result in garbled characters when using the **show logging threat** command to view threat information. Proceed with caution.

By default, the system encodes the attack payload in IPS threat logs by using Base64. The system allows you to disable Base64 encoding for attack payloads, after which the payload will be displayed and delivered in plaintext.

To enable or disable Base64 encoding for attack payloads, in global configuration mode, use the following command:

- Enable: **threat-syslog-send-payload encode base64**
- Disable: **no threat-syslog-send-payload encode**

Viewing the Status of Attack Payload-related Functions

The system allows you to view the status of attack payload-related functions, including the function of IPS threat logs carrying attack payload and the Base64 encoding function for attack payload.

To view the status of attack payload-related functions, in any mode, use the following command:

show security configurations

Sample response:

```
hostname# show security configurations
```

threat-syslog-send-payload on (The function of IPS threat logs carrying attack payload is enabled)

no threat-syslog-send-payload encode (Base64 encoding for attack payload is disabled)

For more information, refer to the **Threat Prevention** > **IPS** > **Configuring IPS** topic in *StoneOS CLI User Guide*. FR 42751

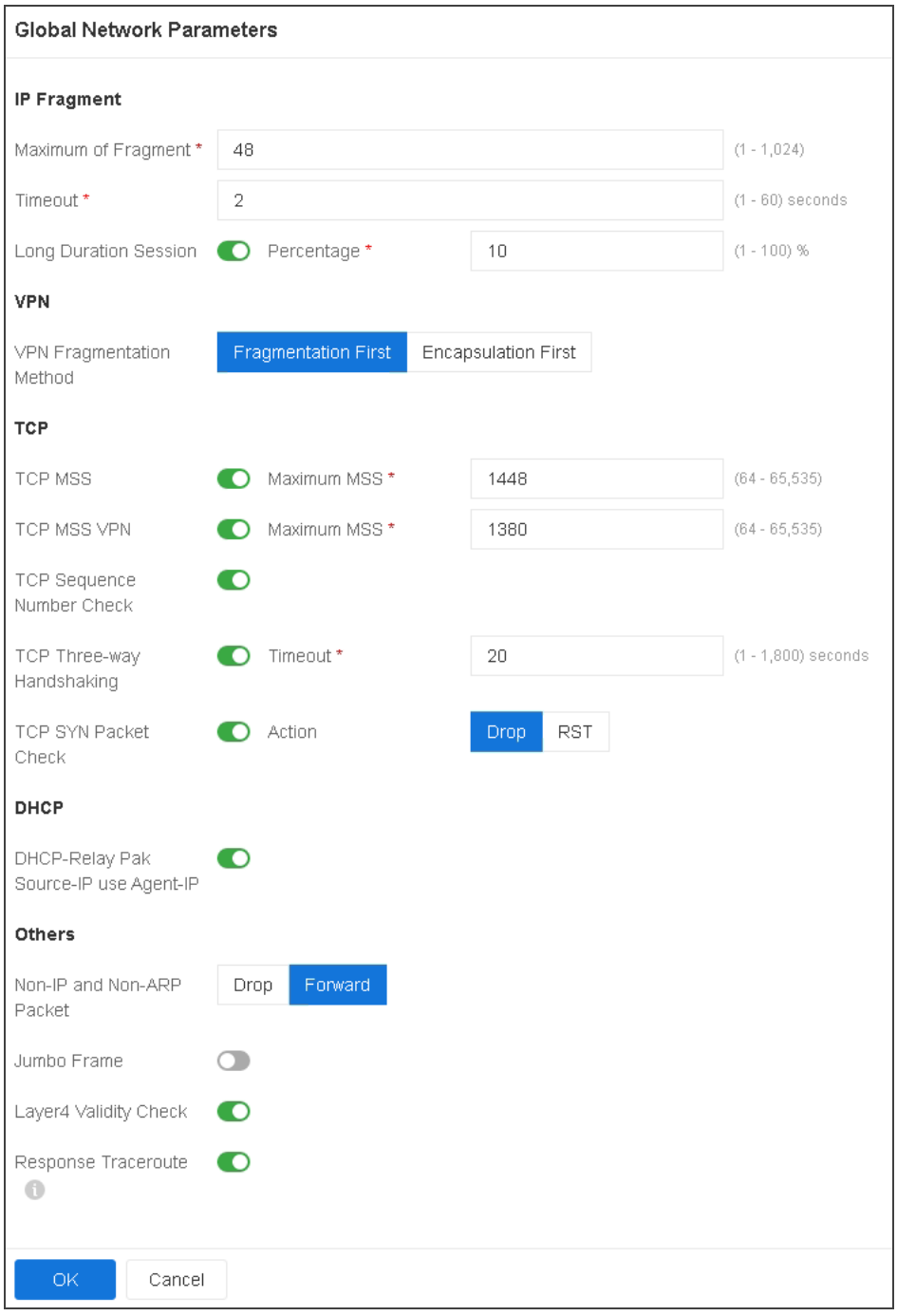
Supporting to Configure the VPN Fragmentation Method in Global Network Parameters

WebUI

Configuring Global Network Parameters

To configure global network parameters, take the following steps:

1. Select **Network > Global Network Parameters > Global Network Parameters.**



2. Configure the following parameters.

Option	Description
IP Fragment	
Maximum Fragment Number	Specifies a maximum fragment number for every IP packet. The value range is 1 to 1024. The default value is 48. Any IP packet that contains more fragments than this number will be dropped.
Timeout	Specifies a timeout period of fragment reassembling. The value range is 1 to 60. The default value is 2. If the Hillstone device has not received all the fragments after the timeout, the packet will be dropped.
Long Duration Session	Enables or disables long duration session. If this function is enabled, specify long duration session's percentage in the Percentage text box below. The default value is 10, i.e., 10% of long duration session in the total sessions.
VPN	
VPN Fragmentation Method	Specifies the fragmentation method for VPN tunnel packets, including **Fragmentation First** and **Encapsulation First**. By default, **Fragmentation First** is selected. • **Fragmentation First**: When transmitting packets via VPN tunnel, if the size of the encapsulated packet exceeds the interface MTU, the system will first fragment the packet and then encapsulate each fragment. If the encapsulated packet does not exceed the interface MTU, it will be transmitted directly. • **Encapsulation First**: When transmitting packets via VPN

Option	Description
	tunnel, the system will first encapsulate the packet. If the size of the encapsulated packet exceeds the interface MTU, the system will then fragment the packet. If the encapsulated packet does not exceed the interface MTU, it will be transmitted directly. Notes: • In ZTNA, SSL VPN, GRE, IPSec, IPv4 over IPv6, VXLAN, L2TP, and L2TPv3 tunnel scenarios, both fragmentation methods mentioned above can be applied. • In IPv6 over IPv4 tunnel scenarios, only the **Encapsulation First** method takes effect. • For X-series devicesSG-6000-K9180/K6580, only the **Fragmentation First** method takes effect when transmitting packets across service module cards (e.g., SSM module cards, SIOM module cards). Different platforms use different service module cards. For more information, refer to *Hillstone SG-6000 Hardware Reference Guide*.
TCP	
TCP MSS	Specifies a MSS value for all the TCP SYN/ACK packets. Click the **Enable** button, and type the value into the Maximum MSS

Option	Description
	text box below.
Maximum MSS	Type the max MSS value into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1448.
TCP MSS VPN	Specifies a MSS value for IPSec VPN's TCP SYN packets. Click the **Enable** button, and type the value into the Maximum MSS text box below.
Maximum MSS	Type the max MSS value for IPSEC VPN into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1380.
TCP Sequence Number Check	Configures if the TCP sequence number will be checked. When this function is enabled, if the TCP sequence number exceeds TCP window, that TCP packet will be dropped.
TCP Three-way Hand-shaking	Configures the function of TCP three-way handshaking. Click the **Enable** button to enable this function, and specify a timeout value in the Timeout text box below. The value range is 1 to 1800 seconds. The default value is 20. If the three-way handshaking has not been completed after timeout, the connection will be dropped.
TCP SYN Packet Check	Click the **Enable** button to enable this function and specify the action for TCP non-SYN packet. When the received packet is a TCP SYN packet, the TCP connection will be established. When the received packet is a TCP non-SYN packet, the packet will be processed according to the specified action.

Option	Description
	• drop: When the received packet is a TCP non-SYN packet, the system will drop the packet. • reset：When the received packet is a TCP non-SYN packet, the system will drop the packet and send RST packet to the peer device.
DHCP	
DHCP-Replay Pak Source IP use Agent-IP	Click the button to enable this function. This way, when the device acts as a DHCP relay proxy, the source IP of the DHCP relay packets is replaced with the agent IP, and the source port of the packets is changed to 67. By default, this function is disabled, indicating that the source IP of the DHCP relay packets is the IP address of the egress interface and the source port of the packets is 68.
Application Layer	
Application Layer Fast Forward	Click the button to enable this function. This way, when only the Intrusion Prevention function at the application layer is enabled and the protocol max scan length configured in the intrusion prevention rule is reached, traffic at the application layer will no longer be forwarded to the SSM module or CPU for parsing and processing. This enhances the device performance. By default, this function is disabled. **Note**: Only SG-6000-A7600/A6800 devices support this function.
Others	
Non-IP and	Specifies how to process packets that are neither IP nor ARP.

Option	Description
Non-ARP Packet	
Jumbo Frame	Click the **Enable/Disable** button to enable or disable the Jumbo Frame function. This function is disabled by default. With the Jumbo Frame function enabled, the system can forward packets less than or equal to 9216 bytes as follows: • For IPv4/IPv6 packets that are less than the MTU value of the outbound interface, forward them directly. • For IPv4 packets that are larger than the MTU value of the outbound interface, the packets are forwarded in fragments. • For IPv6 packets that are larger than the MTU value of the outbound interface, an "ICMPv6 Packet Too Big" error message will be sent to the source node of the packets, and the sender is urged to shorten the length of the packets. Notes: • When the Jumbo Frame function is enabled, the MTU configuration range of the interface will be changed. For more information about the MTU value configuration of the interface, see Configuring an Interface. • SG-6000-X25812/X25803

Option	Description
	/X8180SG-6000-A7600/A6800SG-6000-K9180/K6580K7680/K6280-GS/K2680/K2380does not support the Jumbo Frame function.
Layer4 Validity Check	Enable/Disable validity check for Layer 4 protocol. By default, this function is enabled. Layer 4 indicates the transport layer of the OSI model, which provides end-to-end communication between devices and ensures the integrity of data transmission. When this function is enabled, the system checks TCP packets at Layer 4, such as checking whether the flag of TCP is valid and whether the port number is valid. If the TCP packet is abnormal, it will be dropped.
Response Traceroute	Enable/Disable the Response Traceroute function. By default, this function is enabled. By default, the system will respond to traceroute traffic passing through the device. When the traceroute traffic is not sent or received by the device itself, you can disable the Response Traceroute function to prevent the device from responding to traceroute traffic that does not belong to the device itself. This way, the IP address of the device is hidden, which reduces the possibility of the device being discovered and attacked. **Note**: This parameter takes effect only for traceroute traffic that does not belong to the device itself. For traceroute traffic that does not belong to the device itself, whether this function is enabled does not affect the response of the device to the traffic.

3. Click **OK**.

For more information, refer to the **Network** > **Global Network Parameters** topic in *StoneOS_WebUI_User_Guide*. FR 43479

CLI

Configuring VPN Fragmentation

This section consists of:

- Specifying the VPN fragmentation method
- Viewing the VPN fragmentation method used by the system

Specifying the VPN Fragmentation Method

To ensure normal packet transmission via VPN tunnel, the system supports to specify the fragmentation method for VPN tunnel packets, including **Fragmentation First** and **Encapsulation First**. By default, **Fragmentation First** is used.

- **Fragmentation First**: When transmitting packets via VPN tunnel, if the size of the encapsulated packet exceeds the interface MTU, the system will first fragment the packet and then encapsulate each fragment. If the encapsulated packet does not exceed the interface MTU, it will be transmitted directly.
- **Encapsulation First**: When transmitting packets via VPN tunnel, the system will first encapsulate the packet. If the size of the encapsulated packet exceeds the interface MTU, the system will then fragment the packet. If the encapsulated packet does not exceed the interface MTU, it will be transmitted directly.

Notes:

- In ZTNA, SSL VPN, GRE, IPSec, IPv4 over IPv6, VXLAN, L2TP, and L2TPv3 tunnel scenarios, both fragmentation methods mentioned above can be applied.
- In IPv6 over IPv4 tunnel scenarios, only the **Encapsulation First** method takes effect.
- For X-series devicesSG-6000-K9180/K6580, only the **Fragmentation First** method takes effect when transmitting packets across service module cards (e.g., SSM module cards, SIOM module cards).
- Different platforms use different service module cards. For more information, refer to *Hillstone SG-6000 Hardware Reference Guide*.

To specify the **Encapsulation First** method, in global configuration mode, use the following command:

vpn-fragment-post-frag

To restore the default fragmentation mode, in global configuration mode, use the following command:

no vpn-fragment-post-frag

Viewing the VPN Fragmentation Method Used by the System

To view the VPN fragmentation method used by the system, in any mode, use the following command:

show vpn-fragment-post-frag

If the returned result is as follows, the VPN fragmentation method used by the system is **Fragmentation First**.

```
hostname#show vpn-fragment-post-frag
vpn-fragment-post-frag: disabled
```

If the returned result is as follows, the VPN fragmentation method used by the system is **Encapsulation First**.

```
hostname#show vpn-fragment-post-frag
vpn-fragment-post-frag: enable
```

For more information, refer to the **Firewall** > **Global Network Parameters** > **Configuring VPN Fragmentation** section in *StoneOS_CLI_User_Guide*. FR 43479

BGP Route Reflector

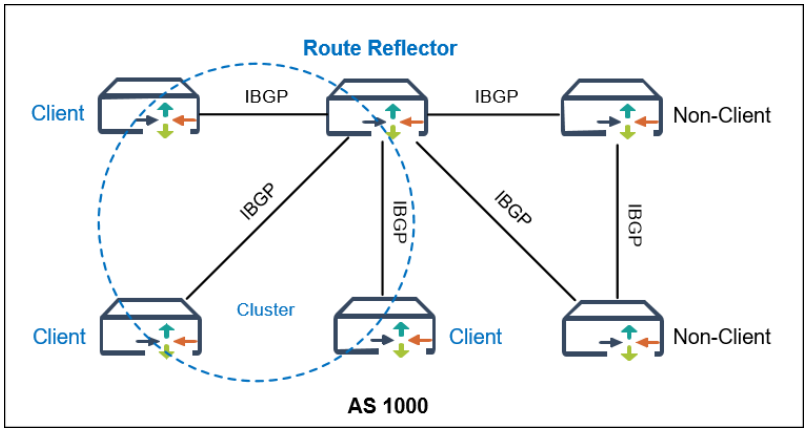
To ensure the exchange of routing information between IBGP peers within an Autonomous System (AS), the traditional practice is to establish full-mesh connectivity between these peers. However, as the network scale expands and the number of IBGP peers increases dramatically, making the configuration of a full-mash network complex and resource-intensive in terms of both network and CPU resources.

To resolve this issue, the system supports the BGP Route Reflector function. BGP Route Reflector is a network optimization mechanism that allows one or more devices within an AD to be configured as route reflectors, with other BGP devices connecting to them as clients. Route reflectors server as information storage and forwarding centers, responsible for reflecting (forwarding) routing information between clients, thus avoiding the need for establishing full-mesh connectivity among a large number of IBGP peers.

Basic Principles of BGP Route Reflectors

Within an AS, a router is configured as a Route Reflector (RR), while other routers are configured as clients or non-clients as required. RR and clients form a cluster, where clients within the same cluster only need to establish IBGP connections with RR to exchange routing information, without the need to establish IBGP connections with other clients. This reduces the number of IBGP connections within the AS.

As shown in the figure below, within AS1000, six routers are present. One router is configured as an RR, three routers as clients, and the remaining two as non-clients. The RR and clients form a cluster. In this configuration, only six IBGP connections need to be established, significantly fewer than the 15 connections required without RR configuration (calculated by using n(n-1)/2). Note that non-clients still need to establish full-mesh connectivity with RR and other non-clients.



Roles of route reflector:

- Route Reflector (RR): BGP devices within an AS that reflect route learned from IBGP peer to other IBGP peers.
- Client: IBGP devices forming reflection neighbor relationships with RR. Within the AS, client only needs to connect to the RR.
- Non-Client: IBGP devices that are neither RR nor clients. Within the AS, non-clients still need to establish full-mesh connectivity with the RR and all other non-clients.
- Originator: Devices originating routes within the AS. They have an Originator_ID attribute used to prevent route loops within a cluster.
- Cluster: A set of RR and RR clients. It has a Cluster_List attribute used to prevent route loops between clusters.

Route reflection rules of RR:

- Routes learned from non-client are advertised to all clients of this RR.
- Routes learned from client are advertised to all clients and non-clients of this RR.
- Routes learned from EBGP neighbors are advertised to all clients and non-clients of this RR.

Route Loop Prevention Mechanism of BGP Route Reflector

BGP route reflector prevents route loops by using the Originator_ID and Cluster_List attributes.

The Originator_ID, created by the RR, carries the Router ID of the route originator within the AS. The Originator_ID attribute prevents route loops within a cluster:

- When an RR initially reflects a route, it adds the Originator_ID attribute to the route to identify the device initiating the route. If the RR detects that the route already contains the Originator_ID attribute, it will not create an Originator_ID attribute.
- When other BGP peers receive this route, they compare the received Originator_ID with their own Router ID. If they match, it indicates that the route was initiated by themselves, so they will ignore the route, thus preventing route loops.

Within the AS, each RR uses a unique Cluster_ID for identification. The Cluster_List attribute records all Cluster_IDs that the route traverses during reflection, representing the complete RR path of route reflection. The Cluster_List attribute prevents route loops between clusters:

- When an RR initially reflects a route, it adds its own Cluster_ID to the Cluster_List. If the route does not contain a Cluster_List, the RR creates one.
- When an RR receives a route update, it checks the Cluster_List of the route. If the local Cluster_ID is already in the Cluster_List, it indicates that the route has already passed through the current RR, so the RR discards the route to avoid loops. If the local Cluster_ID is not in the Cluster_List, the RR adds it and continues to reflect the updated route.

For more information, refer to the **Routing** > **Dynamic Routing** > **Configuring BGP** topic in *StoneOS CLI User Guide* or **Advanced Routing** > **Configuring BGP** topic in *StoneOS WebUI User Guide*. FR43483

CLI

Configuring BGP Protocol

You can configure the BGP protocol for different VRouters respectively. The BGP protocol configuration includes:

- Entering the BGP configuration mode
- Specifying a Router ID
- Creating a route aggregation
- Adding a static BGP route
- Configuring a timer
- Specifying the administration distance of BGP route
- Specifying the default metric
- Configuring redistribute
- Creating a BGP peer group
- Adding a BGP peer to the peer group
- Configuring a BGP peer
- Activating a BGP connection
- Configuring the default information originate
- Configuring description
- Configuring a BGP peer timer
- Configuring the next hop as itself

- Configuring EBGP multihop
- Disabling a peer or peer group
- Resetting a BGP connection
- Configuring an AS-path access list
- Configuring BGP communities
- Redistributing routes into BGP
- Configuring a route map
- Modifying attributes of introduced routing information
- Configuring route filters based on the AS-path access list
- Sending communities path attributes to peers or peer groups
- Configuring route filters based on the route map
- Configuring equal cost multipath routing
- Enabling/Disabling multipath-relax of EBGP
- Configuring BGP GR
- Configuring BGP Route Reflector

Configuring a BGP Route Reflector

It contains the following configurations:

- Configuring BGP route reflector client
- Configuring BGP route reflector Cluster_ID
- Allow/block client-to-client route reflection

Notes: BGP route reflector configuration is required only on the RR, not on the client.

Configuring a BGP Route Reflector Client

To configure IBGP peers as clients of the route reflector, use the following command in BGP instance configuration mode:

neighbor {*A.B.C.D* | *X:X:X:X::X* | *peer-group*} **route-reflector-client**

- *A.B.C.D* | *X:X:X:X::X* | *peer-group* - Specifies the IPv4 address (*A.B.C.D*), IPv6 address (*X:X:X:X::X*), or the name of the peer group (*peer-group*) of the IBGP peer.

To remove the configuration of route reflector client, in BGP instance configuration mode, use the **no neighbor** {*A.B.C.D* | *X:X:X:X::X* | *peer-group*} **route-reflector-client** command.

Configuring BGP Route Reflector Cluster_ID

To configure the Cluster_ID of the route reflector, use the following command in BGP instance configuration mode:

cluster-id {*A.B.C.D* | *number*}

- *A.B.C.D* | *number* - Specifies the Cluster_ID of the route reflector as an IPv4 address (*A.B.C.D*) or a decimal number (*number*). By default, the Router ID of the route reflector is used.

To remove the configuration of the BGP route reflector Cluster_ID, use the command **no cluster-id** in BGP instance configuration mode.

Allowing/Blocking Client-to-Client Route Reflection

In some network environments where IBGP full-mesh connections exist between route reflector clients, the clients do not need to reflect routes by using the RR to avoid unnecessary consumption of bandwidth resources. In such cases, you can block route reflection between clients to reduce route updates. By default, the system allows client-to-client route reflection. To allow or block

client-to-client route reflection, use the following commands in BGP instance configuration mode:

- Allow: **client-to-client reflection**
- Block: **no client-to-client reflection**

For more information, refer to the **Routing** > **Dynamic Routing** > **Configuring BGP** topic in *StoneOS CLI User Guide*. FR43483

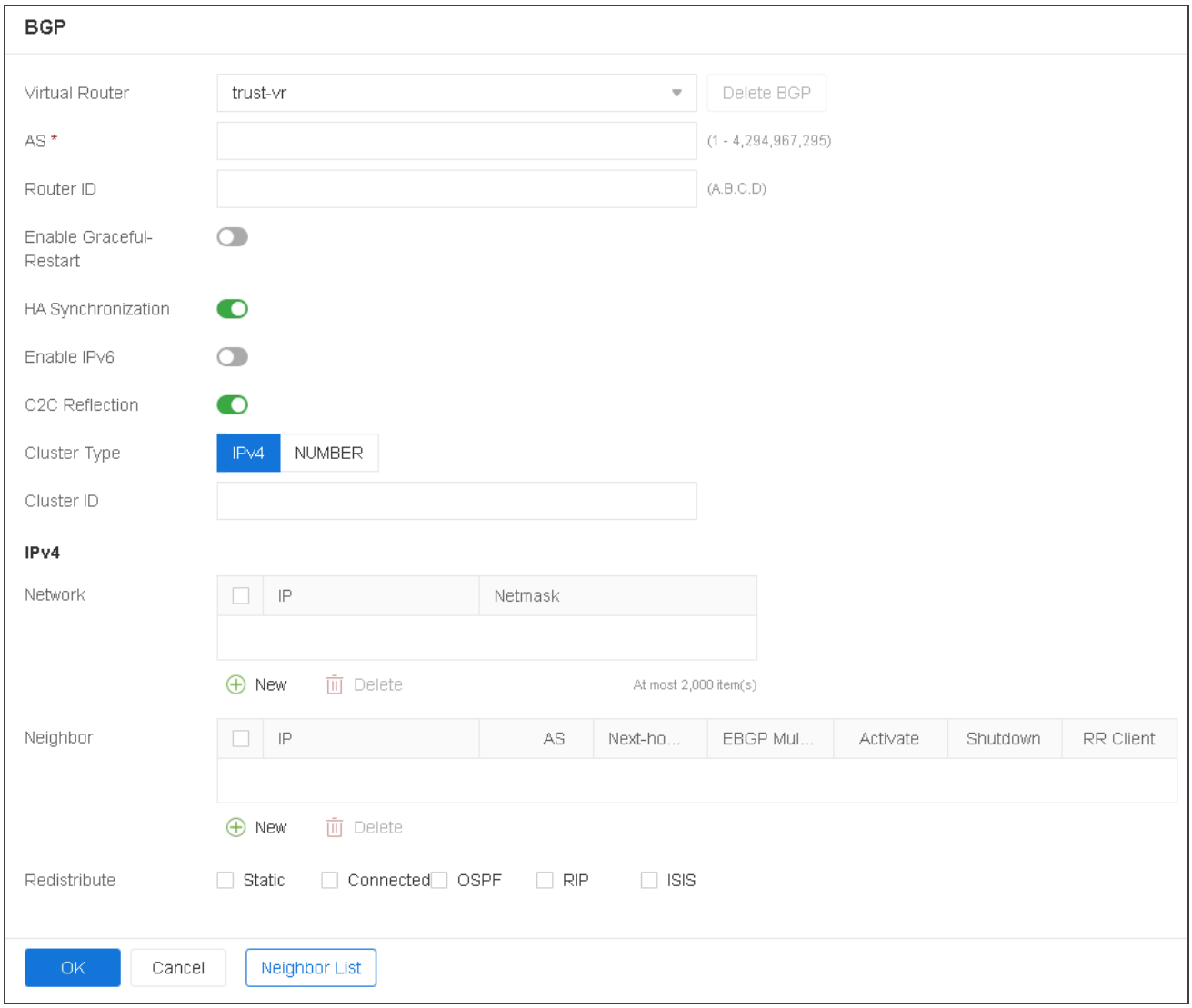
WebUI

Configuring BGP

To configure a basic process, take the following steps:

1. Select **Network** > **Routing** > **BGP**.
2. Select a VR from the **Virtual Router** drop-down list. The default VR is "trust-vr".

3. In this page, enter the basic information of BGP.



4. Configure the options as follows:

Option	Description
AS	Specifies the number of Autonomous System, ranging from 1 to 4294967295.
Enable Graceful-Restart	Click the **Enable** button.

Option	Description
	• Graceful-Restart Restart-Time: Specifies the longest time for a peer to wait for a BGP session to be re-established. The time range from 1 to 3600 seconds. The default Graceful-Restart Restart-Time is 120 seconds. • Graceful-Restart Stale-Path-Time: Specifies the longest time to retain the stale routes of the restarted peers. The time range from 1 to 3600 seconds. The default Graceful-Restart Stale-Path-Time is 360 seconds. • Graceful-Restart Wait-For-Rib-Time: Specifies the longest time for the GR Restarter to wait for the End-of-RIB markers from the neighbors. The time range from 1 to 3600 seconds. The default Graceful-Restart Wait-For-Rib-Time is 180 seconds.
Router ID	Specifies the router ID of the router running the BGP. The router ID is the unique identifier of an router in the BGP domain. The router ID should be in the format of IP address.
Enable IPv6	Click the **Enable** button to support the format of IPv6 address.
HA sync	Click this button to enable the HA Sync function,

Option	Description
	which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
Enable IPv6	Click the **Enable** button to expand the IPv6 configuration items.
C2C Reflection	Click the **Enable** button to enable the C2C Reflection function to allow client-to-client route reflection. However, in some network environments, IBGP full-mesh connection has already been established between the clients of the route reflector, in which case the clients do not need to reflect routes by using the RR to avoid occupying unnecessary bandwidth resources. In this case, you can block route reflection between clients, thus reducing route updates. By default, the C2C reflection function is enabled.
Cluster Type	Specifies the type of cluster composed of route reflector and clients, which can be "IPv4" or "Number".
Cluster ID	Specifies the Cluster_ID of the route reflector, if

Option	Description
	the cluster type is IPv4, you need to enter the IPv4 address; if the cluster type is Number, you need to enter the decimal number.
IPv4	
Network	You can add the specified network in the local routing table to the BGP routing table, and remove the specified network from the list. Then the network will be learned by the neighbor router configured later. • Add: Click **Add**, and specify the IPv4 address and netmask. When IPv6 is enabled, you can specify the IPv6 address and prefix. • Delete: If you want to delete the specified network, click **Delete**.
Neighbor	You can add neighbor routers to exchange routing information with the specified router, or delete the specified router from the list. You can add at most 8 neighbor routers. • Add: To add a neighbor router, click **Add** and enter the information as follows. • **IP**: Enter the IP address of the specified neighbor router.

Option	Description
	• **AS**: Specify the AS number of the neighbor router, ranging from 1 to 4294967295. • **Next-hop Self**: For a neighbor router of the EBGP, if the next-hop address of the IBGP of the neighbor router cannot be reached, you should enable the next-hop as self. • **EBGP Multihops**: For BGP running between different AS (i.e., EBGP), if the specified router and its neighbor router are not directly connected, you need to configure EBGP multi-hops, ranging from 0 to 255. • **Activate**: You can activate the BGP connection between the configured neighbor router and the current device. By default, the function is enabled. • **Shutdown**: You can shutdown the neighbor router in the list. When it's shut down, all sessions with the neighbor router will be cut and all router

Option	Description
	information will be cleared. By default, the function is disabled. • **Route Map In**: Filter routes that are accepted by the neighbor router by using the route map. Only the acceptance of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see Route Map. • **Route Map Out**: Filter routes that are advertised by the neighbor router by using the route map. Only the advertisement of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more

Option	Description
	information about how to configure a route map, see Route Map. • **RR Client**: Configure the IBGP neighbor as a client of route reflector. • Delete: To delete the specified neighbor router, click **Delete**.
Redistribute	When IPv4 is supported, the following routing protocols can be introduced and redistributed. • **Static**: Select the check box to redistribute the static route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see Route Map. • **Connected**: Select the check box to redis-

Option	Description
	tribute the connected route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see Route Map. • **OSPF**: Select the check box to redistribute the OSPF route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map,

Option	Description
	see Route Map. • **RIP**: Select the check box to redistribute the RIP route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see Route Map. • **IS-IS**: Select the check box to redistribute the IS-IS route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Con-**

Option	Description
	figuration panel. For more information about how to configure a route map, see Route Map. When IPv6 is supported, the following routing protocols can be redistributed and advertised. • **Static**: Select the check box to introduce the static route protocol into the BGP route and redistribute. • **Connected**: Select the check box to introduce the connected route protocol into the BGP route and redistribute. • **OSPFv3**: Select the check box to introduce the OSPFv3 route protocol into the BGP route and redistribute. • **RIPng**: Select the check box to introduce the RIPng route protocol into the BGP route and redistribute. • **ISISv6**: Select the check box to introduce the ISISv6 route protocol into the BGP route and redistribute.

5. Click **OK** to save the configurations. The newly-created neighbor router will be displayed in the list.

For more information, refer to the **Advanced Routing** > **Configuring BGP** topic in *StoneOS WebUI User Guide*. FR43483

Supporting to Configure the Switch of Sending Heartbeat Packets

CLI

Enabling/Disabling the Function of Sending Heartbeat Packets

By default, after the 802.1X client is successfully authenticated, the firewall device periodically sends heartbeat packets to the client to track the online status of users. If the client uses the Windows built-in 802.1X client for authentication, the client may still prompt users to re-enter their credentials upon receiving heartbeat packets, even after successful authentication. To avoid this issue, the system allows manually disabling the function of sending heartbeat packets. Once disabled, the firewall device will no longer track the online status of users.

To enable/disable the function of sending heartbeat packets, in dot1x configuration mode, use the following command:

- Enable (default status): **keep-alive enable**
- Disable: **keep-alive disable**

Notes:

- After you disable the function of sending heartbeat packets, the configuration of the **dot1x timeout***timeout-value* command cannot take effect. To make it take effect, turn on the switch of sending heartbeat packets first.
- After you disable the function of sending heartbeat packets, the firewall cannot detect users who disconnect normally and you need to manually kick out disconnected users. For more information, see User Authentication > 802.1X Authentication.

Configuring the Timeout of Authenticated Clients

> **Notes:** To ensure this function can take effect, we recommend that you first use the **show dot1xprofile** *profile-name* command to confirm that the "keep-alive" function is enabled. If it is disabled, enable the function of sending heartbeat packets in dot1x configuration mode by using the **keep-alive enable** command.

You can configure the authentication timeout value for authenticated clients. If the client does not respond within the specified time, it need reapply an authentication. To configure the timeout value, in the global configuration mode, use the following command:

dot1x timeout*timeout-value*

- *timeout-value* – Specifies the client authentication timeout value. The value range is 180 to 3600*24 seconds. The default value is 300.

To restore to the default value, in the global configuration mode, use the command **no dot1x timeout**.

For more information, refer to the **User Authentication > Configuring 802.1X Authentication** topic in *StoneOS CLI User Guide*. FR 41579

A New Session Can Be Created When New TCP SYN Packets Are Received During Session Delay Invalidate

CLI

A New Session Can Be Created When New TCP SYN Packets Are Received During Session Delay Invalidate

If a TCP SYN packet the system receives matches a session that is in DELAY INVALIDATE, subsequent packets may be discarded, resulting in data loss. Therefore, you can configure that a new session can be created when new TCP SYN packet is received at a time when the matched session

is in DELAY INVALIDATE. With this function configured, if the newly received TCP SYN packet matches a session that is in DELAY INVALIDATE, the system will delete that matched session and at the same time create a new session with the same quintuple for subsequent packet forwarding.

To configure that a new session can be created when new TCP SYN packet is received at a time when the matched session is in DELAY INVALIDATE, use the following command in the Flow configuration mode:

support-tcp-time-wait-reuse

To disable the function that a new session can be created when new TCP SYN packet is received at a time when the matched session is in DELAY INVALIDATE, use the following command in the Flow configuration mode:

no support-tcp-time-wait-reuse

To view the status of the function that a new session can be created when new TCP SYN packet is received at a time when the matched session is in DELAY INVALIDATE, use the following command in any mode:

show flow support-tcp-time-wait-reuse

For more information, refer to **Firewall** > **StoneOS Architecture** in *StoneOS_CLI_User_Guide*.
FR 40315

Supporting to Perform Email-based Deployment by Using HSM

WebUI

Email-based Deployment

When deploying firewalls in an SD-WAN scenario, O&M personnel need to go to the site to configure and deploy the device. When there are a large number of devices and they are widely distributed, the O&M personnel need to manually configure each device, which affects the efficiency of device deployment and increases the cost of device O&M. Therefore, the system provides the email-based deployment function, where administrators configure and send deployment emails on

the HSM. Deployment personnel start the deployment process by accessing the URL in the deployment email, enabling remote configuration and deployment of devices, effectively reducing deployment costs.

Before you start

- The administrator has completed the configuration on the HSM and sent the deployment email. For more information about how to configure the deployment email, see **ZTP in SD-WAN Scenario** in *HSM WebUI User Guide*.
- The deployment personnel confirm that the deployment email has been successfully received, and contacts the administrator to obtain the email URL key.
- The deployment personnel confirms that the device has been racked and powered on successfully.

To perform email-based deployment, the deployment personnel needs to take the following steps:

1. Check if the device SN in the deployment email matches the SN of the firewall to be deployed. If they match, proceed to the next steps. If not, contact the administrator to resend the deployment email.
2. Use an Ethernet cable to connect the PC to the MGT interface of the firewall device (or e0/0 interface if MGT interface is unavailable). On the PC, set the IP address of the Ethernet property to an IP address in the same CIDR block as 192.168.1.1/24, for example, 192.168.1.2/255.255.255.0.
   For A200W devices, you can also connect to the default WLAN access device named "WIFI0/0_xxxxxx" (where "xxxxxx" is the last six digits of the firewall device SN), with WLAN security mode set to unencrypted and no key required.
3. The deployment personnel access the URL provided in the deployment email to access the login page of the firewall device.

4. Enter the username and password of the firewall device (default: hillstone/hillstone), then click "Login" to enter the Email-based Deployment page.

5. Enter the obtained email URL key obtained, then click **OK** to enter the **Configuration Information** page to view the deployment configuration information. The deployment configuration information consists of WAN/LAN port configuration, DNS configuration, NTP configuration, and connecting to HSM.

6. Click **OK**, and the firewall device will be automatically configured based on the deployment configuration information and registered into HSM.

For more information, refer to **System Management** in *StoneOS WebUI User Guide*. FR 41415

Supporting to Synchronize FTP Pinhole Information in HA A/P Mode

CLI

Manually Synchronizing HA Information

In some special cases, the master and backup configuration information may not be synchronized. At this time, you need to manually synchronize the configuration information of the master and backup devices. You can determine whether manual synchronization is required by using the following methods:

1. Run the corresponding *show* command on the master and backup devices respectively to view the relevant configuration information, or run the **exec ha sync configuration check** command to query whether the configuration information of the master and backup devices is consistent.

2. Based on the configuration information displayed, determine whether manual synchronization is required:

- If the displayed configuration information is consistent, manual synchronization is not required;
- If the displayed configuration information is inconsistent, you can run the **exec ha sync configuration difference** [**all**] (**all** indicates to compare the configuration information of all VSYSs) command to check the difference between the master and backup devices, and then you need to manually run the corresponding command to complete the synchronization of the configuration information (For more information about the relevant show commands and execute commands, see the following table).

Notes:

- When there is inconsistency in local configuration information, such as hostname, interface configuration of the Local attribute, and HA configuration.
- For dynamic information, such as sessions, manual synchronization is required only when normal dynamic information is not synchronized.

The following table describes the manual synchronization configuration commands:

HA Synchronization Information	show command	manual synchronization command
All static configuration and dynamic data	**show ha sync state all**	**exec ha sync all**
Configuration information	**show configuration**	**exec ha sync configuration**
File information	**show file**	**exec ha sync file***file-name*
ARP entry	**show arp**	**exec ha sync rdo arp**

HA Synchronization Information	show command	manual synchronization command
DNS configuration information	show ip hosts	exec ha sync rdo dns
DNS rewrite rule information	show dns-rewrite-rule	exec ha sync rdo dns-rewrite
DHCP configuration information	show dhcp	exec ha sync rdo dhcp
MAC address table	show mac	exec ha sync rdo mac
PKI configuration information	show pki key	exec ha sync rdo pki
	show pki trust-domain	
Session information	show session	exec ha sync rdo session
IPSec VPN information	show ipsec sa	exec ha sync rdo vpn
	show isakmp sa	

HA Synchronization Information	show command	manual synchronization command
SCVPN information	show scvpn client test	exec ha sync rdo scvpn
	show scvpn host-check-profile	
	show scvpn pool	
	show scvpn user-host-binding	
	show scvpn session	
	show auth-user scvpn	
L2TP information	show l2tp tunnel	exec ha sync rdo l2tp
	show l2tp pool	
	show l2tp client {tunnel-name*name* [user *user-name*] | tunnel-id *ID*}	
	show auth-user l2tp [interface *interface-name* | vrouter*vrouter-name* | slot *slot-no*]	
Web authentication information	show auth-user webauth	exec ha sync rdo webauth
NTP information	show ntp	exec ha sync rdo ntp

HA Synchronization Information	show command	manual synchronization command
SCVPN information	show scvpn	exec ha sync rdo scvpn
Route information	show ip route	exec ha sync rdo route
IGMP information	show ha sync statistic igmp	exec ha sync rdo igmp
	show ha sync state igmp	
Pinhole information	show ha sync rdo pinhole config	exec ha sync rdo pinhole

Enabling/Disabling Automatic Synchronization of HA Pinhole Information

Some applications (such as FTP and SIP) use multi-channel data transmission, where the control channel and data channel are separated. The IP address and port information of the data channel are negotiated in advance by the control channel. When the ALG function of the firewall is enabled, the system stores the IP address and port information of the data channel in the Pinhole information. Packets matching the Pinhole information can then pass through the firewall, ensuring normal communication for multi-channel applications.

By default, Pinhole information is automatically synchronized between HA devices operating in Active-Passive (A/P) mode. However, synchronizing Pinhole information generates certain traffic, which may impact device performance under high load. You can enable or disable the automatic synchronization of HA Pinhole information based on device load conditions to ensure stability.

To enable or disable automatic synchronization of HA Pinhole information, in global configuration mode, use the following command:

- Enable: **ha sync rdo pinhole enable**
- Disable: **ha sync rdo pinhole disable**

Notes: The system supports only to synchronize Pinhole information of the FTP protocol.

For more information, refer to the **High Availability (HA) > Configuring HA > Manually Synchronizing HA Information** section in *StoneOS CLI User Guide*. FR 43007

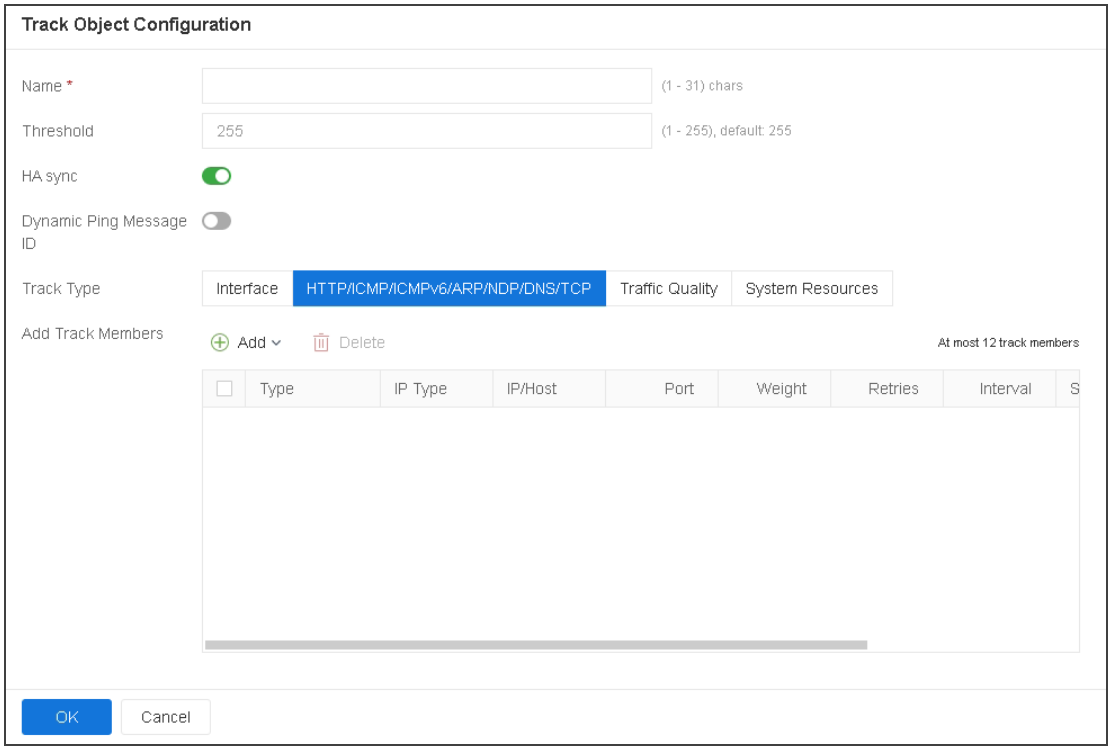
Supporting to Track the CPU Utilization and Memory Utilization of Device

WebUI

Creating a Track Object

To create a track object, take the following steps:

1. Select **Object > Track Object**.
2. Click **New**.



Option	Description
Name	Specifies a name for the new track object.
Threshold	Type the threshold for the track object into the text box.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.
Dynamic Ping Message ID	Select this check box to enable the Dynamic Ping Message ID function. With this function enabled, the header ID of ICMP messages sent by the same track object is a dynamic value. This function is disabled by default. With this function disabled, the header ID of ICMP messages sent by the same track object is a fixed value.

Track Type	Select a track object type, which can be "Interface", "HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP", or System Resources. One track object can only be configured with one type.
	Select Interface
	• Click **Add** in Add Track Members section and then configure the following options in the Add Interfaces dialog box:
	  • Interface - Select a track interface from the drop-down list.
	  • Weight - Specifies a weight for the interface, i.e. the weight for overall failure of the whole track object if this track entry fails.
	• Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member.

Option	Description

	• Delete: From the track member list, select a check box and click **Delete** to delete the track member.
	Select HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP
	• Click **Add**, select a packet type from the drop-down list, and then configure the following options in the Add HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP Member dialog box:
	  • IP Type - Specifies the IP type for the track object when the track is implemented by HTTP/DNS/TCP packets.
	  • IP/Host - Specifies an IP address or host name for the track object when the track is implemented by HTTP/ICMP/ICMPv6/TCP packets.
	  • IP - Specifies an IP address for the track object when the track is implemented by ARP/NDP packets. DNS - Specifies an IP address for the track object when the track is implemented by DNS packets.
	  • Weight - Specifies a weight for overall failure of the whole track object if this track entry fails.
	  • Retries: Specifies a retry threshold. If no response packet is received after the specified times of retries, system will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255.

Option	Description
	The default value is 3. • Interval - Specifies an interval for sending packets. The value range is 1 to 255 seconds. The default value is 3. • Egress Interface - Specifies an egress interface from which HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP packets are sent. • Source Interface- Specifies a source interface for HTTP/ICMP/ICMPv6/ARP/DNS/TCP packets. • Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member. • Delete: From the track member list, select a check box and click **Delete** to delete the track member. **Select Traffic Quality**: • Click **Add** in Add Track Members section and then configure the following options in the Add Traffic Quality Member dialog box: • IP Type - Specifies the address type of the traffic quality member, including IPv4 and IPv6. When "IPv4" is specified, only the IPv4 traffic of the tracked interface; when "IPv6" is specified, only the IPv6 traffic of

Option	Description
	the tracked interface. • Interface - Specifies the name of the tracked interface. • Interval - Specifies the duration of per track period. The unit is second. The value range is 1 to 255. The default value is 3. After a track period is finished, system will reset the tracked value of new session. • Retries - Specifies the threshold value which concludes the track entry is failed. The value range is 1 to 255. The default value is 3. • Weight - Specifies how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255. • Low Watermark - Specifies the failure threshold value of new session success rate. The value range is 0 to 100. The default value is 30. During a track period, when the new session success rate is below the specified low watermark, system will conclude the track is failed. • High Watermark- Specifies the failure threshold value of new session success rate. The value range is 0 to 100. The default value is 50. During a track period, when the new session success rate exceeds the specified low watermark, system will conclude the track is

Option	Description
	successful. • Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member. • Delete: From the track member list, select a check box and click **Delete** to delete the track member. **Note**: During a track period, when the new session success rate is equal to or exceeds the low watermark, and is equal to or below the low watermark, system will keep the previous track state. **Select System Resources to track the CPU utilization and memory utilization of the device, and automatically shut down interfaces based on the track results.** • Click **Add** to add a track member of the system resources type, including **CPU** and **Memory**. • CPU Name: Specifies the name of the CPU to be tracked. If set to **Any**, it indicates all CPUs on the SIOM module and SSM module of the tracked device. If the CPU utilization or memory utilization of any CPU on the SIOM module and SSM module reaches the threshold, it is considered a track failure.**Note**: This parameter is only supported on certain devices (X series, K9180, K6580).

Option	Description
	• Threshold: Specifies the threshold for determining a track member failure. If the CPU utilization or memory utilization reaches the threshold, it is considered a track member failure. Valid values: 1 to 100. Default value for CPU: 85. Default value for memory: 95. • Weight: Specifies the weight that the failure of this track member contributes to the failure of the overall track object. If the total weight contributed by all failed track members under the same track object reaches the threshold configured for the track object, it is considered a track object failure. Valid values: 1 to 255. Default value: 255. • Edit: Select a track member in the track member list and click **Edit** to edit it. • Delete: Select a track member in the track member list and click **Delete** to delete it. **Notes:** The track object of the System Resources type can only be referenced when automatically shutting down interfaces. For more information, refer to **Network** > **Interface** > **Configuring an Interface** in *StoneOS WebUI User Guide*.

3. Click **OK.** The created track object will be displayed in the track object list.

For more information, refer to **Object** > **Track Object** in *StoneOS WebUI User Guide*. FR 40631

CLI

Tracking System Resources

The system supports to track CPU utilization and memory utilization of the device. Based on the track results, it can control the automatic shutdown of interfaces. If the threshold configured for the track object is reached, the system will forcibly shut down the specified interface, enhancing the stability and reliability of network communication to a certain extent.

- Tracking CPU Utilization
- Tracking Memory Utilization

Notes: For more information about how to configure the automatic shutdown of interfaces, see Configuring Interface Force Shutdown.

Tracking CPU Utilization

To track CPU utilization, in track object configuration mode, use the following command:

cpu {**any** | *cpu_name*} [**threshold** *value*] [**weight** *value*]

- **any** | *cpu_name* – Specifies the name of the CPU to be tracked. When set to "any", it tracks all CPUs on the SIOM module and SSM module of the device. If the CPU utilization of any CPU on the SIOM module and SSM module reaches the threshold, it is considered a track member failure.



Device Supported: : This parameter is only supported on certain devices (X series, K9180, K6580).

- **threshold** *value* – Specifies the threshold for determining a track member failure. If the CPU utilization reaches the threshold, it is considered a track member failure. Valid values: 1 to 100. Default value: 85.
- **weight** *value* – Specifies the weight that the failure of this track member contributes to the failure of the overall track object. If the total weight contributed by all failed track members under the same track object reaches the threshold configured for the track object, it is considered a track object failure. Valid values: 1 to 255. Default value: 255.

Tracking Memory Utilization

To track memory utilization, in track object configuration mode, use the following command:

memory {**any** | *cpu_name*} [**threshold** *value*] [**weight** *value*]

- **any** | *cpu_name* – Specifies the name of the CPU to be tracked. When set to "any", it tracks all CPUs on the SIOM module and SSM module of the device. If the memory utilization of any CPU on the SIOM module and SSM module reaches the threshold, it is considered a track member failure.

> **Device Supported:** : This parameter is only supported on certain devices (X series, K9180, K6580).

- **threshold** *value* – Specifies the threshold for determining a track member failure. If the memory utilization reaches the threshold, it is considered a track member failure. Valid values: 1 to 100. Default value: 85.
- **weight** *value* – Specifies the weight that the failure of this track member contributes to the failure of the overall track object. If the total weight contributed by all failed track members under

the same track object reaches the threshold configured for the track object, it is considered a track object failure. Valid values: 1 to 255. Default value: 255.

Track Object Failure Threshold

If the sum of weight values of all track entries exceeds or equals to a certain value, the system concludes that the tracking fails. The value is known as the track object failure threshold value.

To configure the track object failure threshold value, in the track object configuration mode, use the following command:

threshold*value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no threshold

Configuring Interface Force Shutdown

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

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

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

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

- **schedule***schedule-name* – Specifies a schedule. If this parameter is specified, the interface will remain shut during the schedule time. For information on the time schedule, see Creating a Schedule of System Management.

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

For more information, refer to the **System Management > Configuring a Threshold** topic in *StoneOS CLI User Guide*. FR 40631

Supporting to Configure the Maximum Number of SIP Registrations and SIP Dialogs

CLI

ALG SIP Communication Optimization

In high-concurrency communication scenarios, when you use the ALG SIP function for communication, normal communication can be affected if the number of SIP registrations or SIP dialogs reaches the default upper limit of the system. Therefore, the system allows you to flexibly configure the maximum number of SIP registrations and SIP dialogs based on your requirements, preventing the limit from affecting normal communication.

- Configuring the Maximum Number of SIP Registrations
- Configuring the Maximum Number of SIP Dialogs

Configuring the Maximum Number of SIP Registrations

To configure the maximum number of SIP registrations, in global configuration mode, use the following command:

alg sip sip-register-max *number*

- *number* - Specifies the maximum number of SIP registrations. Valid values: 1 to 20000. Default value: 5000.

Configuring the Maximum Number of SIP Dialogs

To configure the maximum number of SIP dialogs, in global configuration mode, use the following command:

alg sip sip-dialog-max *number*

- *number* - Specifies the maximum number of SIP dialogs. Valid values: 1 to 20000. Default value: 5000.

For more information, refer to the **Firewall > Application Layer Identification and Control > Configuring ALG** topic in *StoneOS CLI User Guide*. FR 41027

MIB

HILLSTONE-STATISTICS-MIB

The following tables is the parsing results of HILLSTONE-STATISTICS-MIB.

Name	OID	Value
hillstoneSystemStatistics: System statistics information		
onlineUserNum	.1.3.6.1.4.1.28557.2.3.1.1	Data type: Integer Description: Number of login users via Console, Telnet and SSH
hillstoneIPSecStatistic: IPSec statistical information		
hillstoneIPSecGlobalActiveTunnels	.1.3.6.1.4.1.28557.2.3.2.1	Data type: Gauge Description: Alive tunnel number

Name	OID	Value
hillstoneIPSecGlobalActiveSas	.1.3.6.1.4.1.28557.2.3.2.2	Data type: Gauge Description: Number of alive and expired P2 SA
hillstoneIPSecStatistic: Detailed statistic information of IPSec Tunnel		
hillstoneIPsecTunnelID	.1.3.6.1.4.1.28557.2.3.2.3.1.1	Data type: Counter Description: Tunnel ID
hillstoneIPSecInOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.2	Data type: Counter64 Description: Number of received bytes
hillstoneIPSecInDecompOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.3	Data type: Counter64 Description: Number of received decompressed types
hillstoneIPSecInPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.4	Data type: Counter64 Description: Number of received packets
hillstoneIPSecInDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.5	Data type: Counter64

Name	OID	Value
		Description: Number of dropped packets during trans-mission
hillstoneIPSecInReplayDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.6	Data type: Counter32 Description: Number of dropped packets due to anti-replay
hillstoneIPSecInAuthFails	.1.3.6.1.4.1.28557.2.3.2.3.1.7	Data type: Counter32 Description: Number of dropped packets due to authen-tication failure
hillstoneIPSecInDecryptFails	.1.3.6.1.4.1.28557.2.3.2.3.1.8	Data type: Counter32 Description: Number of pack-ets that failed to decrypt
hillstoneIPSecOutOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.9	Data type: Counter64 Description: Byte count of sent packets

Name	OID	Value
hillstoneIPSecOutUncompOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.10	Data type: Counter64 Description: Byte count of sent uncompressed data
hillstoneIPSecOutPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.11	Data type: Counter64 Description: Number of sent packet
hillstoneIPSecOutDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.12	Data type: Counter64 Description: Number of dropped packets during trans-mission
hillstoneIPSecOutEncryptFails	.1.3.6.1.4.1.28557.2.3.2.3.1.13	Data type: Counter32 Description: Number of pack-ets that failed to encrypt during transmission
hillstoneIPSecNoMemoryDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.14	Data type: Counter32 Description: Number of

Name	OID	Value
		dropped packets due to insufficient memory
hillstoneIPSecNoFindSaDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.15	Data type: Counter32 Description: Number of dropped packets due to no available SA
hillstoneIPSecQueueFullDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.16	Data type: Counter32 Description: Number of dropped packets due to queuing jam
hillstoneIPSecInvalidLenDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.17	Data type: Counter32 Description: Number of dropped packets due to invalid packet length
hillstoneIPSecTooLongDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.18	Data type: Counter32 Description: Number of dropped packets due to over length

Name	OID	Value
hillstoneIPSecInvalidSaDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.19	Data type: Counter32 Description: Number of dropped packets due to invalid SA
hillstoneIpsEventStatistics: IPS statistical information by protocol type		
hillstoneIpsFlowStatistics: IPS statistical information, the same information as that of hillstoneIpsEventStatistics		
hillstoneEventHttpAtk	.1.3.6.1.4.1.28557.2.3.3.1	Data type: Counter64 Description: HTTP attack count
hillstoneEventFtpAtk	.1.3.6.1.4.1.28557.2.3.3.2	Data type: Counter64 Description: FTP attack count
hillstoneEventSmtpAtk	.1.3.6.1.4.1.28557.2.3.3.3	Data type: Counter64 Description: SMTP attack count. This value represents the cumulative statistical data within the last 24 hours and will not constantly increase.

Name	OID	Value
hillstoneEventDnsAtk	.1.3.6.1.4.1.28557.2.3.3.4	Data type: Counter64 Description: DNS attack count
hillstoneEventNetbiosAtk	.1.3.6.1.4.1.28557.2.3.3.5	Data type: Counter64 Description: NETBIOS attack count
hillstoneEventPop3Atk	.1.3.6.1.4.1.28557.2.3.3.6	Data type: Counter64 Description: POP3 attack count
hillstoneEventSipAtk	.1.3.6.1.4.1.28557.2.3.3.7	Data type: Counter64 Description: SIP attack count
hillstoneEventH323Atk	.1.3.6.1.4.1.28557.2.3.3.8	Data type: Counter64 Description: H323 attack count
hillstoneEventImapAtk	.1.3.6.1.4.1.28557.2.3.3.9	Data type: Counter64 Description: IMAP attack count
hillstoneEventP2PAtk	.1.3.6.1.4.1.28557.2.3.3.10	Data type:

Name	OID	Value
		Counter64 Description: P2P attack count
hillstoneEventImAtk	.1.3.6.1.4.1.28557.2.3.3.11	Data type: Counter64 Description: IM attack count
hillstoneEventSQLAtk	.1.3.6.1.4.1.28557.2.3.3.12	Data type: Counter64 Description: SQL injection attack count
hillstoneEventIPSOthersAtk	.1.3.6.1.4.1.28557.2.3.3.13	Data type: Counter64 Description: Othes
hillstoneAVEventStatistics: AV statistics, AV count by protocol type		
hillstoneEventAVHttpClear	.1.3.6.1.4.1.28557.2.3.7.1	Data type: Counter64 Description: HTTP virus count
hillstoneEventAVFtpClear	.1.3.6.1.4.1.28557.2.3.7.2	Data type: Counter64 Description: FTP virus count
hillstoneEventAVSmtpClear	.1.3.6.1.4.1.28557.2.3.7.3	Data type: Counter64

Name	OID	Value
		Description: SMTP virus count
hillstoneEventAVPopClear	.1.3.6.1.4.1.28557.2.3.7.4	Data type: Counter64 Description: POP virus count
hillstoneEventAVImapClear	.1.3.6.1.4.1.28557.2.3.7.5	Data type: Counter64 Description: IMAP virus count
hillstoneALGStatistics: ALG statistical information		
hillstoneALGSipDialog	.1.3.6.1.4.1.28557.2.3.8.1.0	Data type: Integer Description: Obtain the current number of SIP dialogs of the device
hillstoneALGSipRegister	.1.3.6.1.4.1.28557.2.3.8.2.0	Data type: Integer Description: Obtain the current number of SIP registrations of the device
hillstoneALGSipDialogMax	.1.3.6.1.4.1.28557.2.3.8.3.0	Data type: Integer Description: Obtain the maximum number of SIP dialogs of the device

Name	OID	Value
hillstoneALGSipRegisterMax	.1.3.6.1.4.1.28557.2.3.8.4.0	Data type: Integer Description: Obtain the maximum number of SIP registrations of the device
hillstoneAtkEventStatisticsTable: AD statistics, attacks count by zone		
hillstoneAtkFlowStatisticsTable: AD statistics, the same as that of hillstoneAtkEventStatisticsTable		
hillstoneAtkEventZoneIdx	.1.3.6.1.4.1.28557.2.3.10.1.1	Data type: Counter Description: Zone number
hillstoneAtkEventZoneName	.1.3.6.1.4.1.28557.2.3.10.1.2	Data type: Octet String Description: Zone name (maximum 255 characters)
hillstoneAtkEventIpSpoof	.1.3.6.1.4.1.28557.2.3.10.1.3	Data type: Counter64 Description: IP address spoofing count
hillstoneAtkEventLandAtk	.1.3.6.1.4.1.28557.2.3.10.1.4	Data type: Counter64 Description: Land attack count

Name	OID	Value
hillstoneAtkEventWinnuke	.1.3.6.1.4.1.28557.2.3.10.1.7	Data type: Counter64 Description: WinNuke attack count
hillstoneAtkEventSynSourceFlood	.1.3.6.1.4.1.28557.2.3.10.1.10	Data type: Counter64 Description: SYN Source Flood attack count
hillstoneAtkEventSynDestFlood	.1.3.6.1.4.1.28557.2.3.10.1.11	Data type: Counter64 Description: SYN Destination Flood attack count
hillstoneAtkEventIcmpFlood	.1.3.6.1.4.1.28557.2.3.10.1.13	Data type: Counter64 Description: ICMP Flood attack count
hillstoneAtkEventIpSweep	.1.3.6.1.4.1.28557.2.3.10.1.16	Data type: Counter64 Description: IP Sweep attack count
hillstoneAtkEventPortScan	.1.3.6.1.4.1.28557.2.3.10.1.17	Data type: Counter64 Description: Port Scan attack count

Name	OID	Value
hillstoneAtkEventIpOptAtk	.1.3.6.1.4.1.28557.2.3.10.1.18	Data type: Counter64 Description: IP Option attack count
hillstoneAtkEventPingOfDeathAtk	.1.3.6.1.4.1.28557.2.3.10.1.23	Data type: Counter64 Description: Ping of Death attack count
hillstoneAtkEventTearDropAtk	.1.3.6.1.4.1.28557.2.3.10.1.24	Data type: Counter64 Description: Tear Drop attack count
hillstoneAtkEventIpFragAtk	.1.3.6.1.4.1.28557.2.3.10.1.26	Data type: Counter64 Description: IP Fraggle attack count
hillstoneAtkEventLargeIcmpAtk	.1.3.6.1.4.1.28557.2.3.10.1.27	Data type: Counter64 Description: Large ICMP attack count
hillstoneAtkEventSynProxyAtk	.1.3.6.1.4.1.28557.2.3.10.1.31	Data type: Counter64 Description: SYN-Proxy attack count

Name	OID	Value
hillstoneAtkEventSynCookieAtk	.1.3.6.1.4.1.28557.2.3.10.1.32	Data type: Counter64 Description: SYN Cookie attack count
hillstoneAtkEventTCPAnomalyAtk	.1.3.6.1.4.1.28557.2.3.10.1.33	Data type: Counter64 Description: TCP Anomaly attack count
hillstoneAtkEventIPDirectedAtk	.1.3.6.1.4.1.28557.2.3.10.1.34	Data type: Counter64 Description: IP Directed attack count

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 41027

Supporting to Update IPS Entire Signature Database by Certain A-series Devices

WebUI

Updating Signature Database

The signature databases that can be installed include Encrypted traffic detection database,Share Access signature database,Application signature database, URL signature database, Antivirus signature database, antivirus intelligence file engine database, Sandbox Whitelist Database, IPS signature database, IP reputation database, SSL proxy domain whitelist signature database, Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and

IP geography database. Except Encrypted traffic detection database,SSL proxy domain whitelist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, you can only view other signature databases when the system is installed with the corresponding licenses. The system support the following two methods to upgrade signature databases: remote update via HTTP and HTTPS; local update via downloading update package through the default signature database update server.

The system supports to download each signature database over IPv6.

Notes:

The following devices support to antivirus intelligence file engine database.

- A-series: Except SG-6000-A200.
- K-series: SG-6000-K2680, SG-6000-K2380, SG-6000-K6280-GS, SG-6000-K6580, and SG-6000-K9180.
- X-series: SG-6000-X25803 and SG-6000-X25812.
- CloudEdge: Only CloudEdge that is deployed on X86-based server.

To update signature database, take the following steps:

1. Select **System** > **Upgrade Management** > **Signature Database Update**.
2. **In the Signature Database Update page, configure the following.**

Option	Description
Current Version	Show the current version number.
Latest Version	Show the latest version number. **Note:**The latest version of the ISP information database and IP geography database can be displayed only when the current version exists. The latest version of other signature databases can be

Option	Description
	displayed only when the corresponding signature database licenses are activated and the current version exists.
Update Entire Signature	In the IPS signature database module, you can update the current IPS signature database to the IPS entire signature database. By default, this option is disabled. Click  to update the IPS entire signature database. This operation may cause the throughput performance of the device to drop by up to 20%. It is recommended that you configure it based on the actual load of the device. Click  to cancel updating the IPS entire signature database. This operation reduces the current number of signatures in the IPS signature database and may affect the details of threat events that have been generated. **Notes:** The following devices support this option: • A-series: SG-6000-A200/A200G4B /A200W/A1000/A1100
Remote Update	Encrypted traffic detection database, Application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database. • Protocol: Select the update method of the signature data-

Option	Description
	base, including HTTP and HTTPS. Click **Restore Default** to restore the default HTTPS transmission method. • Update Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. The IPv4 and IPv6 address are supported for configuring the update server address. Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers according to your need. In **Update Server**, specify the server IP or domain name and Virtual Router. • Update Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally. In **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button of **Auto Update** and specify the auto update time. Click **Ok** to save your changes. • Update Now: Click **Ok And Online Update** to update the signature database right now.

Option	Description
Local Update	Download the update package from the default feature update server for local update. • Download the upgrade packages of the encrypted traffic detection database, application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database, SSL proxy domain whitelist signature database, , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database from https://update1.hillstonenet.com and https://update2.hillstonenet.com. • Click **Browse** and select the signature file in your local PC, and then click **Upload**. **Notes:** 1. Before StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Botnet C&C Detection Package" link of the default update server. From StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Encrypt Botnet C&C Detection Package" link of the default update server. 2. If a large number of devices (with the same version and model) need local update, contact Hillstone's support team to acquire bulk update solutions.

For more information, refer to **System Management** > **Upgrading System** in *StoneOS WebUI User Guide*. FR 39117, FR 37659

CLI

Updating IPS Entire Signature Database

Due to differences in memory sizes among devices, some devices load an incomplete number of signatures in the IPS signature database by default. To meet your security protection needs, you can manually update the current IPS signature database to an entire IPS signature database, enhancing the security protection capability of the system.

Supported devices:

- A-series: SG-6000-A200/A200G4B/A200W/A1000/A1100

Before you start:

- Install the IPS license. For more information, see **System Management** > **License Management**.

Precautions:

- By default, the Update IPS Entire Signature Database function is not enabled.
- The operation of updating the IPS entire signature database may cause the throughput performance of the device to drop by up to 20%. It is recommended that you configure it based on the actual load of the device.
- After you update to the IPS entire signature database, if you disable this function, this operation reduces the current number of signatures in the IPS signature database and may affect the details of threat events that have been generated.

Procedure:

To update to the IPS entire signature database, in global configuration mode, use the following command:

ips signature update entire

To cancel updating to the IPS entire signature database, in global configuration mode, use the following command:

no ips signature update entire

For more information, refer to **Threat Prevention** > **Updating Signature Database** in *StoneOS CLI User Guide*. FR 39117, FR 37659

Querying Traffic and Session Information of Top 32 Users/Top 32 Applications/Address Books by Using SNMP

MIB

HILLSTONE-STATISTICS-MIB

The following tables is the parsing results of HILLSTONE-STATISTICS-MIB.

Name	OID	Value
hillstoneSystemStatistics: System statistics information		
onlineUserNum	.1.3.6.1.4.1.28557.2.3.1.1	Data type: Integer Description: Number of login users via Console, Telnet and SSH
hillstoneIPSecStatistic: IPSec statistical information		
hillstoneIPSecGlobalActiveTunnels	.1.3.6.1.4.1.28557.2.3.2.1	Data type: Gauge Description:

Name	OID	Value
		Alive tunnel number
hillstoneIPSecGlobalActiveSas	.1.3.6.1.4.1.28557.2.3.2.2	Data type: Gauge Description: Number of alive and expired P2 SA
hillstoneIPSecStatisticTable: Detailed statistic information of IPSec Tunnel		
hillstoneIPsecTunnelID	.1.3.6.1.4.1.28557.2.3.2.3.1.1	Data type: Counter Description: Tunnel ID
hillstoneIPSecInOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.2	Data type: Counter64 Description: Number of received bytes
hillstoneIPSecInDecompOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.3	Data type: Counter64 Description: Number of received decompressed types
hillstoneIPSecInPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.4	Data type: Counter64 Description:

Name	OID	Value
		Number of received packets
hillstoneIPSecInDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.5	Data type: Counter64 Description: Number of dropped packets during transmission
hillstoneIPSecInReplayDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.6	Data type: Counter32 Description: Number of dropped packets due to anti-replay
hillstoneIPSecInAuthFails	.1.3.6.1.4.1.28557.2.3.2.3.1.7	Data type: Counter32 Description: Number of dropped packets due to authentication failure
hillstoneIPSecInDecryptFails	.1.3.6.1.4.1.28557.2.3.2.3.1.8	Data type: Counter32 Description: Number of packets that

Name	OID	Value
		failed to decrypt
hillstoneIPSecOutOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.9	Data type: Counter64 Description: Byte count of sent packets
hillstoneIPSecOutUncompOctets	.1.3.6.1.4.1.28557.2.3.2.3.1.10	Data type: Counter64 Description: Byte count of sent uncompressed data
hillstoneIPSecOutPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.11	Data type: Counter64 Description: Number of sent packet
hillstoneIPSecOutDrops	.1.3.6.1.4.1.28557.2.3.2.3.1.12	Data type: Counter64 Description: Number of dropped packets during transmission
hillstoneIPSecOutEncryptFails	.1.3.6.1.4.1.28557.2.3.2.3.1.13	Data type: Counter32 Description: Number of

Name	OID	Value
		packets that failed to encrypt during transmission
hillstoneIPSecNoMemoryDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.14	Data type: Counter32 Description: Number of dropped packets due to insufficient memory
hillstoneIPSecNoFindSaDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.15	Data type: Counter32 Description: Number of dropped packets due to no available SA
hillstoneIPSecQueueFullDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.16	Data type: Counter32 Description: Number of dropped packets due to queuing jam
hillstoneIPSecInvalidLenDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.17	Data type: Counter32 Description: Number of

Name	OID	Value
		dropped packets due to invalid packet length
hillstoneIPSecTooLongDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.18	Data type: Counter32 Description: Number of dropped packets due to over length
hillstoneIPSecInvalidSaDropPkts	.1.3.6.1.4.1.28557.2.3.2.3.1.19	Data type: Counter32 Description: Number of dropped packets due to invalid SA
hillstoneIpsEventStatistics: IPS statistical information by protocol type		
hillstoneIpsFlowStatistics: IPS statistical information, the same information as that of hillstoneIpsEventStatistics		
hillstoneEventHttpAtk	.1.3.6.1.4.1.28557.2.3.3.1	Data type: Counter64 Description: HTTP attack count
hillstoneEventFtpAtk	.1.3.6.1.4.1.28557.2.3.3.2	Data type: Counter64

Name	OID	Value
		Description: FTP attack count
hillstoneEventSmtpAtk	.1.3.6.1.4.1.28557.2.3.3.3	Data type: Counter64 Description: SMTP attack count. This value represents the cumulative statistical data within the last 24 hours and will not constantly increase.
hillstoneEventDnsAtk	.1.3.6.1.4.1.28557.2.3.3.4	Data type: Counter64 Description: DNS attack count
hillstoneEventNetbiosAtk	.1.3.6.1.4.1.28557.2.3.3.5	Data type: Counter64 Description: NETBIOS attack count
hillstoneEventPop3Atk	.1.3.6.1.4.1.28557.2.3.3.6	Data type: Counter64 Description:

Name	OID	Value
		POP3 attack count
hillstoneEventSipAtk	.1.3.6.1.4.1.28557.2.3.3.7	Data type: Counter64 Description: SIP attack count
hillstoneEventH323Atk	.1.3.6.1.4.1.28557.2.3.3.8	Data type: Counter64 Description: H323 attack count
hillstoneEventImapAtk	.1.3.6.1.4.1.28557.2.3.3.9	Data type: Counter64 Description: IMAP attack count
hillstoneEventP2PAtk	.1.3.6.1.4.1.28557.2.3.3.10	Data type: Counter64 Description: P2P attack count
hillstoneEventImAtk	.1.3.6.1.4.1.28557.2.3.3.11	Data type: Counter64 Description: IM attack count
hillstoneEventSQLAtk	.1.3.6.1.4.1.28557.2.3.3.12	Data type: Counter64

Name	OID	Value
		Description: SQL injection attack count
hillstoneEventIPSOthersAtk	.1.3.6.1.4.1.28557.2.3.3.13	Data type: Counter64 Description: Othes
hillstoneAVEventStatistics: AV statistics, AV count by protocol type		
hillstoneEventAVHttpClear	.1.3.6.1.4.1.28557.2.3.7.1	Data type: Counter64 Description: HTTP virus count
hillstoneEventAVFtpClear	.1.3.6.1.4.1.28557.2.3.7.2	Data type: Counter64 Description: FTP virus count
hillstoneEventAVSmtpClear	.1.3.6.1.4.1.28557.2.3.7.3	Data type: Counter64 Description: SMTP virus count
hillstoneEventAVPopClear	.1.3.6.1.4.1.28557.2.3.7.4	Data type: Counter64 Description: POP virus count
hillstoneEventAVImapClear	.1.3.6.1.4.1.28557.2.3.7.5	Data type:

Name	OID	Value
		Counter64 Description: IMAP virus count
hillstoneAtkEventStatisticsTable: AD statistics, attacks count by zone		
hillstoneAtkFlowStatisticsTable: AD statistics, the same as that of hillstoneAtkEventStatisticsTable		
hillstoneAtkEventZoneIdx	.1.3.6.1.4.1.28557.2.3.10.1.1	Data type: Counter Description: Zone number
hillstoneAtkEventZoneName	.1.3.6.1.4.1.28557.2.3.10.1.2	Data type: Octet String Description: Zone name (maximum 255 characters)
hillstoneAtkEventIpSpoof	.1.3.6.1.4.1.28557.2.3.10.1.3	Data type: Counter64 Description: IP address spoofing count
hillstoneAtkEventLandAtk	.1.3.6.1.4.1.28557.2.3.10.1.4	Data type: Counter64 Description: Land attack

Name	OID	Value
		count
hillstoneAtkEventSmurfAtk	.1.3.6.1.4.1.28557.2.3.10.1.5	Data type: Counter64 Description: Smurf attack count
hillstoneAtkEventFraggleAtk	.1.3.6.1.4.1.28557.2.3.10.1.6	Data type: Counter64 Description: Fraggle attack count
hillstoneAtkEventWinnuke	.1.3.6.1.4.1.28557.2.3.10.1.7	Data type: Counter64 Description: WinNuke attack count
hillstoneAtkEventDnsFlood	.1.3.6.1.4.1.28557.2.3.10.1.8	Data type: Counter64 Description: DNS Query Flood attack count
hillstoneAtkEventTcpFlood	.1.3.6.1.4.1.28557.2.3.10.1.9	Data type: Counter64 Description: TCP Flood attack count
hillstoneAtkEventSynSourceFlood	.1.3.6.1.4.1.28557.2.3.10.1.10	Data type: Counter64

Name	OID	Value
		Description: SYN Source Flood attack count
hillstoneAtkEventSynDestFlood	.1.3.6.1.4.1.28557.2.3.10.1.11	Data type: Counter64 Description: SYN Destination Flood attack count
hillstoneAtkEventUdpFlood	.1.3.6.1.4.1.28557.2.3.10.1.12	Data type: Counter64 Description: UDP Flood attack count
hillstoneAtkEventIcmpFlood	.1.3.6.1.4.1.28557.2.3.10.1.13	Data type: Counter64 Description: ICMP Flood attack count
hillstoneAtkEventRedirect	.1.3.6.1.4.1.28557.2.3.10.1.14	Data type: Counter64 Description: ICMP Redirect attack count
hillstoneAtkEventUnreacheableAtk	.1.3.6.1.4.1.28557.2.3.10.1.15	Data type: Counter64 Description:

Name	OID	Value
		Unreachable attack count
hillstoneAtkEventIpSweep	.1.3.6.1.4.1.28557.2.3.10.1.16	Data type: Counter64 Description: IP Sweep attack count
hillstoneAtkEventPortScan	.1.3.6.1.4.1.28557.2.3.10.1.17	Data type: Counter64 Description: Port Scan attack count
hillstoneAtkEventIpOptAtk	.1.3.6.1.4.1.28557.2.3.10.1.18	Data type: Counter64 Description: IP Option attack count
hillstoneAtkEventIpOptSrcRoutAtk	.1.3.6.1.4.1.28557.2.3.10.1.19	Data type: Counter64 Description: IP Option Strict Source Route attack count
hillstoneAtkEventIpOptRoutRecord	.1.3.6.1.4.1.28557.2.3.10.1.20	Data type: Counter64 Description: IP Option Route attack

Name	OID	Value
		count
hillstoneAtkEventTraceRoutAtk	.1.3.6.1.4.1.28557.2.3.10.1.21	Data type: Counter64 Description: Trace Route attack count
hillstoneAtkEventTimeStampAtk	.1.3.6.1.4.1.28557.2.3.10.1.22	Data type: Counter64 Description: Time Stamp attack count
hillstoneAtkEventPingOfDeathAtk	.1.3.6.1.4.1.28557.2.3.10.1.23	Data type: Counter64 Description: Ping of Death attack count
hillstoneAtkEventTearDropAtk	.1.3.6.1.4.1.28557.2.3.10.1.24	Data type: Counter64 Description: Tear Drop attack count
hillstoneAtkEventTcpFlagAtk	.1.3.6.1.4.1.28557.2.3.10.1.25	Data type: Counter64 Description: TCP Flag attack count
hillstoneAtkEventIpFragAtk	.1.3.6.1.4.1.28557.2.3.10.1.26	Data type: Counter64

Name	OID	Value
		Description: IP Fraggle attack count
hillstoneAtkEventLargeIcmpAtk	.1.3.6.1.4.1.28557.2.3.10.1.27	Data type: Counter64 Description: Large ICMP attack count
hillstoneAtkEventSweepAndScanAtk	.1.3.6.1.4.1.28557.2.3.10.1.28	Data type: Counter64 Description: Sweep and Scan attack count
hillstoneAtkEventHalfConnAtk	.1.3.6.1.4.1.28557.2.3.10.1.29	Data type: Counter64 Description: Half Con-nection attack count
hillstoneAtkEventFtpBounceAtk	.1.3.6.1.4.1.28557.2.3.10.1.30	Data type: Counter64 Description: FTP Bounce attack count
hillstoneAtkEventSynProxyAtk	.1.3.6.1.4.1.28557.2.3.10.1.31	Data type: Counter64 Description: SYN-Proxy

Name	OID	Value
		attack count
hillstoneAtkEventSynCookieAtk	.1.3.6.1.4.1.28557.2.3.10.1.32	Data type: Counter64 Description: SYN Cookie attack count
hillstoneAtkEventTCPAnomalyAtk	.1.3.6.1.4.1.28557.2.3.10.1.33	Data type: Counter64 Description: TCP Anomaly attack count
hillstoneAtkEventIPDirectedAtk	.1.3.6.1.4.1.28557.2.3.10.1.34	Data type: Counter64 Description: IP Directed attack count
hillstoneAtkEventAtkOthersAtk	.1.3.6.1.4.1.28557.2.3.10.1.35	Data type: Counter64 Description: Others
hillstoneSSetAddressBooksMonitorTable: Traffic and session information of address book		
hillstoneSSetAddressBookIdx	.1.3.6.1.4.1.28557.2.3.12.1.1	Data type: Counter Description: Address book index

Name	OID	Value
hillstoneSSetAddressBookName	.1.3.6.1.4.1.28557.2.3.12.1.2	Data type: Octet String Description: Address book name
hillstoneSSetAddressBookCurrentUpstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.3	Data type: Counter64 Description: Real-time upstream traffic of address book. Unit: bps
hillstoneSSetAddressBookCurrentDownstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.4	Data type: Counter64 Description: Real-time down-stream traffic of address book. Unit: bps
hillstoneSSetAddressBookCurrentSessionCount	.1.3.6.1.4.1.28557.2.3.12.1.5	Data type: Gauge32 Description: Real-time num-ber of sessions of address book
hillstoneSSetAddressBookLastHour	.1.3.6.1.4.1.28557.2.3.12.1.6	Data type:

Name	OID	Value
UpstreamTraffic		Counter64 Description: Upstream traffic of address book within the last 60 minutes. Unit: bytes
hillstoneSSetAddressBookLastHour DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.7	Data type: Counter64 Description: Downstream traffic of address book within the last 60 minutes. Unit: bytes
hillstoneSSetAddressBookLastDay UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.8	Data type: Counter64 Description: Upstream traffic of address book within the last 24 hours. Unit: bytes
hillstoneSSetAddressBookLastDay DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.9	Data type: Counter64

Name	OID	Value
		Description: Downstream traffic of address book within the last 24 hours. Unit: bytes
hillstoneSSetAddressBookLastMonth UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.10	Data type: Counter64 Description: Upstream traffic of address book within the last 30 days. Unit: bytes
hillstoneSSetAddressBookLastMonth DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.12.1.11	Data type: Counter64 Description: Downstream traffic of address book within the last 30 days. Unit: bytes
hillstoneUserRealTimeRank: Real-time traffic and session information of top 32 users		
hillstoneUserRealTimeRankEntryIdx	.1.3.6.1.4.1.28557.2.3.13.1.1	Data type: Counter Description: User ranking

Name	OID	Value
hillstoneUserRealTimeRankEntryName	.1.3.6.1.4.1.28557.2.3.13.1.2	Data type: Octet String Description: Username
hillstoneUserRealTimeRankEntry UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.13.1.3	Data type: Counter64 Description: Real-time upstream traffic of user. Unit: bps
hillstoneUserRealTimeRankEntry DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.13.1.4	Data type: Counter64 Description: Real-time down-stream traffic of user. Unit: bps
hillstoneUserRealTimeRankEntry AllTraffic	.1.3.6.1.4.1.28557.2.3.13.1.5	Data type: Counter64 Description: Real-time total traffic of user. Unit: bps
hillstoneUserRealTimeRankEntry RealTimeSessionCount	.1.3.6.1.4.1.28557.2.3.13.1.6	Data type: Gauge32 Description:

Name	OID	Value
		Real-time number of sessions of user
hillstoneUserRealTimeRankEntry RealTimeSessionCountPercentage	.1.3.6.1.4.1.28557.2.3.13.1.7	Data type: Octet String Description: The percentage of real-time number of sessions of user to that of all users
hillstoneUserRealTimeRankEntry AllTrafficPercentage	.1.3.6.1.4.1.28557.2.3.13.1.8	Data type: Octet String Description: The percentage of real-time total traffic of user to that of all users
hillstoneUserRealTimeRankEntry UpstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.13.1.9	Data type: Octet String Description: The percentage of real-time upstream traffic of user to that of all users

Name	OID	Value
hillstoneUserRealTimeRankEntry DownstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.13.1.10	Data type: Octet String Description: The percentage of real-time down-stream traffic of user to that of all users
hillstoneUserLastHourRank: Traffic and session information of the top 32 users within the last 60 minutes		
hillstoneUserLastHourRankEntryIdx	.1.3.6.1.4.1.28557.2.3.14.1.1	Data type: Counter Description: User ranking
hillstoneUserLastHourRankEntryName	.1.3.6.1.4.1.28557.2.3.14.1.2	Data type: Octet String Description: Username
hillstoneUserLastHourRankEntry UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.14.1.3	Data type: Counter64 Description: Upstream traffic of user within the last 60 minutes. Unit:

Name	OID	Value
		bytes
hillstoneUserLastHourRankEntry DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.14.1.4	Data type: Counter64 Description: Downstream traffic of user within the last 60 minutes. Unit: bytes
hillstoneUserLastHourRankEntry AllTraffic	.1.3.6.1.4.1.28557.2.3.14.1.5	Data type: Counter64 Description: Total traffic of user within the last 60 minutes. Unit: bytes
hillstoneUserLastHourRankEntry RealTimeSessionCount	.1.3.6.1.4.1.28557.2.3.14.1.6	Data type: Gauge32 Description: Real-time number of sessions of user
hillstoneUserLastHourRankEntry RealTimeSessionCountPercentage	.1.3.6.1.4.1.28557.2.3.14.1.7	Data type: Octet String Description: The percentage of

Name	OID	Value
		number of sessions of user within the last 60 minutes to that of all users
hillstoneUserLastHourRankEntry AllTrafficPercentage	.1.3.6.1.4.1.28557.2.3.14.1.8	Data type: Octet String Description: The percentage of total traffic of user within the last 60 minutes to that of all users
hillstoneUserLastHourRankEntry UpstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.14.1.9	Data type: Octet String Description: The percentage of upstream traffic of user within the last 60 minutes to that of all users
hillstoneUserLastHourRankEntry DownstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.14.1.10	Data type: Octet String

Name	OID	Value
		Description: The percentage of downstream traffic of user within the last 60 minutes to that of all users
hillstoneUserLastDayRank: Traffic and session information of the top 32 users within the last 24 hours		
hillstoneUserLastDayRankEntryIdx	.1.3.6.1.4.1.28557.2.3.15.1.1	Data type: Counter Description: User ranking
hillstoneUserLastDayRankEntryName	.1.3.6.1.4.1.28557.2.3.15.1.2	Data type: Octet String Description: Username
hillstoneUserLastDayRankEntry UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.15.1.3	Data type: Counter64 Description: Upstream traffic of user within the last 24 hours. Unit: bytes
hillstoneUserLastDayRankEntry DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.15.1.4	Data type:

Name	OID	Value
		Counter64 Description: Downstream traffic of user within the last 24 hours. Unit: bytes
hillstoneUserLastDayRankEntry AllTraffic	.1.3.6.1.4.1.28557.2.3.15.1.5	Data type: Counter64 Description: Total traffic of user within the last 24 hours. Unit: bytes
hillstoneUserLastDayRankEntry RealTimeSessionCount	.1.3.6.1.4.1.28557.2.3.15.1.6	Data type: Gauge32 Description: Real-time number of sessions of user
hillstoneUserLastDayRankEntry RealTimeSessionCountPercentage	.1.3.6.1.4.1.28557.2.3.15.1.7	Data type: Octet String Description: The percentage of number of sessions of user

Name	OID	Value
		within the last 24 hours to that of all users
hillstoneUserLastDayRankEntry AllTrafficPercentage	.1.3.6.1.4.1.28557.2.3.15.1.8	Data type: Octet String Description: The percentage of total traffic of user within the last 24 hours to that of all users
hillstoneUserLastDayRankEntry UpstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.15.1.9	Data type: Octet String Description: The percentage of upstream traffic of user within the last 24 hours to that of all users
hillstoneUserLastDayRankEntry DownstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.15.1.10	Data type: Octet String Description: The percentage of downstream traffic of user

Name	OID	Value
		within the last 24 hours to that of all users
hillstoneUserLastMonthRank: Traffic and session information of the top 32 users within the last 30 days		
hillstoneUserLastMonthRankEntryIdx	.1.3.6.1.4.1.28557.2.3.16.1.1	Data type: Counter Description: User ranking
hillstoneUserLastMonthRankEntryName	.1.3.6.1.4.1.28557.2.3.16.1.2	Data type: Octet String Description: Username
hillstoneUserLastMonthRankEntry UpstreamTraffic	.1.3.6.1.4.1.28557.2.3.16.1.3	Data type: Counter64 Description: Upstream traffic of user within the last 30 days. Unit: bytes
hillstoneUserLastMonthRankEntry DownstreamTraffic	.1.3.6.1.4.1.28557.2.3.16.1.4	Data type: Counter64 Description: Downstream traffic of user

Name	OID	Value
		within the last 30 days. Unit: bytes
hillstoneUserLastMonthRankEntry AllTraffic	.1.3.6.1.4.1.28557.2.3.16.1.5	Data type: Counter64 Description: Total traffic of user within the last 30 days. Unit: bytes
hillstoneUserLastMonthRankEntry RealTimeSessionCount	.1.3.6.1.4.1.28557.2.3.16.1.6	Data type: Gauge32 Description: Real-time number of sessions of user
hillstoneUserLastMonthRankEntry RealTimeSessionCountPercentage	.1.3.6.1.4.1.28557.2.3.16.1.7	Data type: Octet String Description: The percentage of number of sessions of user within the last 30 days to that of all users
hillstoneUserLastMonthRankEntry AllTrafficPercentage	.1.3.6.1.4.1.28557.2.3.16.1.8	Data type: Octet String

Name	OID	Value
		Description: The percentage of total traffic of user within the last 30 days to that of all users
hillstoneUserLastMonthRankEntry UpstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.16.1.9	Data type: Octet String Description: The percentage of upstream traffic of user within the last 30 days to that of all users
hillstoneUserLastMonthRankEntry DownstreamTrafficPercentage	.1.3.6.1.4.1.28557.2.3.16.1.10	Data type: Octet String Description: The percentage of downstream traffic of user within the last 30 days to that of all users
hillstoneAppRealTimeRank: Real-time traffic and session information of top 32 applications		

Name	OID	Value
hillstoneAppRealTimeRankEntryIdx	.1.3.6.1.4.1.28557.2.3.17.1.1	Data type: Counter Description: Application ranking
hillstoneAppRealTimeRankEntryName	.1.3.6.1.4.1.28557.2.3.17.1.2	Data type: Octet String Description: Application name
hillstoneAppRealTimeRankEntry AppCategory	.1.3.6.1.4.1.28557.2.3.17.1.3	Data type: Octet String Description: Application category
hillstoneAppRealTimeRankEntry AppSubCategory	.1.3.6.1.4.1.28557.2.3.17.1.4	Data type: Octet String Description: Application subcategory
hillstoneAppRealTimeRankEntryTraffic	.1.3.6.1.4.1.28557.2.3.17.1.5	Data type: Counter64 Description: Real-time total traffic of application. Unit: bps

Name	OID	Value
hillstoneAppRealTimeRankEntry TrafficPercentage	.1.3.6.1.4.1.28557.2.3.17.1.6	Data type: Octet String Description: The percentage of real-time total traffic of application to that of all applications
hillstoneAppRealTimeRankEntry SessionCount	.1.3.6.1.4.1.28557.2.3.17.1.7	Data type: Gauge32 Description: Real-time number of sessions of application
hillstoneAppRealTimeRankEntry SessionCountPercentage	.1.3.6.1.4.1.28557.2.3.17.1.8	Data type: Octet String Description: The percentage of real-time number of sessions of application to that of all applications
hillstoneAppLastHourRank: Traffic and session information of top 32 applications within the last 60 minutes		

Name	OID	Value
hillstoneAppLastHourRankEntryIdx	.1.3.6.1.4.1.28557.2.3.18.1.1	Data type: Counter Description: Application ranking
hillstoneAppLastHourRankEntryName	.1.3.6.1.4.1.28557.2.3.18.1.2	Data type: Octet String Description: Application name
hillstoneAppLastHourRankEntry AppCategory	.1.3.6.1.4.1.28557.2.3.18.1.3	Data type: Octet String Description: Application category
hillstoneAppLastHourRankEntry AppSubCategory	.1.3.6.1.4.1.28557.2.3.18.1.4	Data type: Octet String Description: Application subcategory
hillstoneAppLastHourRankEntryTraffic	.1.3.6.1.4.1.28557.2.3.18.1.5	Data type: Counter64 Description: Total traffic of application within the last 60

Name	OID	Value
		minutes. Unit: bytes
hillstoneAppLastHourRankEntry TrafficPercentage	.1.3.6.1.4.1.28557.2.3.18.1.6	Data type: Octet String Description: The percentage of total traffic of application within the last 60 minutes to that of all applications
hillstoneAppLastHourRankEntry SessionCount	.1.3.6.1.4.1.28557.2.3.18.1.7	Data type: Gauge32 Description: Real-time number of sessions of application
hillstoneAppLastHourRankEntry SessionCountPercentage	.1.3.6.1.4.1.28557.2.3.18.1.8	Data type: Octet String Description: The percentage of number of sessions of application within the last 60 minutes to that of all

Name	OID	Value
		applications
hillstoneAppLastDayRank: Traffic and session information of top 32 applications within the last 24 hours		
hillstoneAppLastDayRankEntryIdx	.1.3.6.1.4.1.28557.2.3.19.1.1	Data type: Counter Description: Application ranking
hillstoneAppLastDayRankEntryName	.1.3.6.1.4.1.28557.2.3.19.1.2	Data type: Octet String Description: Application name
hillstoneAppLastDayRankEntry AppCategory	.1.3.6.1.4.1.28557.2.3.19.1.3	Data type: Octet String Description: Application category
hillstoneAppLastDayRankEntry AppSubCategory	.1.3.6.1.4.1.28557.2.3.19.1.4	Data type: Octet String Description: Application subcategory
hillstoneAppLastDayRankEntryTraffic	.1.3.6.1.4.1.28557.2.3.19.1.5	Data type: Counter64

Name	OID	Value
		Description: Total traffic of application within the last 24 hours. Unit: bytes
hillstoneAppLastDayRankEntry TrafficPercentage	.1.3.6.1.4.1.28557.2.3.19.1.6	Data type: Octet String Description: The percentage of total traffic of application within the last 24 hours to that of all applications
hillstoneAppLastDayRankEntry SessionCount	.1.3.6.1.4.1.28557.2.3.19.1.7	Data type: Gauge32 Description: Real-time num-ber of sessions of application
hillstoneAppLastDayRankEntry SessionCountPercentage	.1.3.6.1.4.1.28557.2.3.19.1.8	Data type: Octet String Description: The percentage of

Name	OID	Value
		number of sessions of application within the last 24 hours to that of all applications
hillstoneAppLastMonthRank: Traffic and session information of top 32 applications within the last 30 days		
hillstoneAppLastMonthRankEntryIdx	.1.3.6.1.4.1.28557.2.3.20.1.1	Data type: Counter Description: Application ranking
hillstoneAppLastMonthRankEntryName	.1.3.6.1.4.1.28557.2.3.20.1.2	Data type: Octet String Description: Application name
hillstoneAppLastMonthRankEntry AppCategory	.1.3.6.1.4.1.28557.2.3.20.1.3	Data type: Octet String Description: Application category
hillstoneAppLastMonthRankEntry AppSubCategory	.1.3.6.1.4.1.28557.2.3.20.1.4	Data type: Octet String Description:

Name	OID	Value
		Application sub-category
hill-stoneAppLastMonthRankEntryTraffic	.1.3.6.1.4.1.28557.2.3.20.1.5	Data type: Counter64 Description: Total traffic of application within the last 30 days. Unit: bytes
hillstoneAppLastMonthRankEntry TrafficPercentage	.1.3.6.1.4.1.28557.2.3.20.1.6	Data type: Octet String Description: The percentage of total traffic of application within the last 30 days to that of all applications
hillstoneAppLastMonthRankEntry SessionCount	.1.3.6.1.4.1.28557.2.3.20.1.7	Data type: Gauge32 Description: Real-time num-ber of sessions of application
hillstoneAppLastMonthRankEntry	.1.3.6.1.4.1.28557.2.3.20.1.8	Data type: Octet

Name	OID	Value
SessionCountPercentage		String Description: The percentage of number of sessions of application within the last 30 days to that of all applications

For more information, refer to *StoneOS SNMP Private MIB Reference Guide*. FR 41425, FR 41447

Adding Trap Information to Indicate Status Changes of User Interface

Trap Information

Trap Information Description

Supported private traps for single-device deployment, master device in HA A/P mode, the device on which the interfaces in group0 are in active status in HA A/A mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates that the CPU utilization reaches its threshold (configured in the system mon-	Excessive CPU utilization may cause problems such as packet loss and net-

OID	Severity	Description	Solution
		itor).	work latency. Therefore, troubleshoot the problem in time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as required.
hillstoneFANStatus			
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.

OID	Severity	Description	Solution
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates that the memory utilization exceeds the configured (through the monitor alarm function) threshold.	Necessary clearance of the memory is needed if the memory utilization is too high.
hillstoneMemoryStatusAlertClear			
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high memory utilization as required.
hillstoneHAStatus			
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device failure. Therefore, troubleshoot the problem in time.

OID	Severity	Description	Solution
hillstoneADType			
1.3.6.1.4.1.28557.3.6	Critical	This notification indicates that the Attack Defend(AD) function is enabled in the Security Zone and the device detects the corresponding attack.	Figure out whether the attack exists in the environment. If yes, take further measures, such as using policy rules or blacklist, to block the attacking traffic.
hillstoneVPNDown			
1.3.6.1.4.1.28557.3.7	Warning	This notification indicates that the IPSec VPN tunnel is disconnected.	1. Check the quality of the physical links. 2. Confirm the status of the tunnel peer.
hillstoneVPNUp			
1.3.6.1.4.1.28557.3.8	Warning	This notification indicates that the IPSec VPN tunnel is connected.	Troubleshoot the previous disconnection of the tunnel.

OID	Severity	Description	Solution
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address changes.	Check whether the interface is disconnected physically. For example, whether the interface cable is loose.
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of notification alarm. You can ignore or troubleshoot it according to your conditions.
hillstoneIPSStatus			
1.3.6.1.4.1.28557.3.11	Critical	This notification indicates that IPS is enabled or disabled.	Confirm whether the IPS status is the same as what you have configured.
hillstoneAVStatus			
1.3.6.1.4.1.28557.3.12	Critical	This notification indicates that AV is enabled or disabled.	Confirm whether the AV status is the same as what you have configured.
hillstoneSystemReboot			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.
HillstoneDiskSpaceStatus			
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.
hillstoneSessionOverThreshold			
1.3.6.1.4.1.28557.3.15	Warning	This notification indicates that the Session ratio exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarming Session ratio is normal.

OID	Severity	Description	Solution
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates that the using ratio of the Log Buffer exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log Buffer is normal.
hillstoneIfBandwidthOverThreshold			
1.3.6.1.4.1.28557.3.17	Critical	This notification indicates that the percentage of the interface bandwidth exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarming percentage of the interface bandwidth is normal.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as required.
hillstonePolicyCountOverThreshold			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.18	Critical	This notification indicates that the number of the configured policies exceeds the threshold.	You can clean up policies or control the number of subsequent new policies.
hillstoneConfigurationChange			
1.3.6.1.4.1.28557.3.19	Critical	This notification indicates that the configuration changes.	Confirm whether the changed configuration is the same as what you have configured.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates that the slot is offline.	Confirm whether the slot is offline or it is a false alarm.
hillstoneSNATResourceOverThreshold			
1.3.6.1.4.1.28557.3.22	Critical	This notification indicates that the using ratio of the SNAT resources reaches the configured (through the monitor alarm function) threshold.	Once SNAT resources are used up, the network connection will fail because sub-

OID	Severity	Description	Solution
			sequent traffic cannot be translated. Therefore troubleshoot this problem in time.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstoneBypassInline			
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates	Malfunction of the

OID	Severity	Description	Solution
		that the status of the power module is abnormal.	power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warning, or fail.	Troubleshoot the malfunction of the fans.
hillstoneFANStopClear			
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan status as required.
hillstoneHardDiskSpaceStatus			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	The Trap host can delete previous alarms of high disk utilization as required.
hillstoneUserLogoutAlarm			
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneIFPhysicalUp			
1.3.6.1.4.1.28557.3.66	Warning	The notification indicates that	It is a type of noti-

OID	Severity	Description	Solution
		the physical status of the interface changes to UP (available).	fication alarm. You can address it according to your conditions.
hillstoneIFPhysicalDown			
1.3.6.1.4.1.28557.3.67	Warning	The notification indicates that the physical status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFAdminUp			
1.3.6.1.4.1.28557.3.68	Warning	The notification indicates that the admin status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFAdminDown			
1.3.6.1.4.1.28557.3.69	Warning	The notification indicates that the admin status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFLinkUp			
1.3.6.1.4.1.28557.3.70	Warning	The notification indicates that the link status of the interface	It is a type of notification alarm. You

OID	Severity	Description	Solution
		changes to UP (available).	can address it according to your conditions.
hillstoneIFLinkDown			
1.3.6.1.4.1.28557.3.71	Warning	The notification indicates that the link status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocolUp			
1.3.6.1.4.1.28557.3.72	Warning	The notification indicates that the IPv4 protocol status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocolDown			
1.3.6.1.4.1.28557.3.73	Warning	The notification indicates that the IPv4 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocol6Up			
1.3.6.1.4.1.28557.3.74	Warning	The notification indicates that the IPv6 protocol status of the interface changes to UP	It is a type of notification alarm. You can address it

OID	Severity	Description	Solution
		(available).	according to your conditions.
hillstoneIFProtocol6Down			
1.3.6.1.4.1.28557.3.75	Warning	The notification indicates that the IPv6 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.

Supported private traps for the backup device in HA A/P mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates that the CPU utilization reaches its threshold (configured in the system monitor).	Excessive CPU utilization may cause problems such as packet loss and network latency. Therefore, troubleshoot the problem in time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as

OID	Severity	Description	Solution
			required.
hillstoneFANStatus			
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates that the memory utilization	Necessary clearance of the

OID	Severity	Description	Solution
		exceeds the configured (through the monitor alarm function) threshold.	memory is needed if the memory utilization is too high.
hillstoneMemoryStatusAlertClear			
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high memory utilization as required.
hillstoneHAStatus			
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device failure. Therefore, troubleshoot the problem in time.
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address changes.	Check whether the interface is disconnected physically. For example, whether the interface cable is loose.

OID	Severity	Description	Solution
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of notification alarm. You can ignore or troubleshoot it according to your conditions.
hillstoneSystemReboot			
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.
HillstoneDiskSpaceStatus			
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.

OID	Severity	Description	Solution
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates that the using ratio of the Log Buffer exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log Buffer is normal.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates that the slot is offline.	Confirm whether the slot is offline or it is a false alarm.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstoneBypassInline			
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates that the status of the power module is abnormal.	Malfunction of the power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.

OID	Severity	Description	Solution
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warning, or fail.	Troubleshoot the malfunction of the fans.
hillstoneFANStopClear			
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan status as required.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as required.
hillstoneHardDiskSpaceStatus			
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.

OID	Severity	Description	Solution
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	The Trap host can delete previous alarms of high disk utilization as required.
hillstoneUserLogoutAlarm			
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneIFPhysicalUp			
1.3.6.1.4.1.28557.3.66	Warning	The notification indicates that the physical status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.

OID	Severity	Description	Solution
hillstoneIFPhysicalDown			
1.3.6.1.4.1.28557.3.67	Warning	The notification indicates that the physical status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFAdminUp			
1.3.6.1.4.1.28557.3.68	Warning	The notification indicates that the admin status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFAdminDown			
1.3.6.1.4.1.28557.3.69	Warning	The notification indicates that the admin status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFLinkUp			
1.3.6.1.4.1.28557.3.70	Warning	The notification indicates that the link status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.

OID	Severity	Description	Solution
hillstoneIFLinkDown			
1.3.6.1.4.1.28557.3.71	Warning	The notification indicates that the link status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocolUp			
1.3.6.1.4.1.28557.3.72	Warning	The notification indicates that the IPv4 protocol status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocolDown			
1.3.6.1.4.1.28557.3.73	Warning	The notification indicates that the IPv4 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocol6Up			
1.3.6.1.4.1.28557.3.74	Warning	The notification indicates that the IPv6 protocol status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocol6Down			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.75	Warning	The notification indicates that the IPv6 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.

Supported private traps for the device on which the interfaces in group1 are in active status in HA A/A Peer mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates that the CPU utilization reaches its threshold (configured in the system monitor).	Excessive CPU utilization may cause problems such as packet loss and network latency. Therefore, troubleshoot the problem in time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as required.
hillstoneFANStatus			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates that the memory utilization exceeds the configured (through the monitor alarm	Necessary clearance of the memory is needed if the memory util-

OID	Severity	Description	Solution
		function) threshold.	ization is too high.
hillstoneMemoryStatusAlertClear			
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high memory utilization as required.
hillstoneHAStatus			
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device failure. Therefore, troubleshoot the problem in time.
hillstoneADType			
1.3.6.1.4.1.28557.3.6	Critical	This notification indicates that the Attack Defend(AD) function is enabled in the Security Zone and the device detects the corresponding attack.	Figure out whether the attack exists in the environment. If yes, take further measures, such as using policy rules or blacklist, to block the attacking traffic.

OID	Severity	Description	Solution
hillstoneVPNDown			
1.3.6.1.4.1.28557.3.7	Warning	This notification indicates that the IPSec VPN tunnel is disconnected.	1. Check the quality of the physical links. 2. Confirm the status of the tunnel peer.
hillstoneVPNUp			
1.3.6.1.4.1.28557.3.8	Warning	This notification indicates that the IPSec VPN tunnel is connected.	Troubleshoot the previous disconnection of the tunnel.
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address changes.	Check whether the interface is disconnected physically. For example, whether the interface cable is loose.
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of notification alarm. You can ignore or

OID	Severity	Description	Solution
			troubleshoot it according to your conditions.
hillstoneSystemReboot			
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.
HillstoneDiskSpaceStatus			
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.
hillstoneSessionOverThreshold			
1.3.6.1.4.1.28557.3.15	Warning	This notification indicates that the Session ratio exceeds the threshold.	This alarm is based on your con-

OID	Severity	Description	Solution
			figuration of the threshold. Confirm whether the alarming Session ratio is normal.
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates that the using ratio of the Log Buffer exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log Buffer is normal.
hillstonePolicyCountOverThreshold			
1.3.6.1.4.1.28557.3.18	Critical	This notification indicates that the number of the configured policies exceeds the threshold.	You can clean up policies or control the number of subsequent new policies.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates	Confirm whether

OID	Severity	Description	Solution
		that the slot is offline.	the slot is offline or it is a false alarm.
hillstoneSNATResourceOverThreshold			
1.3.6.1.4.1.28557.3.22	Critical	This notification indicates that the using ratio of the SNAT resources reaches the configured (through the monitor alarm function) threshold.	Once SNAT resources are used up, the network connection will fail because subsequent traffic cannot be translated. Therefore troubleshoot this problem in time.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.

OID	Severity	Description	Solution
hillstoneBypassInline			
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates that the status of the power module is abnormal.	Malfunction of the power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warning, or fail.	Troubleshoot the malfunction of the fans.

OID	Severity	Description	Solution
hillstoneFANStopClear			
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan status as required.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as required.
hillstoneHardDiskSpaceStatus			
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	The Trap host can delete previous alarms of high disk utilization as required.

OID	Severity	Description	Solution
hillstoneUserLogoutAlarm			
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneIFPhysicalUp			
1.3.6.1.4.1.28557.3.66	Warning	The notification indicates that the physical status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFPhysicalDown			
1.3.6.1.4.1.28557.3.67	Warning	The notification indicates that the physical status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFAdminUp			
1.3.6.1.4.1.28557.3.68	Warning	The notification indicates that	It is a type of noti-

OID	Severity	Description	Solution
		the admin status of the interface changes to UP (available).	fication alarm. You can address it according to your conditions.
hillstoneIFAdminDown			
1.3.6.1.4.1.28557.3.69	Warning	The notification indicates that the admin status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFLinkUp			
1.3.6.1.4.1.28557.3.70	Warning	The notification indicates that the link status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFLinkDown			
1.3.6.1.4.1.28557.3.71	Warning	The notification indicates that the link status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocolUp			
1.3.6.1.4.1.28557.3.72	Warning	The notification indicates that the IPv4 protocol status of	It is a type of notification alarm. You

OID	Severity	Description	Solution
		the interface changes to UP (available).	can address it according to your conditions.
hillstoneIFProtocolDown			
1.3.6.1.4.1.28557.3.73	Warning	The notification indicates that the IPv4 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocol6Up			
1.3.6.1.4.1.28557.3.74	Warning	The notification indicates that the IPv6 protocol status of the interface changes to UP (available).	It is a type of notification alarm. You can address it according to your conditions.
hillstoneIFProtocol6Down			
1.3.6.1.4.1.28557.3.75	Warning	The notification indicates that the IPv6 protocol status of the interface changes to Down (unavailable).	It is a type of notification alarm. You can address it according to your conditions.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 41829

Supporting to Obtain the Number of Concurrent Connections and New Connection Rate of Current NAT Sessions of Device by Using SNMP

MIB

HILLSTONE-SYSTEM-MIB

The following tables is the parsing results of HILLSTONE-SYSTEM-MIB.

Name	OID	Value
sysSerialNumber	.1.3.6.1.4.1.28557.2.2.1.1	Data type: String Description: Product serial number
sysSoftware	.1.3.6.1.4.1.28557.2.2.1.2	Data type: String Description: Software version
sysCPU	.1.3.6.1.4.1.28557.2.2.1.3	Data type: Integer Description: CPU utilization
sysTotalMemory	.1.3.6.1.4.1.28557.2.2.1.4	Data type: Gauge32 Description: Total memory

Name	OID	Value
sysCurMemory	.1.3.6.1.4.1.28557.2.2.1.5	Data type: Gauge32 Description: Used memory
sysTotalSession	.1.3.6.1.4.1.28557.2.2.1.6	Data type: Counter Description: Maximum session number of the system
sysCurSession	.1.3.6.1.4.1.28557.2.2.1.7	Data type: Gauge32 Description: Active session number
sysHAStatus	.1.3.6.1.4.1.28557.2.2.1.8	Data type: Integer Description: HA status • 0 - Invalid • 1 - Started • 2 - Hello • 3 - Backup device • 4 - Primary

Name	OID	Value
		device • 15 - Failure
sysSnmpStackStatus	.1.3.6.1.4.1.28557.2.2.1.9	Data type: Integer Description: SNMP running status
sysTr069StackStatus	.1.3.6.1.4.1.28557.2.2.1.10	Data type: Integer Description: TR069 running status
sysVedorOUI	.1.3.6.1.4.1.28557.2.2.1.11	Data type: String Description: Provider name
sysLogStackStatus	.1.3.6.1.4.1.28557.2.2.1.12	Data type: Integer Description: Syslog running status
sysLogServerAddress1	.1.3.6.1.4.1.28557.2.2.1.13	Data type: String Description: Syslog server IP address 1

Name	OID	Value
sysLogServerAddress2	.1.3.6.1.4.1.28557.2.2.1.14	Data type: String Description: Syslog server IP address 2
sysDeviceReloadAction	.1.3.6.1.4.1.28557.2.2.1.15	Data type: Integer Data type: String Description: Device reloading. When the value equals 2, the device will reboot.
sysStatisticsPeriod	.1.3.6.1.4.1.28557.2.2.1.16	Data type: Integer Description: Statistic interval. Default value is 24 hours.
sysMemRatio	.1.3.6.1.4.1.28557.2.2.1.17	Data type: Gauge32 Description: Memory usage ratio.
sysSessionRampupRate	.1.3.6.1.4.1.28557.2.2.1.18	Data type:

Name	OID	Value
		Gauge32 Description: New session connection ratio(used for Statistics).
sysOverallThroughput	.1.3.6.1.4.1.28557.2.2.1.19	Data type: Counter64 Description: Root VSYS throughput.
sysCTWapStat	.1.3.6.1.4.1.28557.2.2.1.20	Data type: String Description: WAP status information
sysRamupRate	.1.3.6.1.4.1.28557.2.2.1.21	Data type: Integer Description: New session connection ratio(not related to Statistics).
sysL4SynCheckDrop	.1.3.6.1.4.1.28557.2.2.1.22	Data type: Integer Description: Number of the

Name	OID	Value
		dropped packets during TCP snchronous message error
sys L4SynBitCheckDrop	.1.3.6.1.4.1.28557.2.2.1.23	Data type: Integer Description: Number of the dropped packets during syc bit of TCP message error
sysL4SeqCheckDrop	.1.3.6.1.4.1.28557.2.2.1.24	Data type: Integer Description: Number of the dropped packets during serial number error
sysL4HwCPUError	.1.3.6.1.4.1.28557.2.2.1.25	Data type: Integer Description: Number of the dropped packets during Octeon chip error
sysHistoryMaxSessNum	.1.3.6.1.4.1.28557.2.2.1.26	Data type:

Name	OID	Value
		Gauge32 Description: Maximum number of sessions in history.
sysTCPSessNum	.1.3.6.1.4.1.28557.2.2.1.27	Data type: Gauge32 Description: Number of current TCP sessions.
sysUDPSessNum	.1.3.6.1.4.1.28557.2.2.1.28	Data type: Gauge32 Description: Number of current UDP sessions.
sysICMPSessNum	.1.3.6.1.4.1.28557.2.2.1.29	Data type: Gauge32 Description: Number of current ICMP sessions.
sysCurSessionIPv4	.1.3.6.1.4.1.28557.2.2.1.31	Data type: Gauge32 Description: Total number

Name	OID	Value
		of concurrent IPv4 sessions
sysCurSessionIPv6	.1.3.6.1.4.1.28557.2.2.1.32	Data type: Gauge32 Description: Total number of concurrent IPv6 sessions
sysRampupRateIPv4	.1.3.6.1.4.1.28557.2.2.1.33	Data type: Integer Description: Total rate of new IPv4 sessions
sysRampupRateIPv6	.1.3.6.1.4.1.28557.2.2.1.34	Data type: Integer Description: Total rate of new IPv6 sessions
sysPeerHAStatus	.1.3.6.1.4.1.28557.2.2.1.36	Data type: Integer Description: HA status of the peer device • 0 - none

Name	OID	Value
		• 1 - init • 2 - hello • 3 - backup • 4 - master • 15 – failed
sysHAGroupStatus	.1.3.6.1.4.1.28557.2.2.1.37	Data type: Integer Description: HA status of the master device and backup device in the HA group • 0 - normal • 1 - abnormal
sysHAStatusChangeTimes	.1.3.6.1.4.1.28557.2.2.1.38	Data type: Integer Description: Number of master/backup status changes in the HA group

Name	OID	Value
sysOverallIPv4Throughput	.1.3.6.1.4.1.28557.2.2.1.39	Data type: Counter64 Description: IPv4 throughout of root VSYS
sysOverallIPv6Throughput	.1.3.6.1.4.1.28557.2.2.1.40	Data type: Counter64 Description: IPv6 throughout of root VSYS
sysCurSessionNat	.1.3.6.1.4.1.28557.2.2.1.42	Data type: Gauge32 Description: Number of concurrent connections of current NAT sessions
sysRampupRateNat	.1.3.6.1.4.1.28557.2.2.1.43	Data type: Gauge32 Description: New connection rate of current NAT sessions

Name	OID	Value
sysTopAppthroughputTable: Throughput information of the TOP application		
hillstoneAppIndex	.1.3.6.1.4.1.28557.2.2.1.30.1.1	Data type: Integer Description: The index of the TOP 10 Application.
hillstoneAppthroughput	.1.3.6.1.4.1.28557.2.2.1.30.1.2	Data type: DisplayString Description: The throughput of the TOP 10 application in last 24 hours.
sysPendingSessionQueueFullDrop	.1.3.6.1.4.1.28557.2.2.1.35	Data type: Integer Description: Number of packets dropped caused by full cache queue of sessions.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 41159

Supporting to Store URL Logs of Certain Devices to the Local Database

CLI

Sending Traffic Logs

Traffic logs consist of session logs, NAT logs, and web surfing logs. You can send traffic logs to the console, syslog server, memory buffer and local SSD. You can select the output destination according to your requirements.

To send the traffic logs to the console , buffer or syslog server, use the following command in the global configuration mode:

logging traffic {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** [**size***buffer-size*] }

To send session logs, NAT logs, and URL logs to the local SSD, in the global configuration mode, use the following command:

logging traffic {**session** | **nat** | **urlfilter**} **to localdb**

- **session** | **nat** | **urlfilter** – Specifies the log type that you want to output.
- **console** | **syslog** | **buffer** – Specifies the output destination. You can output the logs to the console ,buffer or syslog server.
- **localdb** – Specifies the output destination of session logs, NAT logs, and URL logs as the SSD on the device. Only CloudEdge, SSD-equipped A-series (except A2200, A1800, and A1600) and SSD-equipped X-series devices (except X10800 and X9180) support this function.
- **size** *buffer-size* - Specifies the buffer size. The value range is 4096 to 524288 bytes. The default value is 1048576.

In the global configuration mode, use the following command to disable the output function: **no logging traffic** {**session** | **nat** | **urlfilter**} **to** {**console** | **syslog** | **buffer** }or **no logging traffic** {**session** | **nat** | **urlfilter**} **to localdb**.

For more information, refer to the **Monitor** > **Log** > **Configuring System Logs** topic in *StoneOS CLI User Guide*. FR37812

Configuring Storage Space of Log

The system allocates a default disk space size for the log of each module, and you can customize the disk space size for the log as needed.

To configure the storage space of log, in the global configuration mode, use the following command:

storage threshold log {**configuration** | **event** | **network** | **sandbox** | **threat** | **traffic** {**session** | **nat** | **urlfilter**} } *percent-value*

- {**configuration** | **event** | **network** | **sandbox** | **threat** | **traffic** {**session** | **nat** | **urlfilter**} } *percent-value* - Specify the disk space size of the log.

To restore to the default disk space size of log, use the following command:

no storage threshold log {**configuration** | **event** | **network** | **sandbox** | **threat** | **traffic** {**session** | **nat** | **urlfilter**} }

The default disk space size differs from devices and log types. After restoring to the default disk space size of log, you can use the **show storage threshold** command to view the default settings.

For more information, refer to the **System Management** > **Configuring Storage Management** topic in *StoneOS CLI User Guide*. FR37812

WebUI

URL Log

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

URL logs can be generated under the conditions that:

- URL logging in the Logging feature is enabled. Refer to Managing Logs.
- You have enabled logging function in URL rules. Refer to URL Filter.

To view URL logs, select **Monitor > Log > URL Log**.



- Configure: Click this button to configure URL logs on the Log Management page.
- Clear: Click this button to clear all URL logs stored in the system. (Note: This option is not available for devices that support to store logs to the local database)
- Export: Click this button, specify the delimiter, and then export all the URL log information stored in the system or search results (search first and then export), and you can add an encrypted password for the exported file as needed. After you add an encrypted password, you can view the file only when you enter this password to view the file.

For more information, refer to the **Monitor > Log > URL Log** topic in *StoneOS WebUI User Guide*. FR37812

Option Descriptions of Various Log Types

URL Log

Option	Description
Enable	Click the button to enable the URL logging function. • Record Host Name: Select to show the host's name in the URL log messages.
Cache	Select the check box to export URL logs to the cache.

Option	Description
	• Max Buffer Size - The maximum size of the cached URL logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send URL logs to the local database. Note: A-series (except A2200, A1800, and A1600)X (except X10800 and X9180)-series firewalls installed with hard disks support this function.
Log Server	Select the check box to export URL logs to a log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

For more information, refer to the **Monitoring** > **Logging** > **Managing Logs** topic in *StoneOS WebUI User Guide*. FR37812

Configuration Item Changes of the Report Task Configuration Page

Description for configuration item changes: The report task configuration page involves three configuration item changes:

- Changes to the time configuration for generating reports immediately. Platforms that only support customized times now support predefined time ranges.

- Support for configuring the language of report content.
- The email address of the report file recipient is changed from text box input to form input.

WebUI

Report Task

The report task is the schedule related to report file. It defines the report template, data range, generation period, generation time, and the output method of report files.

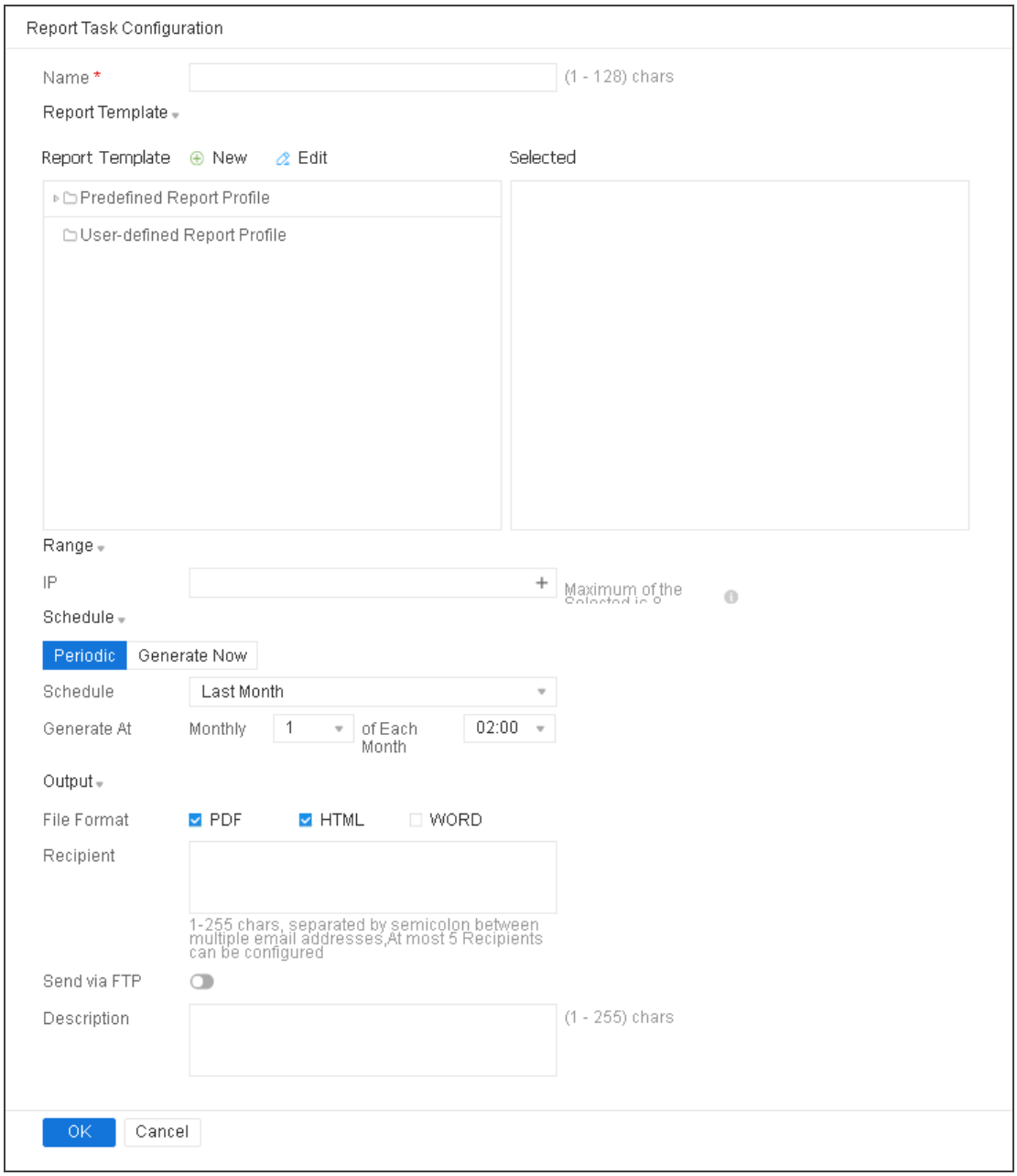
You can configure report tasks and generate report files on the device according to your needs.

Creating a Report Task

To create a report task, take the following steps:

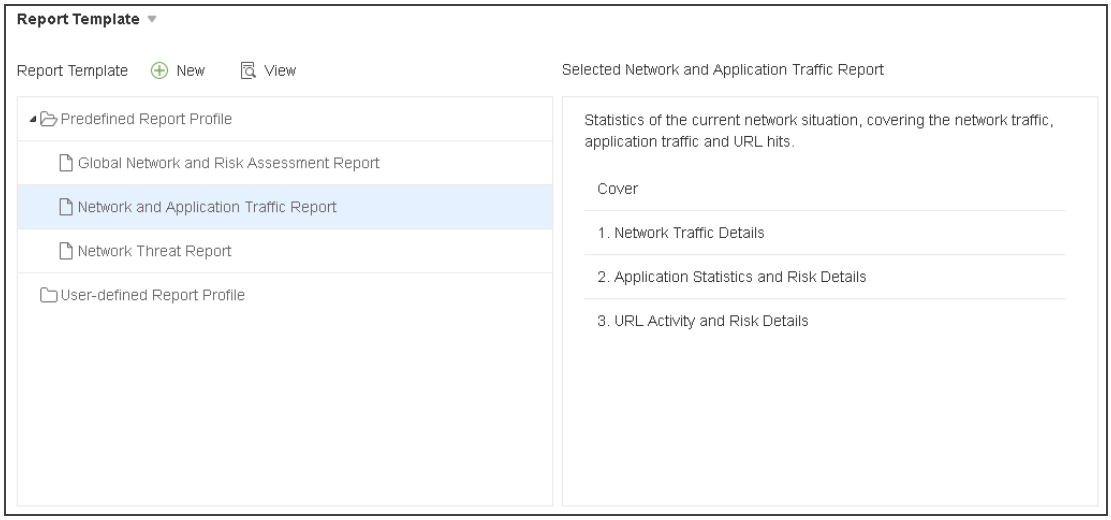
1. Select **Monitor > Report > Report Task**.

2. Click **New**.



In this page, configure the values of report task.

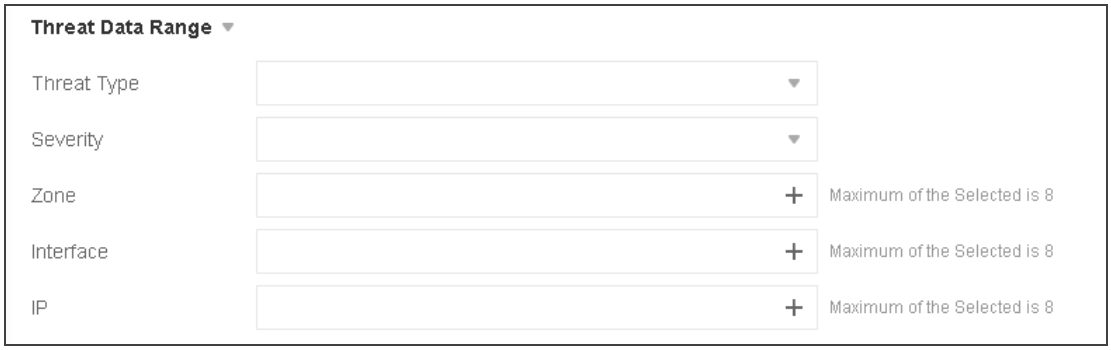
Option	Description
Name	Specifies the name of the report task.
Description	Specifies the description of the report task. You can modify it according to your requirements.





Expand Report Template, select the report template you want to use for the report task.

Option	Description
Report Template	Specifies the report template to be used by the report task: 1. Select the report template (predefined report template or created user-defined report template) from the **Report Template** list on the left. 2. When the report template is selected, the selected report template list shows the description of the template and the details of the report item on the right. You can also click **New** or **Edit** button in the **Report Template** list on the left to open the **Report Template Configuration** page and create or edit a user-defined report template quickly.



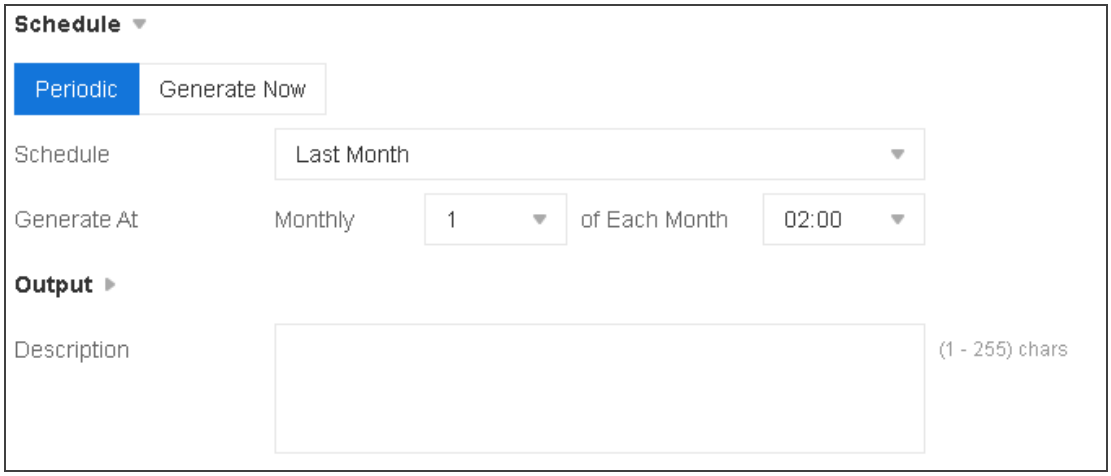
Expand Threat Data Range

Option	Description
Threat Type	Specifies the type of threat to generate report statistics. There are six threat types, which are Scan, Attack, Dos,

Option	Description
	Phishing, Spam, and Malware.
Severity	Specifies the threat level for generating report statistics. The threat level can be Critical, High, Medium, or Low.
Zone	Specifies the security zone of the report statistics. 1. Click + of the **Zone** drop-down list. 2. Specifies the zone from the **Zone** list that appears on the right. • To modify the configuration of a zone, hover your mouse over the zone entry and then click  to go to the **Zone Configuration** page. • To create a new zone, click  to go to the **Zone Configuration** page.
Interface	Specifies the interface of the report statistics. 1. Click + of the **Interface** drop-down list. 2. Specifies the interface from the **Interface** list that appears on the right. • To modify the configuration of an interface, hover your mouse over the interface entry and then click  to go to the **Ethernet Interface** page.

Option	Description
	• To create a new zone, click ⊕ to go to the **Ethernet Interface** page.
IP	Specifies the IP range for generating report statistics. The IP range can include both source IP address and destination IP address. 1. Click **+** of the **IP** drop-down list. 2. Select the IP address type from the **IP** list that appears on the right, including IP/Netmask, IPv4 Range, IPv6/Prefix, and IPv6 Range.and IP Range. 3. Enter the required address of the address type. 4. Click **Add** to add the addresses to the right pane. 5. After adding the desired addresses, click **Close** to complete the configuration. 6. If you need to delete the added address, select the address you want to delete in the right pane, and click ✕.

Notes: This configuration item is supported only by devices with hard disks.



Expand Schedule, configure the running time of the report task.

Option	Description
Schedule	The schedule specifies the running time of the report task. The report task can be run periodically or run immediately. Periodic: Generates report files as planned. • Schedule (E-series): Generates a report file based on data within the specified statistical period, which can be last 24 hours or last 30 days. • Schedule (A-series): Generates a report file based on data within the specified statistical period. For devices installed with SSD (except A2200, A1800, and A1600), the statistical period can be last 24 hours, last 7 days, last 30 days, last three months, last six months, or last 12 months; For A2200, A1800, A1600, and devices that are not installed with SSD, the statistical period can be last 24 hours

Option	Description
	or last 30 days. • Schedule (CloudEdge): Generates a report file based on data within the specified statistical period, which can be last 24 hours, last 7 days, last 30 days, last three months, last six months, or last 12 months. • Schedule (X-series): For X25812, X25803, and X8180 installed with SSD, the statistical period can be last 24 hours, last 7 days, last 30 days, last three months, last six months, or last 12 months; For other models of devices or X25812, X25803, and X8180 that are not installed with SSD, the statistical period can be last 24 hours or last 30 days. • Generate At: Specifies the generation time. Generate Now: Generates report files immediately. • Schedule (E-series): Generates a report file based on data within the specified statistical period, which can be last 24 hours or last 30 days. • Schedule (A-series): Generates a report file based on data within the specified statistical period. For devices installed with SSD (except A2200, A1800, and A1600), the statistical period can be last 24

Option	Description
	hours, last 7 days, last 30 days, last three months, last six months, or last 12 months; For A2200, A1800, A1600, and devices that are not installed with SSD, the statistical period can be last 24 hours or last 30 days. • Schedule (CloudEdge): Generates a report file based on data within the specified statistical period, which can be last 24 hours, last 7 days, last 30 days, last three months, last six months, or last 12 months. • Schedule (X-series): For X25812, X25803, and X8180 installed with SSD, the statistical period can be last 24 hours, last 7 days, last 30 days, last three months, last six months, or last 12 months; For other models of devices or X25812, X25803, and X8180 that are not installed with SSD, the statistical period can be last 24 hours or last 30 days. **Note**: If you customize a time period, you need to specify the start time of the statistical period in the time text box. The start time can be a specific point in time, but the interval between the start time and end time should be longer than 24 hours but less than one year.



Expand Output, configure the output mode information of the report.

Option	Description
Report content language	Specifies the language type of the report content, which can be Chinese or English. By default, the language is consistent with that of the current WebUI.
File Format	Specifies the output format of the report file, including PDF, HTML, and WORD formats.
Recipient	Sends report file via email. To add recipients, enter the email addresses in to the recipient text box (use ";" to separate multiple email addresses. Up to 5 recipients can be configured).
Send via FTP	Click the **Enable** button to send the report file to a specified FTP server. • Server Name/IP: Specifies the FTP server name or the IP address. • Virtual Router: Specifies the virtual router of the FTP server from the drop-down list. To create a new virtual router, click the drop-down list and then click ⊕ on the expanded virtual router list to go to the **Virtual Router Configuration** page. • Username: Specifies the username used to log on to the FTP server. • Password: Enter the password of the FTP user-

Option	Description
	name. • Anonymous: Select the check box to log on to the FTP server anonymously. • Path: Specifies the location where the report file will be saved.

3. Click **OK**.

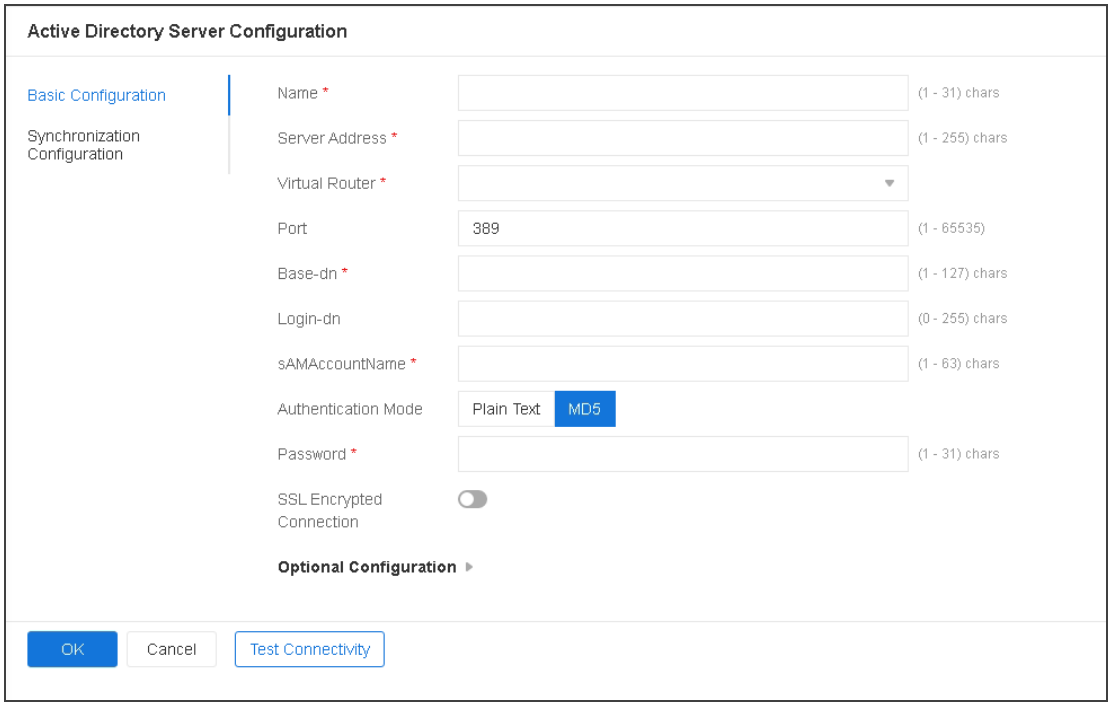
For more information, refer to the **Monitor** > **Reporting** > **Report Task** topic in *StoneOS WebUI User Guide*. FR38691

Supporting not to Verify Server Certificate When Connecting to AD/LDAP Authentication Server by Using SSL Encryption

WebUI

Configuring Active Directory Server

1. Select **Object** > **AAA Server**, and click **New** > **Active Directory Server**.
2. The **Active Directory Server Configuration** page opens.



Configure the following.

Basic Configuration	
Name	Specifies a name for the Active Directory server.
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the Active Directory server.
Virtual Router	Specifies a VR for the Active Directory server.
Port	Specifies a port number for the Active Directory server. The value range is 1 to 65535. The default value is 389.
Base-dn	Specifies a Base-dn for the AD server. The Base-dn is the starting point at which your search will begin when the AD server receives an authentication

Basic Configuration	
	request. For the example of abc.xyz.com as described above, the format for the Base-dn is "dc=a-abc,dc=xyz,dc=com".
Login-dn	Specifies authentication characteristics for the Login-dn (typically a user account with query privilege pre-defined by the AD server). When the authentication mode is plain, the Login-dn should be configured. DN (Distinguished name) is a username of the AD server who has a privilege to read user information. The format of the DN is"cn=xxx, DC=xxx,...". For example, the server domain is abc.xyz.com, and the AD server admin name is administrator who locates in Users directory. Then the login-dn should be "cn=a-administrator,cn=users,dc=abc,dc=xyz,dc=com".
sAMAc-countName	When the authentication mode is MD5, the sAMAc-countName should be configured. sAMAc-countName is a username of the AD server who has a privilege to read user information. The format of sAMAccountName is "xxx". For example, the AD server admin name is administrator , and then the sAMAccountName should be "administrator".
Authentication Mode	Specifies an authentication or synchronization method (either plain text or MD5). The default

Basic Configuration	
	method is MD5. If the sAMAccountName is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating the user.
Password	Specifies a password for the AD server.
SSL Encrypted Connection	Click the **Enable** button to enable the SSL encrypted connection function. With this function enabled, the system connects to the Active Directory authentication server through SSL.
SSL Certificate Verification	Enable or disable the SSL certificate verification function: • If you enable this function, when the firewall is connected to the Active Directory server by using SSL encryption, you need to import the certificate of the Active Directory server to the firewall system for verification. • If you disable this function, when the firewall is connected to the Active Directory server by using SSL encryption, the connection can be successful without importing the certificate of the Active Directory server. When you need to

Basic Configuration	
	connect to the Active Directory server by using SSL encryption but cannot obtain the server certificate, you can disable the SSL certificate verification function. **Note**: The SSL certificate verification function takes effect only after the SSL Encrypted Connection function is enabled.
Optional Configuration	
Authorization Policy	When a user is authenticated by the Radius server, when the user is authenticated successfully, the Radius server will create a security policy for the authenticated user that includes the destination network segment, destination port, protocol, and behavior. This policy is called an authorization policy. System supports two authorization policies: "Authorization Policy During Authentication" and "Dynamic Authorization Policy". You can enable the authorization policy function to enable to obtain the authorization policy from the Radius server and add it to the system's policy list to make it effective. When the authenticated user is disconnected, the authorization policy will be deleted automatically. • By default, the authorization policy is disabled. Select the checkbox after **Authorization**

Basic Configuration	
	Policy to enable the authorization policy. After the authorization policy of the Radius server is enabled, you add the obtained authorization policy to the aggregation policy that has been created, and arrange it as the member of aggregation policy at the end of aggregation policy, which is more convenient for the user to manage the authorization policy uniformly. If it is not added to the aggregation policy, the authorization policy will be added to the end of the system policy list by default. • Select the aggregate policy name from the drop-down list.
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name

Basic Configuration	
	in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.
Authentication Base-DN	Specifies an authentication Base-dn for the AD server. All users in the Base-DN (including those directly under the user group) will be allowed to pass the authentication. The format of the DN is"OU-U=xxx, DC=xxx,...".
Synchronization Base-DN	Specifies a Synchronization Base-dn for the AD server. All users and user groups in the Base-DN will be synchronized to the local. The format of the DN is"OU=xxx, DC=xxx,...".
Synchronization	Check the checkbox to enable the synchronization function; clear the checkbox to disable the synchronization function, and the system will stop synchronizing and clear the existing user information.

Basic Configuration	
	By default, system will synchronize the user information on the configured Active-Directory server with the local server every 30 minutes.
Automatic Synchronization	Click the radio button to specify the automatic synchronization. Interval Synchronization: Specifies the time interval for automatic synchronization. The value range is 15 to 1440 minutes. The default value is 30. Daily Synchronization: Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively. Once Synchronization: If this parameter is specified, system will synchronize automatically when the configuration of Active-Directory server is modified. After executing this command , system will synchronize the user information immediately.
Synchronous Operation Mode	Specifies user synchronization mode, including Group Synchronization and OU Synchronization. By default, the user information will be synchronized

Basic Configuration	
	with the local server based on the group.
Synchronization Object	Filter the synchronization information obtained and retain the information of the specified object. You can select the syn object as users or groups. By default, users and groups are both selected.
OU maximum depth	Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the “OU=” string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.
User Filter	Specifies the user-filter conditions. System can only synchronize and authenticate users that are in accordance with the filtering condition on the authentication server. The length is 0 to 120 characters. For example, if the condition is configured to “memberOf=CN=Admin,DC=test,DC=com”, system only can synchronize or authenticate user whose DN is “memberOf=CN=Admin,DC=test,DC=com”. The commonly used operators are: =(equals a value)、&(and）、|(or)、!(not)、*(Wildcard:

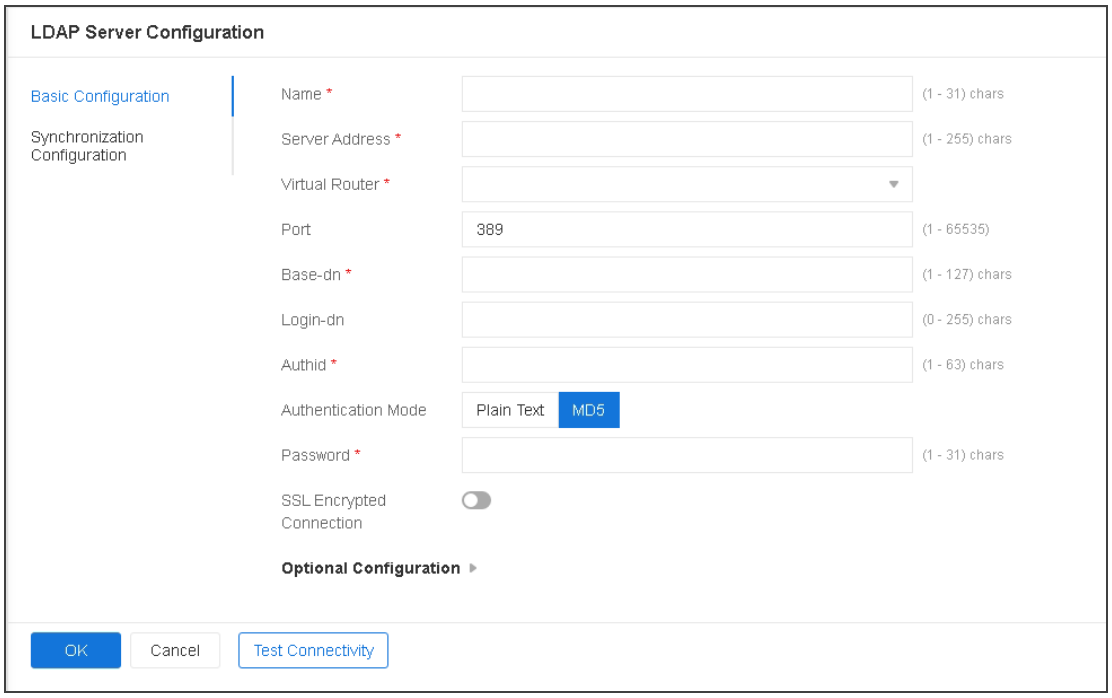
Basic Configuration	
	when matching zero or more characters)、 ~=(fuzzy query.)、 >=Be greater than or equal to a specified value in lexicographical order.)、 <=(Be less than or equal to a specified value in lexicographical order.).
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Synchronization Base-dn	Synchronization Base-DN is the starting point at which the system synchronizes users and user groups from the Active Directory server. Click this field. In the **Server Directory** panel, select the path that you want to synchronize. This way, all users and user groups in the path are synchronized to the local. At most 32 paths can be selected.

3. Click **OK**.

Configuring LDAP Server

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

2. The **LDAP Server Configuration** page opens.



Configure the following

Basic Configuration	
Server Name	Specifies a name for the LDAP server.
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the LDAP server.
Virtual Router	Specifies a VR for the LDAP server.
Port	Specifies a port number for the LDAP server. The value range is 1 to 65535. The default value is 389.
Base-dn	Specifies the details for the Base-dn. The Base-dn is the starting point at which your search will begin when

Basic Configuration	
	the LDAP server receives an authentication request.
Login-dn	Specifies authentication characteristics for the Login-dn (typically a user account with query privileges pre-defined by the LDAP server).
Authid	Specifies the Authid, which is a string of 1 to 63 characters and is case sensitive.
Authentication Mode	Specifies an authentication or synchronization method (either plain text or MD5). The default method is MD5. If the Authid is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.
Password	Specifies a password for the LDAP server. This should correspond to the password for Admin DN.
SSL Encrypted Connection	Click the **Enable** button to enable the SSL encrypted connection function. With this function enabled, the system connects to the LDAP authentication server through SSL.
SSL Certificate Verification	Enable or disable the SSL certificate verification function: • If you enable this function, when the firewall is connected to the Active Directory server by

Basic Configuration	
	using SSL encryption, you need to import the certificate of the Active Directory server to the firewall system for verification. • If you disable this function, when the firewall is connected to the Active Directory server by using SSL encryption, the connection can be successful without importing the certificate of the Active Directory server. When you need to connect to the Active Directory server by using SSL encryption but cannot obtain the server certificate, you can disable the SSL certificate verification function. **Note**: The SSL certificate verification function takes effect only after the SSL Encrypted Connection function is enabled.
Optional Configuration	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".

Basic Configuration	
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "user-name@domain".
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.
Authentication Base-DN	Specifies an authentication Base-dn for the AD server. All users in the Base-DN (including those directly under the user group) will be allowed to pass the authentication. The format of the DN is"OU=xxx, DC=xxx,...".
Synchronization Base-DN	Specifies a Synchronization Base-dn for the AD server.

Basic Configuration	
	All users and user groups in the Base-DN will be synchronized to the local. The format of the DN is"OU-U=xxx, DC=xxx,...".
Synchronization	Check the checkbox to enable the synchronization function; clear the checkbox to disable the synchronization function, and system will stop synchronizing and clear the existing user information. By default, system will synchronize the user information on the configured LDAP server with the local every 30 minutes.
Automatic Synchronization	Click the radio button to specify the automatic synchronization. Interval Synchronization: Specifies the time interval for automatic synchronization. The value range is 15 to 1440 minutes. The default value is 30. Daily Synchronization: Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively. Once Synchronization: If this parameter is specified, system will synchronize automatically when the configuration of LDAP server is modified.

Basic Configuration	
	After executing this command , system will synchronize user information immediately.
Synchronous Operation Mode	Specifies the user synchronization mode, including Group Synchronization and OU Synchronization. By default, the user information will be synchronized with the local server based on the group.
Synchronization Object	Filter the synchronization information obtained and retain the information of the specified object. You can select the syn object as users or groups. By default, users and groups are both selected.
OU maximum depth	Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level(including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.
User Filter	Specifies the user filters. System can only synchronize and authenticate users that match the filters on the authentication server. The length is 0 to 120 characters.

Basic Configuration	
	For example, if the condition is configured to “(|(objectclass=inetOrgperson)(objectclass=person))”, system only can synchronize or authenticate users which are defined as inetOrgperson or person. The commonly used operators are as follows: =(equals a value)、&(and）、|(or)、!(not)、*(Wildcard: when matching zero or more characters)、～=(fuzzy query.)、>=(Be greater than or equal to a specified value in lexicographical order.)、<=(Be less than or equal to a specified value in lexicographical order.).
Naming Attribute	Specifies a naming attribute for the LDAP server. The default naming attribute is uid.
Group Naming Attribute	Specifies a naming attribute of group for the LDAP server. The default naming attribute is uid.
Member Attribute	Specifies a member attribute for the LDAP server. The default member attribute is uniqueMember.
Group Class	Specifies a group class for the LDAP server. The default class is groupofuniquenames.
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the LDAP server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing

Basic Configuration	
	local, Active-Directory, RADIUS or LDAP server defined in system.
Synchronization Base-dn	Synchronization Base-DN is the starting point at which the system synchronizes users and user groups from the LDAP server. Click this field. In the **Server Directory** panel, select the path that you want to synchronize. This way, all users and user groups in the path are synchronized to the local. At most 32 paths can be selected.

3. Click **OK**.

For more information, refer to the **Object** > **AAA Server** topic in *StoneOS WebUI User Guide*.
FR35529

CLI

Configuring an Active-Directory Authentication Server

To enter the Active-Directory server configuration mode, in the global configuration mode, use the command **aaa-server***aaa-server-name***typeactive-directory**.

- The Active-Directory authentication server configuration includes:
- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number

- Configuring the authentication or synchronization method
- Refreshing the connection with the server
- Specifying the Base-DN
- Specifying the Synchronization Base-DN
- Specifying the Synchronization Object
- Specifying the Authentication Base-DN
- Specifying the login DN
- Specifying sAMAccountName
- Specifying the login password
- Specifying the mobile attribute field
- Enabling/Disabling the SSL Encrypted Connection
- Enabling/Disabling SSL Certificate Verification
- Specifying user name format
- Specifying a role mapping rule
- Configuring a user blacklist
- Configuring a LDAP User
- Configuring User Expiration
- Configuring the Brute-force Cracking Defense
- Configuring an AD User
- Configuring User Expiration

- Configuring automatic user information synchronization
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server
- Configuring the User-Groups under Base-DN Synchronization
- Enabling/Disabling Authentication Simplification

Enabling/Disabling SSL Certificate Verification

When the firewall is connected to the Active Directory server by using SSL encryption, you need to import the certificate of the Active Directory server to the firewall system for verification. However, sometimes you may fail to obtain the server certificate so that you cannot use SSL encrypted connection. To resolve this issue, the system allows you to configure whether to enable SSL certificate verification. If disabled, when the firewall is connected to the Active Directory server by using SSL encryption, the connection can be successful without importing the certificate of the Active Directory server.

By default, the SSL certificate verification function is enabled. To enable/disable this function, in Active Directory server configuration mode, use the following command:

verify-certificate {**enable** | **disable**}

- **enable** | **disable** - Enable (**enable**) or disable (**disable**) the SSL certificate verification function.

> **Notes:** The SSL certificate verification function takes effect only after the SSL Encrypted Connection function is enabled.

Configuring an LDAP Authentication Server

To enter the LDAP server configuration mode, in the global configuration mode, use the command **aaa-server***aaa-server-name***typeldap**.

The LDAP authentication server configuration includes:

- Configuring the IP address or domain name of the primary server
- Configuring the IP address or domain name of the backup server 1
- Configuring the IP address or domain name of the backup server 2
- Configuring the port number
- Configuring the authentication or synchronization method
- Refreshing the connection with the Server
- Specifying the Base-DN
- Specifying the Synchronization Base-DN
- Specifying the Synchronization Object
- Specifying the login DN
- Specifying Authid
- Specifying the login password
- Enabling/Disabling the SSL Encrypted Connection
- Enabling/Disabling SSL Certificate Verification
- Specifying the name attribute
- Specifying the Group-class
- Specifying the member attribute
- Specifying the mobile attribute field
- Specifying user name format
- Specifying a role mapping rule

- Configuring a user blacklist
- Configuring the Brute-force Cracking Defense
- Configuring automatic user information synchronization
- Configuring user filter
- Configuring synchronization mode of user information
- Configuring a backup authentication server
- Enabling/Disabling Authentication Simplification

Enabling/Disabling SSL Certificate Verification

When the firewall is connected to the LDAP server by using SSL encryption, you need to import the certificate of the LDAP server to the firewall system for verification. However, sometimes you may fail to obtain the server certificate so that you cannot use SSL encrypted connection. To resolve this issue, the system allows you to configure whether to enable SSL certificate verification. If disabled, when the firewall is connected to the LDAP server by using SSL encryption, the connection can be successful without importing the certificate of the LDAP server.

By default, the SSL certificate verification function is enabled. To enable/disable this function, in LDAP server configuration mode, use the following command:

verify-certificate {**enable** | **disable**}

- **enable** | **disable** - Enable (**enable**) or disable (**disable**) the SSL certificate verification function.

> **Notes:** The SSL certificate verification function takes effect only after the SSL Encrypted Connection function is enabled.

For more information, refer to the **User Authentication** > **Authentication, Authorization and Accounting** > **Configuring an AAA Server** > **Configuring an Active-Directory Authentication Server** topic and **User Authentication** > **Authentication, Authorization and Accounting** > **Con-**

figuring an AAA Server > Configuring an LDAP Authentication Server topic in *StoneOS CLI User Guide*. FR35529

Distributed Devices Support to Send Monitor Data such as Threat Logs to Cloud Platform and iSource

WebUI

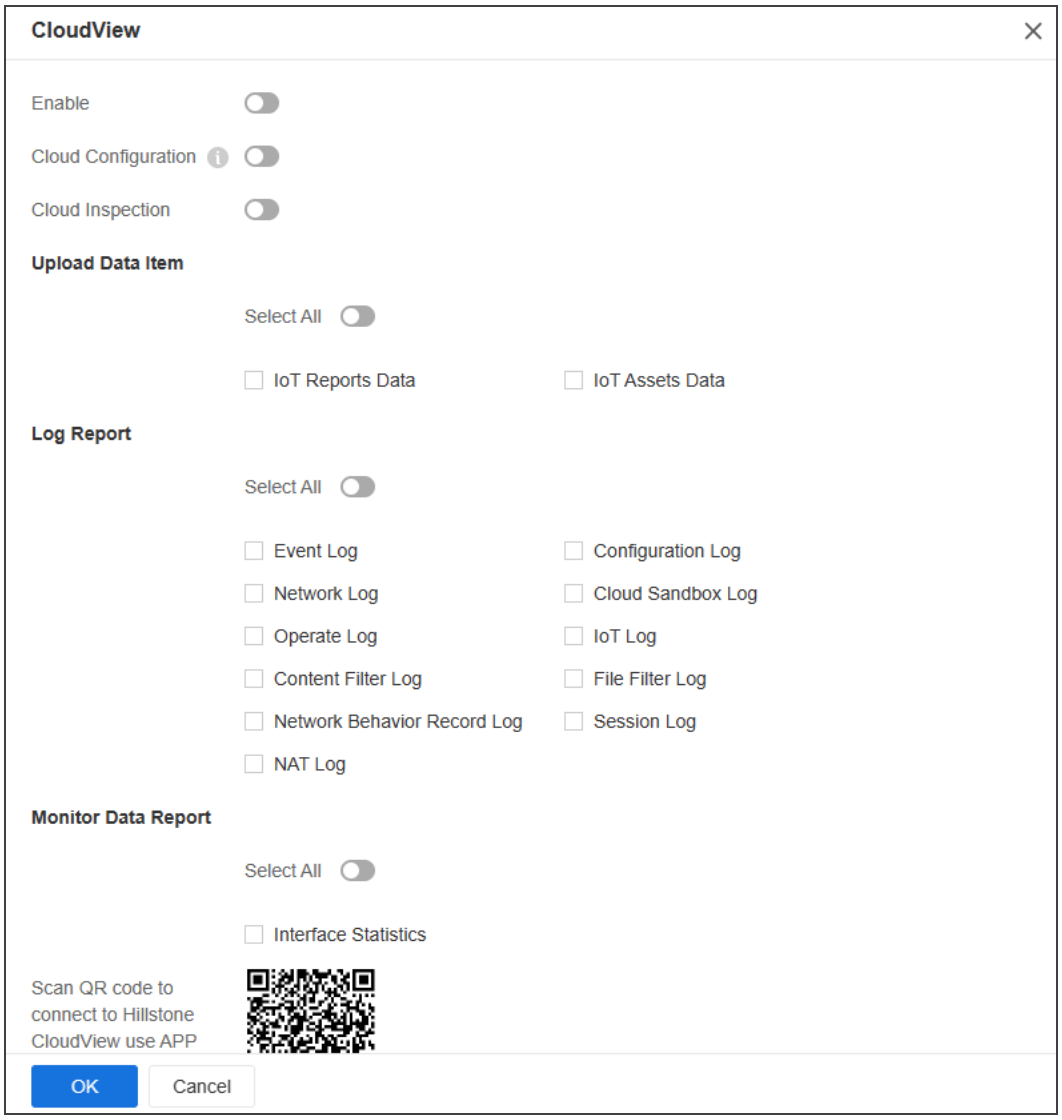
Configuring CloudView

CloudView can be used to visualize device information, traffic data, threat events, and system logs that are uploaded to the cloud platform.

To configure CloudView, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.

2. Click **CloudView**.



3. In this panel, configure the following options.

Option	Description
Enable	Click the **Enable** button to enable the Hillstone CloudView service.

Option	Description
Cloud Configuration	You can configure this function only when CloudView is enabled. Click the enable button to allow CloudView to send configuration to the device. The system will load the real-time configuration sent by CloudView. • PTF Dynamic IP Blacklist: Log in to CloudView to send the configuration of the PTF dynamic IP blacklist to the root VSYS of the device. Both IPv4 and IPv6 addresses are supported. You can also specify the virtual router to take effect as well as the block duration. When the system receives the configuration task from CloucView, corresponding dynamic IP blacklist entries, configuration logs, and operation logs are generated.
Cloud Inspection	Click the **Enable** button to enable the cloud inspection function and upload the collected inspection data to the cloud service platform. With the cloud inspection function, the device can receive and execute the inspection instructions from the cloud, and upload the collected inspection data to the cloud service platform, which enables you to carry out real-time monitoring and management on the cloud anytime and anywhere.
Upload Data Item	Select the data item that you want to upload to the cloud platform, including the IoT reports data, and IoT Assets data. If you enable Select All, all IoT data are uploaded.
Log Report	Select the type of logs that you want to upload to the cloud platform, including event logs, threat logs, configuration logs, net-

Option	Description
	work logs, cloud sandbox logs, operation logs, content filter logs, file filter logs, network behavior record logs, session logs, and NAT logs. If you enable Select All, all logs are uploaded. Note: • For X series devicesK6580/K9180 devices, you are not allowed to upload threat logs to the cloud platform. • The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.
Monitor Data Report	Select the monitor data type that you want to upload to the cloud platform, including the traffic ranking, session ranking, URL ranking, device information, VPN statistics, and interface statistics (including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface in the device). If you enable Select All, all monitor data is uploaded. **Notes:** For X series devicesK6580/K9180 devices, you are only allowed to upload interface statistics to the cloud platform.
Scan QR code to connect to	Scan the QR code using a QR reader app on your smartphone or mobile device to connect to Hillstone CloudView via APP.

Option	Description
Hillstone CloudView use APP	
Visit CloudView	Click the button to visit CloudView.

4. Click **OK**.

For more information, refer to the **System Management > Connecting to Hillstone Cloud Service Platform** topic in *StoneOS_WebUI_User_Guide*. FR 35753, FR 39056, FR 39058

Configuring the Data Types Sent to iSource

To configure the data types sent to iSource after the device is connected to iSource, take the following steps:

1. Select **System > Extended Services**. In the **Connect to Security Operations Platform**, click  in the lower-left corner.

2. In the **Data Upload Configuration** section, configure the following options as needed:

   - Turn on the switch next to Threat Log to send threat logs to iSource. By default, this feature is disabled.
   - Turn on the switch next to Forensic Pcap to send threat-related evidential packets captured by the device to iSource. By default, this feature is disabled.
   - Turn on the switch next to IoT Asset Monitor to send detected IoT asset data to iSource.

3. Click **OK**.

Notes:

- A-series devices that are installed with SSD , K-series devices (except K6580/K9180) that are installed with SSDCloudEdgesupport to upload threat-related evidential packets captured by the device to iSource.

For more information, refer to the **System Management > Connecting to iSource** topic in *StoneOS_WebUI_User_Guide*. FR 35753, FR 39056, FR 39058

CLI

Enabling Log Report

To upload log data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

- **log-cf** -Specifies to upload content filter logs of the device to the cloud platform.
- **log-config** - Specifies to upload configuration logs of the device to the cloud platform.
- **log-dlp** - Specifies to upload file content logs of the device to the cloud platform.
- **log-event** - Specifies to upload event logs of the device to the cloud platform. By default, the upload interval is 10 minutes. Before you enable the function, make sure that the device is enabled with the **logging event on** function.
- **log-iot** - Specifies to upload IoT logs of the device to the cloud platform.
- **log-nat** - Specifies to upload NAT logs of the device to the cloud platform.
- **log-nbr** - Specifies to upload network behavior audit logs of the device to the cloud platform.
- **log-network** - Specifies to upload network logs of the device to the cloud platform.

- **log-operat** - Specifies to upload operation logs of the device to the cloud platform.
- **log-sandbox** - Specifies to upload cloud sandbox logs of the device to the cloud platform.
- **log-session** - Specifies to upload session logs of the device to the cloud platform.
- **threat-event** - Specifies to upload threat events of the device to the cloud platform. By default, the upload interval is 60 minutes.
- **all** - Specifies to upload all monitoring data above of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-log {**all** | **log-cf** | **log-config** | **log-dlp** | **log-event** | **log-iot** | **log-nat** | **log-nbr** | **log-network** | **log-operat** | **log-sandbox**| **log-session** | **threat-event**}

Notes:

- The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.

Enabling Monitoring Data Uploading

To upload monitoring data of the device to the cloud platform, in Cloud View configuration mode, use the following command:

uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}

- **traffic-rank** -Specifies to upload the traffic ranking data of the device to the cloud platform.
- **stats-session** - Specifies to upload the session ranking data of the device to the cloud platform.
- **stats-url-rank** - Specifies to upload the URL ranking data of the device to the cloud platform.

- **stats-device** -Specifies to upload the device information data of the device to the cloud platform.
- **scvpn-user** - Specifies to upload the VPN statistics of the device to the cloud platform.
- **stats-interface** - Specifies to upload the interface statistics of the device to the cloud platform, including the maximum upstream rate, maximum downstream rate, average upstream rate, and average downstream rate of each interface.
- **all** - Specifies to upload all monitoring data of the device to the cloud platform.

In Cloud View configuration mode, use the following command to cancel specifying the upload type of monitoring data:

no uptype-detect {**all** | **traffic-rank** | **stats-session** | **stats-url-rank** | **stats-device** | **scvpn-user**} | **stats-interface**}

For more information, refer to the **System Management** > **Connecting to Hillstone Cloud Service Platform** topic in *StoneOS_CLI_User_Guide*. FR 35753, FR 39056, FR 39058

Configuring the Data Types Sent to iSource

To configure data types sent to iSource, in iSource configuration mode, use the following command:

upload-type {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**}

- **all** – Specifies to send all types of data to iSource.
- **forensic-pcap** – Specifies to send threat-related evidential packets captured by the device to iSource.
- **iot-monitor-property** – Specifies to send detected IoT asset data to iSource.
- **threat-event** – Specifies to send threat logs to iSource

In iSource configuration mode, use the **no upload-type** {**all** | **forensic-pcap** | **threat-event** | **iot-monitor-property**} command to cancel specifying the data types sent to iSource.

Notes:

- A-series devices that are installed with SSD , K-series devices (except K6580/K9180) that are installed with SSDCloudEdgesupport to upload threat-related evidential packets captured by the device to iSource.

For more information, refer to the **System Management > Connecting to iSource** topic in *StoneOS_CLI_User_Guide*. FR 35753, FR 39056, FR 39058

Support to Retrieve Alarm Messages for OSPF/OSPFv3/BGP Neighbor Status and BFD Session Status Change to DOWN by Using SNMP

MIB

Trap Information Description

Supported private traps for single-device deployment, master device in HA A/P mode, the device on which the interfaces in group0 are in active status in HA A/A mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates that the CPU utilization reaches its threshold (configured in the system monitor).	Excessive CPU utilization may cause problems such as packet loss and network latency. Therefore, troubleshoot the problem in

OID	Severity	Description	Solution
			time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as required.
hillstoneFANStatus			
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.

OID	Severity	Description	Solution
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates that the memory utilization exceeds the configured (through the monitor alarm function) threshold.	Necessary clearance of the memory is needed if the memory utilization is too high.
hillstoneMemoryStatusAlertClear			
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high memory utilization as required.
hillstoneHAStatus			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device failure. Therefore, troubleshoot the problem in time.
hillstoneADType			
1.3.6.1.4.1.28557.3.6	Critical	This notification indicates that the Attack Defend(AD) function is enabled in the Security Zone and the device detects the corresponding attack.	Figure out whether the attack exists in the environment. If yes, take further measures, such as using policy rules or blacklist, to block the attacking traffic.
hillstoneVPNDown			
1.3.6.1.4.1.28557.3.7	Warning	This notification indicates that the IPSec VPN tunnel is disconnected.	1. Check the quality of the physical

OID	Severity	Description	Solution
			links. 2. Confirm the status of the tunnel peer.
hillstoneVPNUp			
1.3.6.1.4.1.28557.3.8	Warning	This notification indicates that the IPSec VPN tunnel is connected.	Troubleshoot the previous dis-connection of the tunnel.
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address changes.	Check whether the interface is dis-connected phys-ically. For example, whether the interface cable is loose.
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of noti-fication alarm. You can ignore or

OID	Severity	Description	Solution
			troubleshoot it according to your conditions.
hillstoneIPSStatus			
1.3.6.1.4.1.28557.3.11	Critical	This notification indicates that IPS is enabled or disabled.	Confirm whether the IPS status is the same as what you have configured.
hillstoneAVStatus			
1.3.6.1.4.1.28557.3.12	Critical	This notification indicates that AV is enabled or disabled.	Confirm whether the AV status is the same as what you have configured.
hillstoneSystemReboot			
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.

OID	Severity	Description	Solution
HillstoneDiskSpaceStatus			
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.
hillstoneSessionOverThreshold			
1.3.6.1.4.1.28557.3.15	Warning	This notification indicates that the Session ratio exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarming Session ratio is normal.
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates	This alarm is

OID	Severity	Description	Solution
		that the using ratio of the Log Buffer exceeds the threshold.	based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log Buffer is normal.
hillstoneIfBandwidthOverThreshold			
1.3.6.1.4.1.28557.3.17	Critical	This notification indicates that the percentage of the interface bandwidth exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarming percentage of the interface bandwidth is normal.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as

OID	Severity	Description	Solution
			required.
hillstonePolicyCountOverThreshold			
1.3.6.1.4.1.28557.3.18	Critical	This notification indicates that the number of the configured policies exceeds the threshold.	You can clean up policies or control the number of subsequent new policies.
hillstoneConfigurationChange			
1.3.6.1.4.1.28557.3.19	Critical	This notification indicates that the configuration changes.	Confirm whether the changed configuration is the same as what you have configured.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates that the slot is offline.	Confirm whether the slot is offline or it is a false alarm.
hillstoneSNATResourceOverThreshold			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.22	Critical	This notification indicates that the using ratio of the SNAT resources reaches the configured (through the monitor alarm function) threshold.	Once SNAT resources are used up, the network connection will fail because subsequent traffic cannot be translated. Therefore troubleshoot this problem in time.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstoneBypassInline			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates that the status of the power module is abnormal.	Malfunction of the power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warn-	Troubleshoot the malfunction of the fans.

OID	Severity	Description	Solution
		ing, or fail.	
hillstoneFANStopClear			
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan status as required.
hillstoneHardDiskSpaceStatus			
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	The Trap host can delete previous alarms of high disk utilization as required.
hillstoneUserLogoutAlarm			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneOSPFDown			
1.3.6.1.4.1.28557.3.61	Critical	The notification indicates that the OSPF neighbor state changes from FULL (adjacency formed) to DOWN (adjacency lost).	Invalid interface configuration, OSPF configuration, or link leads to OSPF neighbor state change. Therefore, troubleshoot the problem in time.
hillstoneOSPFV3Down			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.62	Critical	The notification indicates that the OSPFv3 neighbor state changes from FULL (adjacency formed) to DOWN (adjacency lost).	Invalid interface configuration, OSPFv3 configuration, or link leads to OSPFv3 neighbor state change. Therefore, troubleshoot the problem in time.
hillstoneBGPDown			
1.3.6.1.4.1.28557.3.63	Critical	The message indicates that the BGP neighbor state changes from Established to Idle.	Invalid interface configuration, BGP configuration, or link leads to BGP neighbor state change. Therefore, troubleshoot the problem in time.
hillstoneBFDDown			
1.3.6.1.4.1.28557.3.79	Critical	The notification indicates that the BFD session state	Invalid interface configuration,

OID	Severity	Description	Solution
		changes from UP (link connected) to Idle (link disconnected).	BFD configuration, or link leads to BFD session state change. Therefore, troubleshoot the problem in time.
hillstoneDaemonCrash			
1.3.6.1.4.1.28557.3.76	Emergencies	The notification indicates that system process crashes.	Due to various reasons such as invalid access to system memory or receiving a kill signal, the system process crashes, requiring the process or the whole device to be restarted.
hillstoneDaemonMissheartbeat			
1.3.6.1.4.1.28557.3.77	Critical	The notification indicates that the monitoring process (monitord) detects a heartbeat loss.	The corresponding process is deadlocked or stuck in an

OID	Severity	Description	Solution
			infinite loop, failing to send a heartbeat to the monitoring process (monitord) in a timely manner, requiring the process or the whole device to be restarted.
hillstoneDaemonDeadlock			
1.3.6.1.4.1.28557.3.78	Emergencies	The notification indicates that system process is deadlocked.	Due to two or more processes indefinitely waiting for each other to release resources, they are unable to send a heartbeat to the monitoring process (monitord) for an extended period, causing system processes to lock, requiring

OID	Severity	Description	Solution
			the process or the whole device to be restarted.

Supported private traps for the backup device in HA A/P mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates that the CPU utilization reaches its threshold (configured in the system monitor).	Excessive CPU utilization may cause problems such as packet loss and network latency. Therefore, troubleshoot the problem in time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as required.
hillstoneFANStatus			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates	Necessary clear-

OID	Severity	Description	Solution
		that the memory utilization exceeds the configured (through the monitor alarm function) threshold.	ance of the memory is needed if the memory util-ization is too high.
hillstoneMemoryStatusAlertClear			
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete pre-vious alarms of high memory util-ization as required.
hillstoneHAStatus			
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device fail-ure. Therefore, troubleshoot the problem in time.
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address	Check whether the interface is

OID	Severity	Description	Solution
		changes.	disconnected physically. For example, whether the inter-face cable is loose.
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of notification alarm. You can ignore or troubleshoot it according to your conditions.
hillstoneSystemReboot			
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.
HillstoneDiskSpaceStatus			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates that the using ratio of the Log Buffer exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log Buffer is normal.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.

OID	Severity	Description	Solution
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates that the slot is offline.	Confirm whether the slot is offline or it is a false alarm.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstoneBypassInline			
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have

OID	Severity	Description	Solution
			configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates that the status of the power module is abnormal.	Malfunction of the power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warning, or fail.	Troubleshoot the malfunction of the fans.
hillstoneFANStopClear			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan status as required.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as required.
hillstoneHardDiskSpaceStatus			
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates	The Trap host

OID	Severity	Description	Solution
		that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	can delete previous alarms of high disk utilization as required.
hillstoneUserLogoutAlarm			
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneDaemonCrash			
1.3.6.1.4.1.28557.3.76	Emergencies	The notification indicates that system process crashes.	Due to various reasons such as invalid access to system memory

OID	Severity	Description	Solution
			or receiving a kill signal, the system process crashes, requiring the process or the whole device to be restarted.
hillstoneDaemonMissheartbeat			
1.3.6.1.4.1.28557.3.77	Critical	The notification indicates that the monitoring process (monitord) detects a heartbeat loss.	The corresponding process is deadlocked or stuck in an infinite loop, failing to send a heartbeat to the monitoring process (monitord) in a timely manner, requiring the process or the whole device to be restarted.

OID	Severity	Description	Solution
hillstoneDaemonDeadlock			
1.3.6.1.4.1.28557.3.78	Emergencies	The notification indicates that system process is dead-locked.	Due to two or more processes indefinitely wait-ing for each other to release resources, they are unable to send a heartbeat to the mon-itoring process (monitord) for an extended period, causing system processes to lock, requiring the process or the whole device to be restarted.

Supported private traps for the device on which the interfaces in group1 are in active status in HA A/A Peer mode.

OID	Severity	Description	Solution
hillstoneCPUStatus			
1.3.6.1.4.1.28557.3.1	Critical	This notification indicates	Excessive CPU

OID	Severity	Description	Solution
		that the CPU utilization reaches its threshold (configured in the system monitor).	utilization may cause problems such as packet loss and network latency. Therefore, troubleshoot the problem in time.
hillstoneCPUStatusAlertClear			
1.3.6.1.4.1.28557.3.51	Critical	This notification indicates that the CPU utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high CPU utilization as required.
hillstoneFANStatus			
1.3.6.1.4.1.28557.3.2	Critical	This notification indicates that a single fan is in abnormal statuses, such as absent/warning/fail.	Abnormal status of a single fan may cause poor heat dissipation. Therefore, troubleshoot the problem in time.

OID	Severity	Description	Solution
hillstoneTempStatus			
1.3.6.1.4.1.28557.3.3	Critical	This notification indicates that the device temperature exceeds the configured threshold.	In-time troubleshooting is needed if the device temperature reaches its threshold.
hillstoneTemperatureOverheatClear			
1.3.6.1.4.1.28557.3.50	Critical	This notification indicates that the device temperature returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high device temperature as required.
hillstoneMemoryStatus			
1.3.6.1.4.1.28557.3.4	Critical	This notification indicates that the memory utilization exceeds the configured (through the monitor alarm function) threshold.	Necessary clearance of the memory is needed if the memory utilization is too high.
hillstoneMemoryStatusAlertClear			

OID	Severity	Description	Solution
1.3.6.1.4.1.28557.3.52	Critical	This notification indicates that the memory utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high memory utilization as required.
hillstoneHAStatus			
1.3.6.1.4.1.28557.3.5	Critical	This notification indicates that HA status changes to master/backup/standalone.	The change of the HA status might be caused by a device failure. Therefore, troubleshoot the problem in time.
hillstoneADType			
1.3.6.1.4.1.28557.3.6	Critical	This notification indicates that the Attack Defend(AD) function is enabled in the Security Zone and the device detects the corresponding attack.	Figure out whether the attack exists in the environment. If yes, take further measures, such as using policy rules or blacklist, to block

OID	Severity	Description	Solution
			the attacking traffic.
hillstoneVPNDown			
1.3.6.1.4.1.28557.3.7	Warning	This notification indicates that the IPSec VPN tunnel is disconnected.	1. Check the quality of the physical links. 2. Confirm the status of the tunnel peer.
hillstoneVPNUp			
1.3.6.1.4.1.28557.3.8	Warning	This notification indicates that the IPSec VPN tunnel is connected.	Troubleshoot the previous disconnection of the tunnel.
hillstoneIfIpChange			
1.3.6.1.4.1.28557.3.9	Warning	This notification indicates that the interface address changes.	Check whether the interface is disconnected physically. For

OID	Severity	Description	Solution
			example, whether the interface cable is loose.
hillstoneDeviceNameChange			
1.3.6.1.4.1.28557.3.10	Warning	This notification indicates that the device name changes.	It is a type of notification alarm. You can ignore or troubleshoot it according to your conditions.
hillstoneSystemReboot			
1.3.6.1.4.1.28557.3.13	Critical	This notification indicates that the system reboots.	Figure out why the system reboots, whether it is a manual reboot or because of an abnormal device.
HillstoneDiskSpaceStatus			
1.3.6.1.4.1.28557.3.14	Critical	This notification indicates that the available disk space is insufficient.	It is recommended to free up the disk space in this scenario.

OID	Severity	Description	Solution
hillstoneDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.53	Critical	This notification indicates that the disk space returns to normal.	The Trap host can delete previous alarms of low remaining disk space as required.
hillstoneSessionOverThreshold			
1.3.6.1.4.1.28557.3.15	Warning	This notification indicates that the Session ratio exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarming Session ratio is normal.
hillstoneLog OverThreshold			
1.3.6.1.4.1.28557.3.16	Critical	This notification indicates that the using ratio of the Log Buffer exceeds the threshold.	This alarm is based on your configuration of the threshold. Confirm whether the alarmed using ratio of the Log

OID	Severity	Description	Solution
			Buffer is normal.
hillstonePolicyCountOverThreshold			
1.3.6.1.4.1.28557.3.18	Critical	This notification indicates that the number of the configured policies exceeds the threshold.	You can clean up policies or control the number of subsequent new policies.
hillstoneSlotUp			
1.3.6.1.4.1.28557.3.20	Critical	This notification indicates that the slot is online.	The slot is online.
hillstoneSlotDown			
1.3.6.1.4.1.28557.3.21	Critical	This notification indicates that the slot is offline.	Confirm whether the slot is offline or it is a false alarm.
hillstoneSNATResourceOverThreshold			
1.3.6.1.4.1.28557.3.22	Critical	This notification indicates that the using ratio of the SNAT resources reaches the configured (through the monitor alarm function) threshold.	Once SNAT resources are used up, the network connection will fail because subsequent traffic cannot be trans-

OID	Severity	Description	Solution
			lated. Therefore troubleshoot this problem in time.
hillstoneLoginFailed			
1.3.6.1.4.1.28557.3.23	Warning	This notification indicates that the administrator fails to log in.	It is a type of notification alarm. You can address it according to your conditions.
hillstoneBypassBypass			
1.3.6.1.4.1.28557.3.24	Critical	This notification indicates that the status of the Bypass module is switched to be in Bypass mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstoneBypassInline			
1.3.6.1.4.1.28557.3.25	Critical	This notification indicates that the status of the Bypass module is switched to be in Inline mode.	Confirm whether the Bypass status is the same as what you have configured.
hillstonePowerStatus			
1.3.6.1.4.1.28557.3.37	Critical	This notification indicates	Malfunction of

OID	Severity	Description	Solution
		that the status of the power module is abnormal.	the power module may affect the functions of the device. Therefore, troubleshoot the problem in time.
hillstonePowerErrorClear			
1.3.6.1.4.1.28557.3.49	Critical	This notification indicates that the status of the power module returns to normal.	The Trap host can delete previous alarms of abnormal power module status as required.
hillstoneFanError			
1.3.6.1.4.1.28557.3.38	Critical	This notification indicates that the fan status is abnormal, such as absent, warning, or fail.	Troubleshoot the malfunction of the fans.
hillstoneFANStopClear			
1.3.6.1.4.1.28557.3.48	Critical	This notification indicates that the status of fan as a whole returns to normal.	The Trap host can delete previous alarms of abnormal fan

OID	Severity	Description	Solution
			status as required.
hillstoneBandwidthOverThresholdAlertClear			
1.3.6.1.4.1.28557.3.54	Critical	This notification indicates that the interface bandwidth utilization returns to normal (lower than the threshold).	The Trap host can delete previous alarms of high interface bandwidth utilization as required.
hillstoneHardDiskSpaceStatus			
1.3.6.1.4.1.28557.3.55	Critical	This notification indicates that the disk utilization exceeds the threshold. **Note**: This is supported only by devices installed with SSD.	The disk utilization is too high and needs to be cleaned up.
hillstoneHardDiskSpaceStatusAlertClear			
1.3.6.1.4.1.28557.3.56	Critical	This notification indicates that the disk utilization returns to normal (lower than the threshold). **Note**: This is supported only by devices installed with SSD.	The Trap host can delete previous alarms of high disk utilization as required.

OID	Severity	Description	Solution
hillstoneUserLogoutAlarm			
1.3.6.1.4.1.28557.3.59	Warning	This notification indicates that the number of times that users go offline exceeds the threshold (configured in the going offline alarm function of User) within a specified period of time.	Notify the administrator that there is a situation where a large number of users are offline, and there may be a fault with the L2TP link. Therefore, troubleshoot the problem in time.
hillstoneOSPFDown			
1.3.6.1.4.1.28557.3.61	Critical	The notification indicates that the OSPF neighbor state changes from FULL (adjacency formed) to DOWN (adjacency lost).	Invalid interface configuration, OSPF configuration, or link leads to OSPF neighbor state change. Therefore, troubleshoot the problem in time.

OID	Severity	Description	Solution
hillstoneOSPFV3Down			
1.3.6.1.4.1.28557.3.62	Critical	The notification indicates that the OSPFv3 neighbor state changes from FULL (adjacency formed) to DOWN (adjacency lost).	Invalid interface configuration, OSPFv3 configuration, or link leads to OSPFv3 neighbor state change. Therefore, troubleshoot the problem in time.
hillstoneBGPDown			
1.3.6.1.4.1.28557.3.63	Critical	The message indicates that the BGP neighbor state changes from Established to Idle.	Invalid interface configuration, BGP configuration, or link leads to BGP neighbor state change. Therefore, troubleshoot the problem in time.
hillstoneBFDDown			
1.3.6.1.4.1.28557.3.79	Critical	The notification indicates	Invalid interface

OID	Severity	Description	Solution
		that the BFD session state changes from UP (link connected) to Idle (link disconnected).	configuration, BFD configuration, or link leads to BFD session state change. Therefore, troubleshoot the problem in time.
hillstoneDaemonCrash			
1.3.6.1.4.1.28557.3.76	Emergencies	The notification indicates that system process crashes.	Due to various reasons such as invalid access to system memory or receiving a kill signal, the system process crashes, requiring the process or the whole device to be restarted.
hillstoneDaemonMissheartbeat			
1.3.6.1.4.1.28557.3.77	Critical	The notification indicates that the monitoring process (monitord) detects a heart-	The corresponding process is deadlocked

OID	Severity	Description	Solution
		beat loss.	or stuck in an infinite loop, failing to send a heartbeat to the monitoring process (monitord) in a timely manner, requiring the process or the whole device to be restarted.
hillstoneDaemonDeadlock			
1.3.6.1.4.1.28557.3.78	Emergencies	The notification indicates that system process is deadlocked.	Due to two or more processes indefinitely waiting for each other to release resources, they are unable to send a heartbeat to the monitoring process (monitord) for an extended period, causing system processes

OID	Severity	Description	Solution
			to lock, requiring the process or the whole device to be restarted.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 41151, FR41157

Supporting to Configure SNAT Port Group via WebUI

WebUI

Port Group

By configuring the excluded port rules, you can rule out port or port range. The system will not convert the specified port when the source address is translated.

Notes:

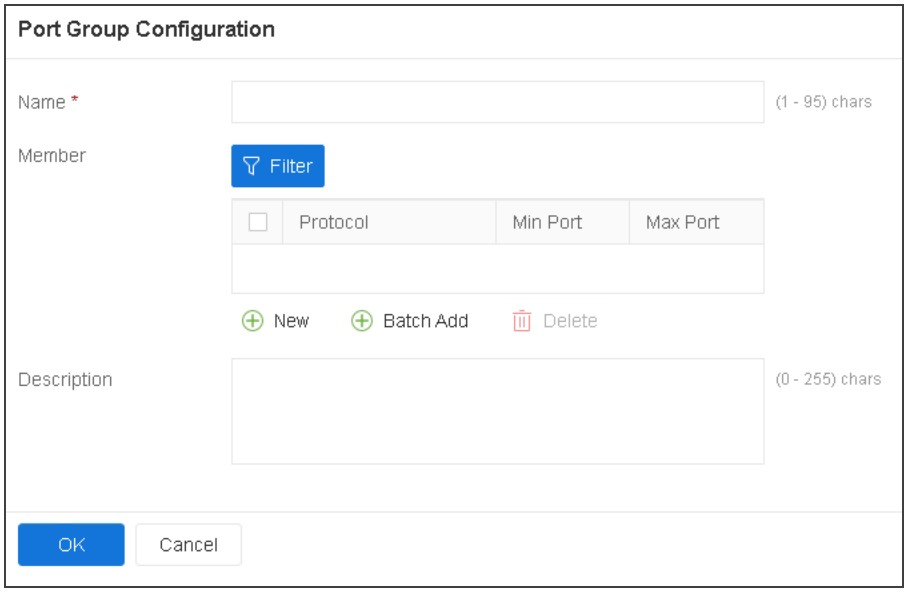
- The device allows you to configure a maximum of 8 port groups, each with up to 512 entries, and each entry can configure up to 16 ports, with a maximum of 512 ports per port group.
- When both SNAT rules and virtual routers bind different exclude port groups, the port group bound to SNAT rule takes higher priority.
- DNAT rules do not support binding exclude port groups. When DNAT source translation is enabled, the exclude port group bound to the virtual router applies to the source translation address of DNAT rules.

To implement the exclude port function of SNAT, take the following steps:

1. Create an SNAT port group.
2. Bind the SNAT port group to a specified VRouter.
3. Bind the SNAT port group to a specified SNAT rule.

Creating an Exclude Port Group

1. Select **Object** > **Port Group**.
2. Click **New**.



Option	Description
Name	Enter the name of the exclude port group.
Member	Specify the members of the exclude port group. • Click **New** and select the port protocol from the drop-down list, and enter the minimum port and maximum port in the fields. The minimum port cannot be greater than the maximum port, and the number of ports cannot exceed 16.

Option	Description

	• Click Batch Add, enter member entries in the <Batch Add Members> panel. Configure one member in each row, separate the protocol, minimum port, and maximum port with ";", and press the Enter key for a new row. For example:
	`TCP;23;25`
	`UDP;26;32`

Description	Enter a description for the exclude port group entry.

3. Click **OK**.

Editing/Deleting an Exclude Port Group

To edit or delete an exclude port group, take the following steps:

1. Select **Object** > **Port Group**.
2. Select the port group that you want to edit or delete from the list.
3. Click **Edit** or **Delete** at the top of the list to edit or delete the port group.

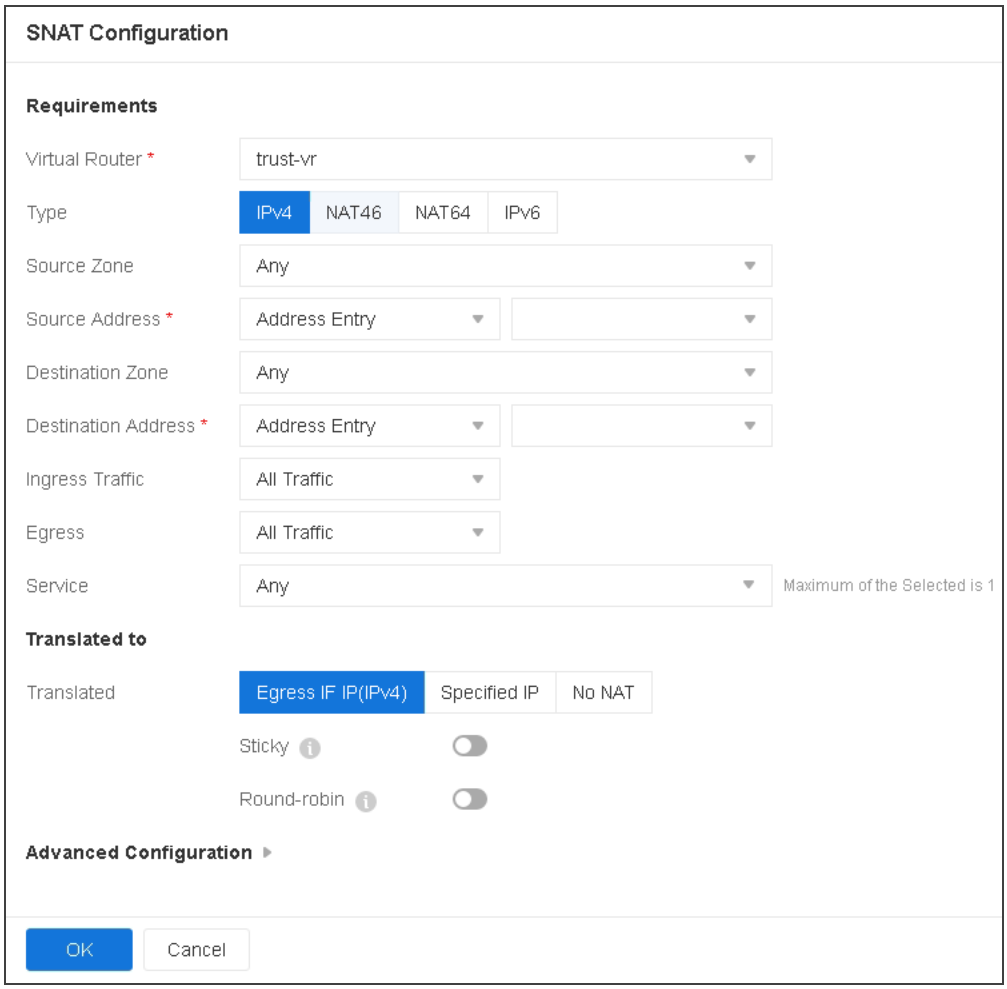
For more information, refer to the **Object** > **Port Group** topic in *StoneOS_WebUI_User_Guide*.
FR38974

Configuring SNAT

To create an SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Click **New** to open the SNAT Configuration page.



In this page, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the SNAT rule. The SNAT rule will take effect when the traffic flows into this VRouter and matches the SNAT rule conditions.
Type	Specifies the type of the SNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types

Requirements	
	of SNAT rules may vary in this page, please refer to the actual page.
Source Zone	Specifies the security zone to which the ingress interface of traffic that matches the SNAT rule is bound. By default, Any is selected. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the SNAT rule. **Note:** The source zone needs to belong to the specified virtual router.
Source Address	Specifies the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the SNAT rule is NAT64 or IPv6.
Destination	Specifies the destination IP address of the traffic, including:

Requirements	
Address	• Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the SNAT rule is NAT64 or IPv6.
Ingress Traffic	Specifies the ingress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the ingress traffic. Traffic from any ingress interfaces will continue to match this SNAT rule. • Ingress Interface - Specifies the ingress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.
Egress	Specifies the egress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the egress traffic. Traffic

Requirements	
	from all egress interfaces will continue to match this SNAT rule. • Egress Interface - Specifies the egress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not. • Next Virtual Router - Specifies the next virtual router of traffic. Select a virtual router from the drop-down list.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **New Service** or **New Group**.
Translated to	
Translated	Specifies the translated NAT IP address, including: • Egress IF IP (IPv4)/Egress IF IP (IPv6) - Specifies the NAT IP address to be an egress interface IP address. • Specified IP - Specifies the NAT IP address to be a specified IP address. After selecting this option, continue to specify the available IP address in the **Address** drop-down list. • No NAT - Do not implement NAT. The translated action for different types of SNAT rules may vary in this page, please refer to the actual page.

Requirements	

Mode	Specifies the translation mode, including:
	• Static - Static mode means one-to-one translation. This mode requires the translated address entry to contain the same number of IP addresses as that of the source address entry.
	• Dynamic IP - Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
	• Dynamic port - Called PAT. Multiple source addresses will be translated to one specified IP address in an address entry.
	  • If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Sticky to enable Sticky.
	  • If Round-robin is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Round-robin to enable Round-robin.
	  • If Sticky and Round-robin are not enabled, the first address in the address entry will be used first; when the port resources of the first address are exhausted, the second address will be used.

Requirements	
	• If Track is enabled, the system will track whether the translated public address is valid, i.e., use the translated address as the source address to track if the destination website or host is accessible. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see Track Object. This function only supports SNAT of IPv4 or NAT64 type, and the translated address should be an IP address or an address in address book, as well as the translation mode is dynamicport mode. The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log. Click the **Enable** button behind Track to enable the function, and select a track object from the drop-down list • NPTv6: Select the NPTv6 mode. NPTv6 (IPv6-to-IPv6 Network Prefix Translation) is described in RFC 6296 and

Requirements	
	used to implement NAT66. When this mode is selected, NPTv6 can translate an inside IPv6 source address prefix to outside IPv6 source prefix in IPv6 packet header. The translation is based on the algorithm described in RFC 6296, which serves as a useful mechanism for implementing address independence. This mode supports a larger number of address translation and reduces resource consumption by using quick address mapping. **Note**: The Sticky function and the Round-robin function are mutually exclusive and cannot be configured at the same time. **Notes:** • The NPTv6 mode is available only when the Type parameter is set to IPv6 and the Translated parameter is set to Specified IP. • The NPTv6 mode requires that both the source address of the traffic and the translated address are either "IPv6/prefix" or address from address book. • If the source address of the traffic and the translated address are "IPv6/prefix", the IPv6 prefix needs to be 8 to 64 in length. • If the source address of the traffic and the translated address are address from address

Requirements	
	book, you can only configure one IPv6 subnet mask member whose subnet mask is 8 to 64 in length.

Expand Advanced Configuration, configure the corresponding options.

Option	Description
HA Group	Specifies the HA group that the SNAT rule belongs to. The default setting is 0.
Exclude Port Group	Select an exclude port group that you want to bind from the drop-down list. After you bind the exclude port group to the specified SNAT rule, this SNAT rule will exclude port numbers specified in the port group. For more information about how to create an exclude port group, see Port Group. **Notes:** The exclude port group bound to SNAT rule has a higher priority than the exclude port group bound to VRouter.
Schedule	Specifies the schedule of the SNAT rule. Select a schedule from the drop-down list. In addition, fuzzy search is supported. To create a schedule, click ⊕.
NAT Log	Click the Enable button to enable the log function for this SNAT rule. The system will generate log information when there is traffic matching this NAT rule. **Note**: If the translated NAT IP address is an egress interface IP address, it is necessary to specify the egress interface of the traffic at the same time in order to generate logging information.
Position	Specifies the position of the rule. Each SNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the

Option	Description
	first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all SNAT rules. • Top - The rule is located at the top of all the rules in the SNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specifies the method you get the rule ID. Each rule has its unique ID. It can be automatically assigned by system or manually assigned by yourself. If you select **Manually assign** , type an ID number into the box behind.
Description	Types the description.

3. Click **OK** to save the settings.

Notes:

- When configuring a static source NAT66 rule, the minimum subnet mask must be 48 bits.

- If the SNAT rule is configured with a source zone or destination zone that is not Any, the zone cannot be deleted.

For more information, refer to the **Policy** > **NAT** > **Configuring SNAT** topic in *StoneOS_WebUI_User_Guide*. FR38974

Virtual Router

- After Multi-Virtual Router is enabled or disabled, system must reboot to make it take effect. After rebooting, system's max concurrent sessions might decrease if the function is enabled, or restore to normal if the function is disabled. For more information about the maximum concurrent sessions, see The Maximum Concurrent Sessions.
- If Multi-Virtual Router is enabled, traffic can traverse up to 3 Virtual Routers, and any traffic that has to traverse more than 3 Virtual Routers will be dropped.

To create a Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Virtual Router**.
2. Click **New**.
3. Type the name into the Virtual Router name box.
4. Click the **Enable** button for Vsys Share to share the Virtual Router between different virtual systems.
5. Select an exclude port group that you want to bind from the Exclude Port Group drop-down list. After the port group is bound to the specified VRouter, SNAT rules of all dynamic ports within the VRouter will exclude port numbers specified in the port group. For more information about how to create an exclude port group, see Port Group.

> **Notes:** The exclude port group bound to SNAT rule has a higher priority than the exclude port group bound to VRouter.

6. Click **OK**.

For more information, refer to the **Network** > **Vritual Router** topic in *StoneOS_WebUI_User_Guide*. FR38974

CLI

Configuring an Excluding Port Rule

By configuring the excluded port rules, you can rule out port or port range. The system will not convert the specified port when the source address is translated.

> **Notes:**
>
> - The device allows you to configure a maximum of 8 port groups, each with up to 512 entries, and each entry can configure up to 16 ports, with a maximum of 512 ports per port group.
> - When both SNAT rules and virtual routers bind different exclude port groups, the port group bound to SNAT rule takes higher priority.
> - DNAT rules do not support binding exclude port groups. When DNAT source translation is enabled, the exclude port group bound to the virtual router applies to the source translation address of DNAT rules.

To configure the excluding port function, take the following steps:

1. Create a SNAT port group.
2. Configure the SNAT port group, and specify the description excluded port number.

3. Bind the SNAT port group to a specified VRouter.

4. Bind the SNAT port group to a specified SNAT rule.

Creating a SNAT Port Group

To create a SNAT port group, in the global configuration mode, use the following command:

snat-port-group*snat-port-group-name*

- *snat-port-group-name* - Specifies the SNAT port group name and enters the SNAT port group configuration mode. If the specified name exists, then the system will directly enter the SNAT port group configuration mode. The name range is 1 to 95 characters.

Notes: System supports at most 8 SNAT port groups.

To delete a SNAT port group, in the global configuration mode, use the following command:

no snat-port-group*snat-port-group-name*

Specifying the Description of SNAT Port Group

To specify the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

description*description*

- *description* – Specifies the description of SNAT port group, the range is 0 to 256 characters.

To delete the description of SNAT port group, in the SNAT port group configuration mode, use the following command:

no description

Specifying the Excluding Port Number

To specify the port range that needs to be excluded, in the SNAT port group configuration mode, use the following command:

port {**TCP** | **UDP**} **min-port***min-port* [**max-port***max-port*]

- **TCP** | **UDP** – Specifies the protocol type of excluded ports.
- **min-port***min-port* [**max-port***max-port*]- Specifies the excluded port number. If the port number is a number range, then *min-port* is the minimum port number, and *max-port*is the maximum port number.

To cancel the above configuration, in the SNAT port group configuration mode, use the following command:

no port {**TCP** | **UDP**} **min-port***min-port* [**max-port***max-port*]

Binding the SNAT Port Group to VRouter

> **Notes:** The exclude port group bound to SNAT rule has a higher priority than the exclude port group bound to VRouter.

After binding the SNAT port group to the specified VRouter, the SNAT rule of all dynamic ports of the VRouter excludes the port number specified in the SNAT port group, in the VRouter configuration mode, use the following command:

snat-exclude-port*snat-port-group-name*

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

no snat-exclude-port

Binding the SNAT Port Group to SNAT Rule

After you bind the SNAT port group to the specified SNAT rule, this SNAT rule will exclude all port numbers specified in the port group.

> **Notes:** The exclude port group bound to SNAT rule has a higher priority than the exclude port group bound to VRouter.

To specify the exclude port group bound to the SNAT rule, in VRouter configuration mode, use the following command:

snatrule id*id***exclude-port***exclude-port-group-name*

- *id* – Specifies the ID of the SNAT rule that you want to bind to the exclude port group.
- *exclude-port-group-name* – Specifies the exclude port group of the SNAT rule.

In VRouter configuration mode, use the following command to cancel the configuration:

no snatrule id*id***exclude-port**

For more information, refer to the **Firewall** > **Configuring a NAT Rule** topic in *StoneOS_CLI_User_Guide*. FR38974

Supporting to Clear Sessions and Display the TCP Status on the Session Details Page

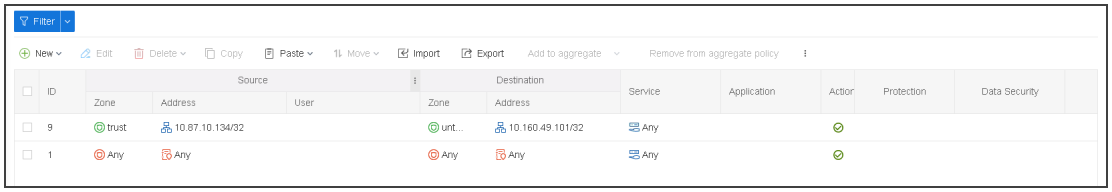
WebUI

Viewing and Searching Security Policy Rules/ Policy Groups/ Mini Policy

You can view and search the policy rules or policy groups in the policy/ policy group/ mini Policy list.

Viewing the Policy/ Policy Group/ Mini Policy

View the security policy rules in the policy rule list.



- Each column displays the corresponding configurations.
- Click  icon under the Session Detail column in the Policy list to open then the **Session Detail** page. You can view the current session status of the selected policy.
    - You can also click 

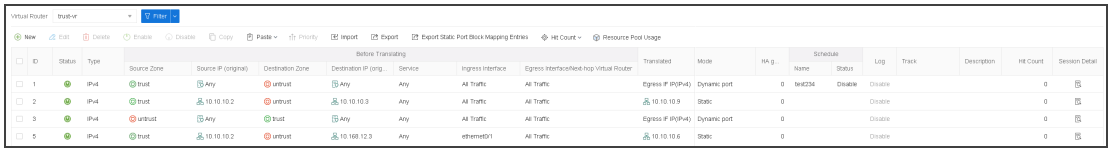
button to add filtering conditions and search out the filtered sessions.
    - The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. You can select Long Session to view the status of persistent sessions. For more information, see Session Timeout.
    - Select one or more sessions and click **Clear** to clear them. You can select at most all sessions on the current page and clear them.
- Hover over your mouse on the configuration in a certain column. Then based on the configuration type, the WebUI displays either icon or the detailed configurations.
    - You can view the detailed configurations directly.
    - You can click icon. Based on the configuration type, the WebUI displays **Add Filter** or **Details**.
        - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.
        - Click **Add Filter**, the filter condition of the configuration you are hovering over with your mouse appears on the top of the list, and then you can filter the policy according to the filter condition. For detailed information of filtering policy rules, see Searching Security Policy Rules/ Policy Groups.

For more information, refer to the **Policy** > **Security Policy** topic in *StoneOS_WebUI_User_Guide*. FR 33389

Viewing and Searching SNAT Rules

You can view and search the SNAT rules on the SNAT rule list.

View the SNAT rules on the SNAT rule list.



- Each column displays the corresponding configurations. The **Schedule** column displays the name and status of SNAT rules. If **Disable** is displayed, it indicates that the SNAT rule does not take effect or has expired.
- Click icon in the Session Detail column on the SNAT rule list to go to the **Session Detail** page. You can view the current session status of the selected SNAT rule. You can also click Filter to add filtering conditions and search for the sessions that conform to the filtering conditions.
  - You can filter **Session ID**, **Source Address**, **Source Port**, **Destination Address**, **Destination Port**, **Protocol**, **Application**, **Flow0 Interface**, **Flow1 Interface**, and **Slot**. You can add multiple filter conditions at the same time. The relationship between filter conditions is **And**.
  - Select one or more sessions and click **Clear** to clear them. You can select at most all sessions on the current page and clear them.
- Hover over your mouse over the configurations in different columns, then the WebUI displays either icon or the detailed information of this configuration based on the configuration type.

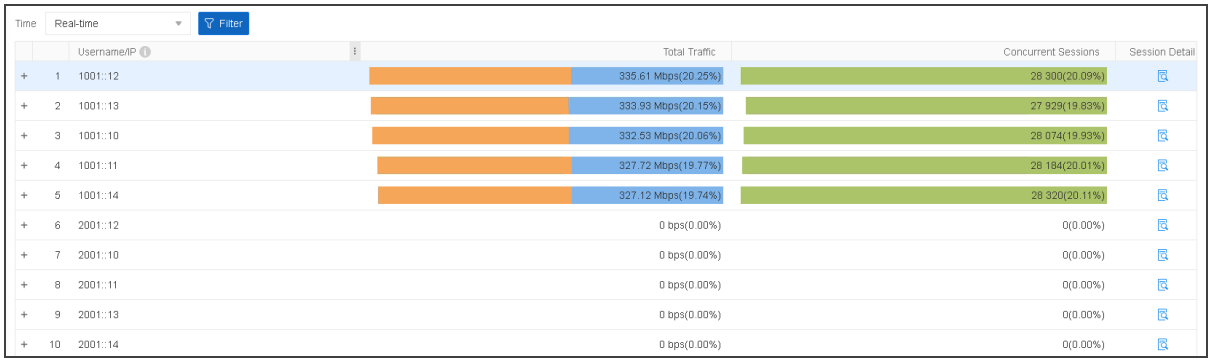
- You can view the detailed configurations directly.
- You can click ⋮ icon. Based on the configuration type, the WebUI displays **Filter**, **Add Filter**, or **Details**.
  - Click **Filter** or **Add Filter**, you can see the filter conditions of this configuration above the list, and then you can filter the SNAT rule according to the filter conditions.
  - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.

For more information, refer to the **Policy** > **NAT** > **Configuring SNAT** topic in *StoneOS_WebUI_User_Guide*. FR 33389

User Monitor

User Details

Click **Monitor** > **User Monitor**> **User Details**.



- Click Filter to select the condition in the drop-down list to search the desired users.
- To view the detailed information of a certain user , select the user entry in the list, and click "+".

- Application (real-time): Select the Application(real-time)tab and display the detailed information of the category, subcategory, risk level, technology, upstream traffic, downstream traffic, total traffic. Click **Details** in the list to view the line chart.
- Cloud Application (real-time): Select the Cloud Application tab to display the cloud application information of selected user.
- URL (real-time): Select the URL tab to display the URL hit count of selected user.
- URL Category (real-time) : Select the URL Category tab to display the URL category hit count of selected user.
- Traffic: Select the Traffic tab to display the traffic trends of selected user .
- Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of selected user .

- Within the user entry list, hover your cursor over a user entry, and there is a button to its right. Click this button and select **Add to Black List**.
- Select an user item in the user list, and click the button in the Session Detail column to open the <Session Detail> page and check all the session details of the selected user.
  - Click Filter to select the condition in the drop-down list to search the desired sessions.
  - Select one or more sessions and click **Clear** to clear them. You can select at most all sessions on the current page and clear them.

For more information, refer to the **Monitor** > **User Monitor** topic in *StoneOS_WebUI_User_Guide*. FR 33389

Supporting AD Script to be Used Together with SSO Monitor

CLI

SSO Monitor for SSO

Kicking Out AD-Script Logged-In Users

The system supports to combine the AD-Script function with the SSO Monitor function to achieve faster response. First, use AD-Script for SSO to log in and provide users with basic internet access permissions. Meanwhile, use the SSO Monitor function to provide more precise internet access permissions. In AD-Scripting configuration mode, use the following command to kick out AD-Script logged-in users after SSO Monitor users log in:

kickout-by sso-monitor

By default, AD-Script logged-in users cannot be kicked out. To restore the default setting, use the following command in AD-Scripting configuration mode:

no kickout-by sso-monitor

For more information, refer to the **User Authentication** > **User Identification** > **Single Sign-On** topic in *StoneOS_CLI_User_Guide*. FR40651

Example of Configuring AD Scripting for SSO

This section describes a typical AD Scripting example. After the configuration, you can be authenticated by the device if only you have been authenticated by the Active Directory server.

The following steps only describe configurations related to AAA Server and AD Scripting, and omit other configurations.

Step 1: Configure an AAA server of Active-Directory type

```
hostname(config)# aaa-server ad type active-directroy
hostname(config-aaa-server)# host 1.1.1.1
hostname(config-aaa-server)# base-dn dc=hillstonenet
```

```
hostname(config-aaa-server)# login-dn cn=user,dc=hillstonenet
hostname(config-aaa-server)# login-password admin
hostname(config-aaa-server)# exit
hostname(config)#
```

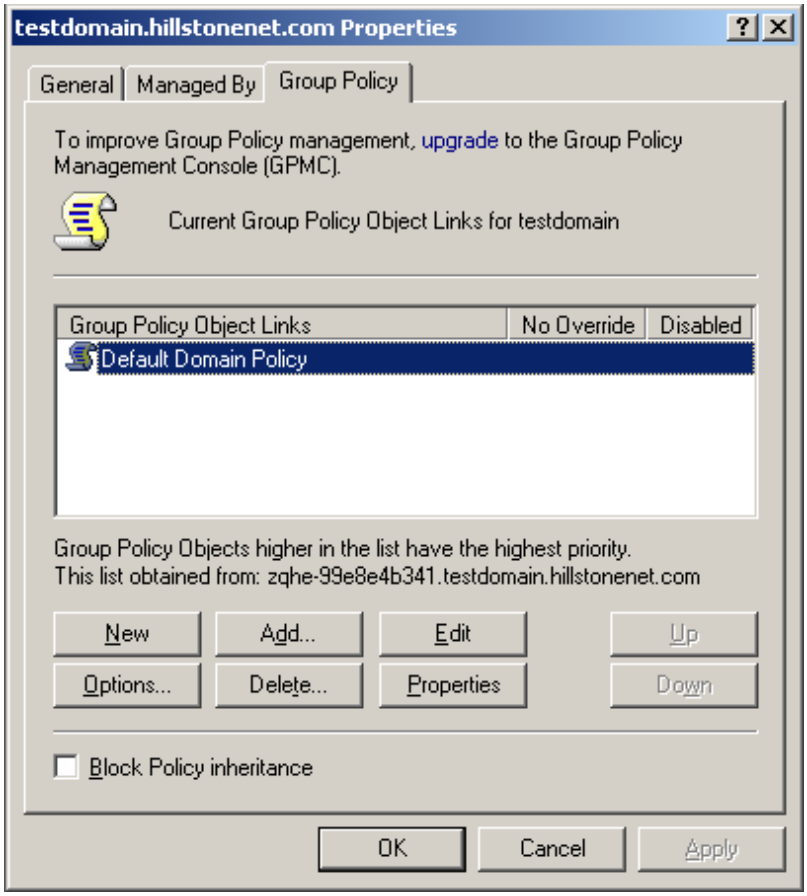
Step 2: Configure the AD Scripting

```
hostname(config)# user-sso server ad-scripting default
hostname(config-ad-scripting)# enable
hostname(config-ad-scripting)# aaa-server ad
hostname(config-ad-scripting)# exit
hostname(config)#
```

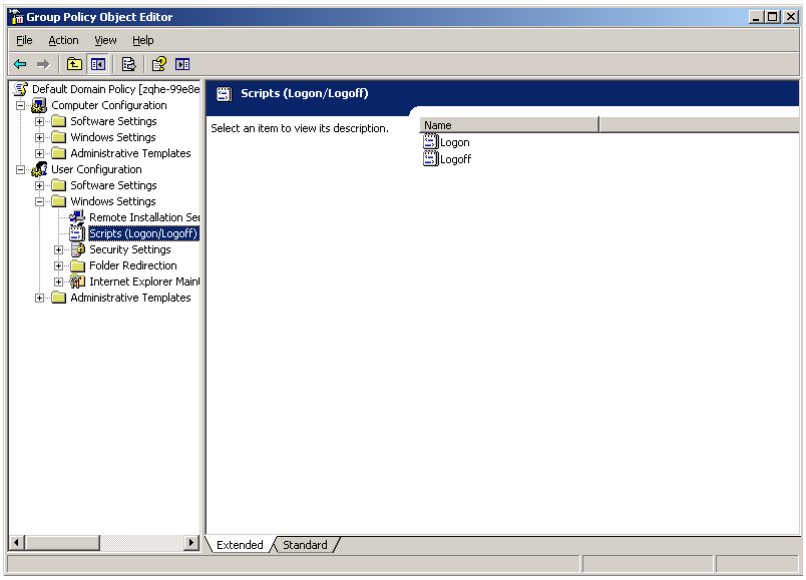
Step 3: In the Active-Directory server, import the logon/logout script

1. On the <AD Scripting> tab of the AD Agent software, click **Get AD Scripting** to get the script "Logonscript.exe", "adscripting-startup.bat", and "adscripting-dispatch.bat"), and save it under a directory where all AD server users can access .
2. In AD server, go to Start menu, select **Mangement Tools> Active Directory User and Computer**.

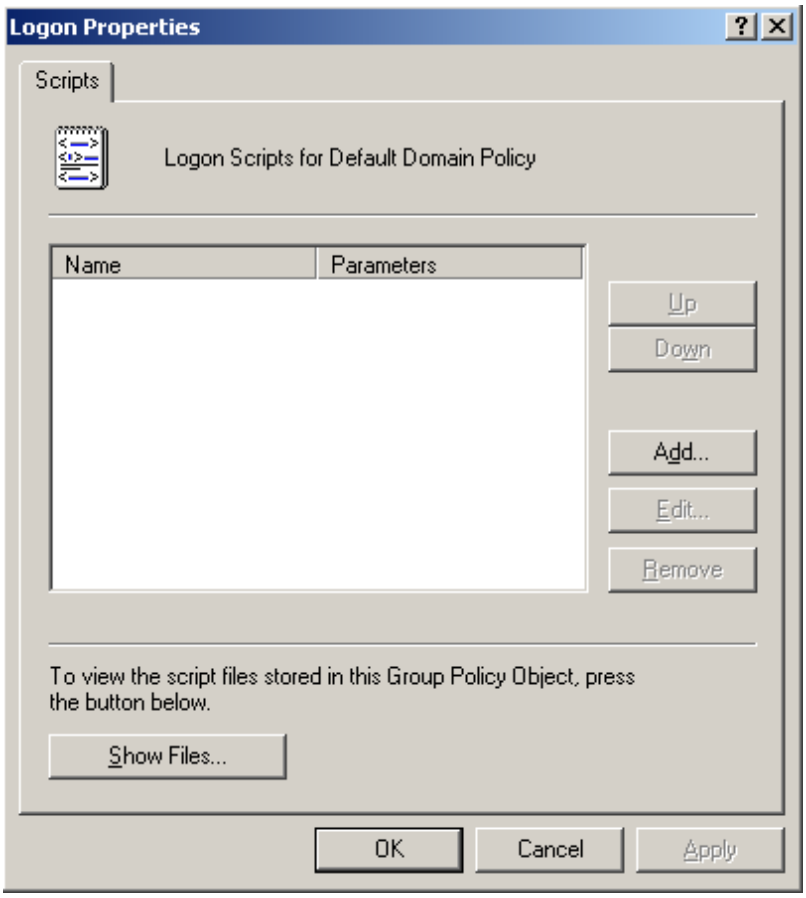
3. In the prompt, right click the domain of SSO, and select **Properties**, then click <Group Policy> tab.



4. Double click the group policy of SSO, and in the prompt, select **User Configuration>Windows>Script (Logon/Logout)**.



5. Double click **Logon** on the right, and click **Add** in the prompt.



6. In the **Add a Script** dialog box, click **Browse** and select a script:

   - When you select "Logonscript.exe", enter *ip-adddress***logon** in the Script Parameter field. *ip-adddress* is used to specify the IP address of the authentication interface of StoneOS, which can send login requests to multiple devices. You can configure up to 20 IP addresses. Multiple IP addresses need to be separated by ",".

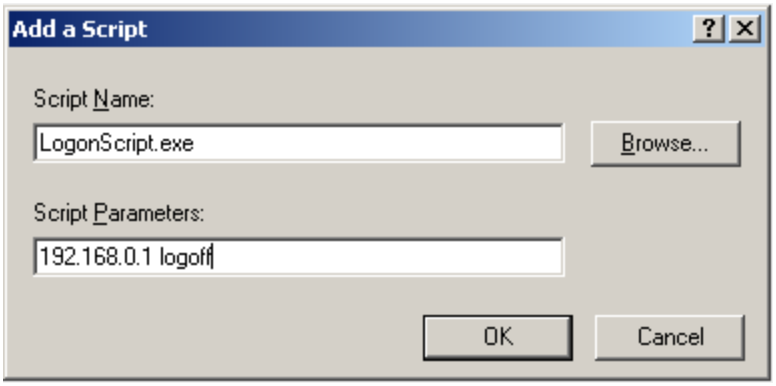
   - When you select "Logonscript.exe", enter *ip-adddress***logon daemon** [**cycle***cycle-times*] in the Script Parameter field. **daemon** indicates that user IP changes can be tracked. **cycle***cycle-times* is used to specify the track interval for user IP changes, which ranges from 1 to 300 seconds and defaults to 5 seconds.

- When you select "adscripting-dispatch.bat", modify the *ip-adddress*logon daemon [cycle*cycle-times*] parameter in "adscripting-startup.bat".

If there are a large number of clients, we recommend that you use "adscripting-dispatch.bat"; If there are a small number of clients, we recommend that you use "Logonscript.exe".

7. Click **OK**.

8. Similarly, import the script into the logout setting. In the **Add a Script** dialog box, click **Browse** and select the script (Logonscript.exe). In the Script Parameter field, enter *ip-adddress*logoff. You can configure up to 20 IP addresses. Multiple IP addresses need to be separated by ",".



Notes: The directory of saving the script must be accessible to all domain users, otherwise, when a user who does not have access will not trigger the script when he logs in or out.

For more information, refer to the **User Authentication** > **User Identification** > **Example of Configuring SSO** topic in *StoneOS_CLI_User_Guide*. FR40651

WebUI

AD Scripting for SSO

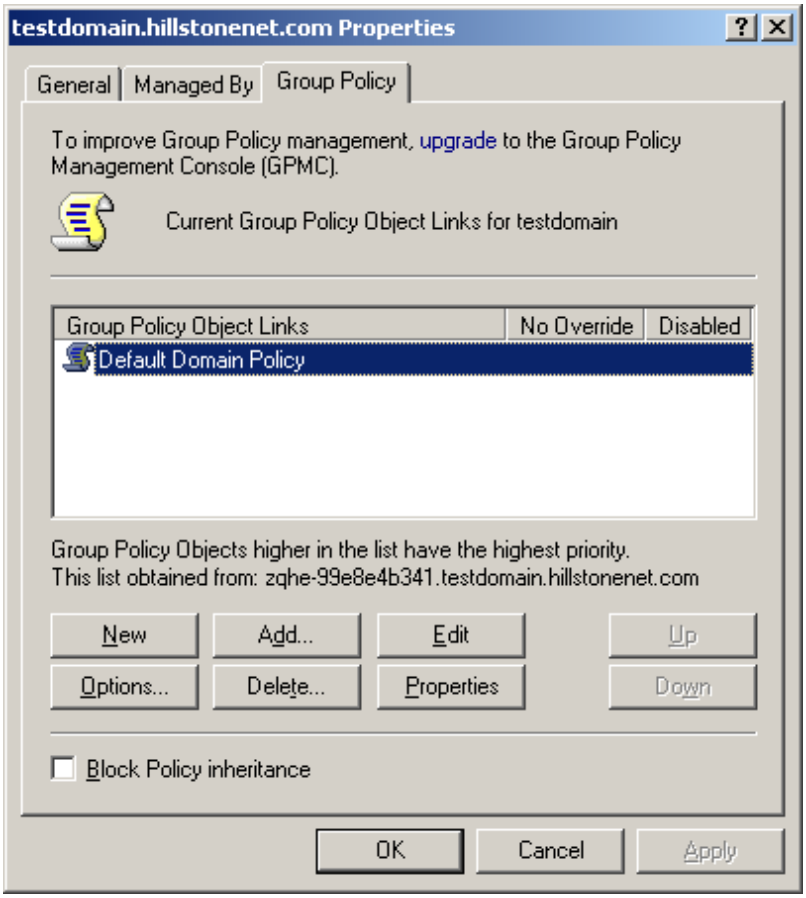
Before using a script for SSO, make sure you have established your Active Directory server first. To use a script for SSO, take the following steps:

Step 1: Configuring the Script for AD Server

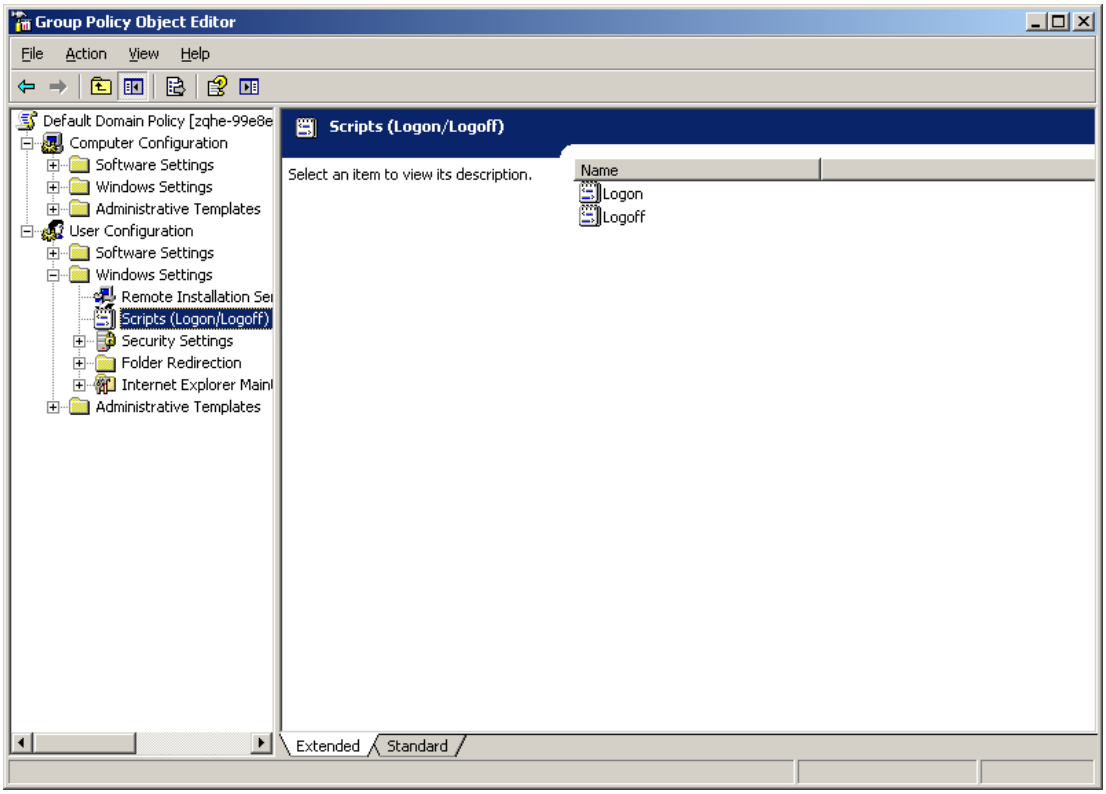
1. Open the AD Security Agent software(for detailed information of the software, see Using AD Agent Software for SSO. On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe", "adscripting-startup.bat", and "adscripting-dispatch.bat"), and save it under a directory where all AD server users can access.

2. In the AD server, enter **Start** menu, and select **Mangement Tools > Active Directory User and Computer**.

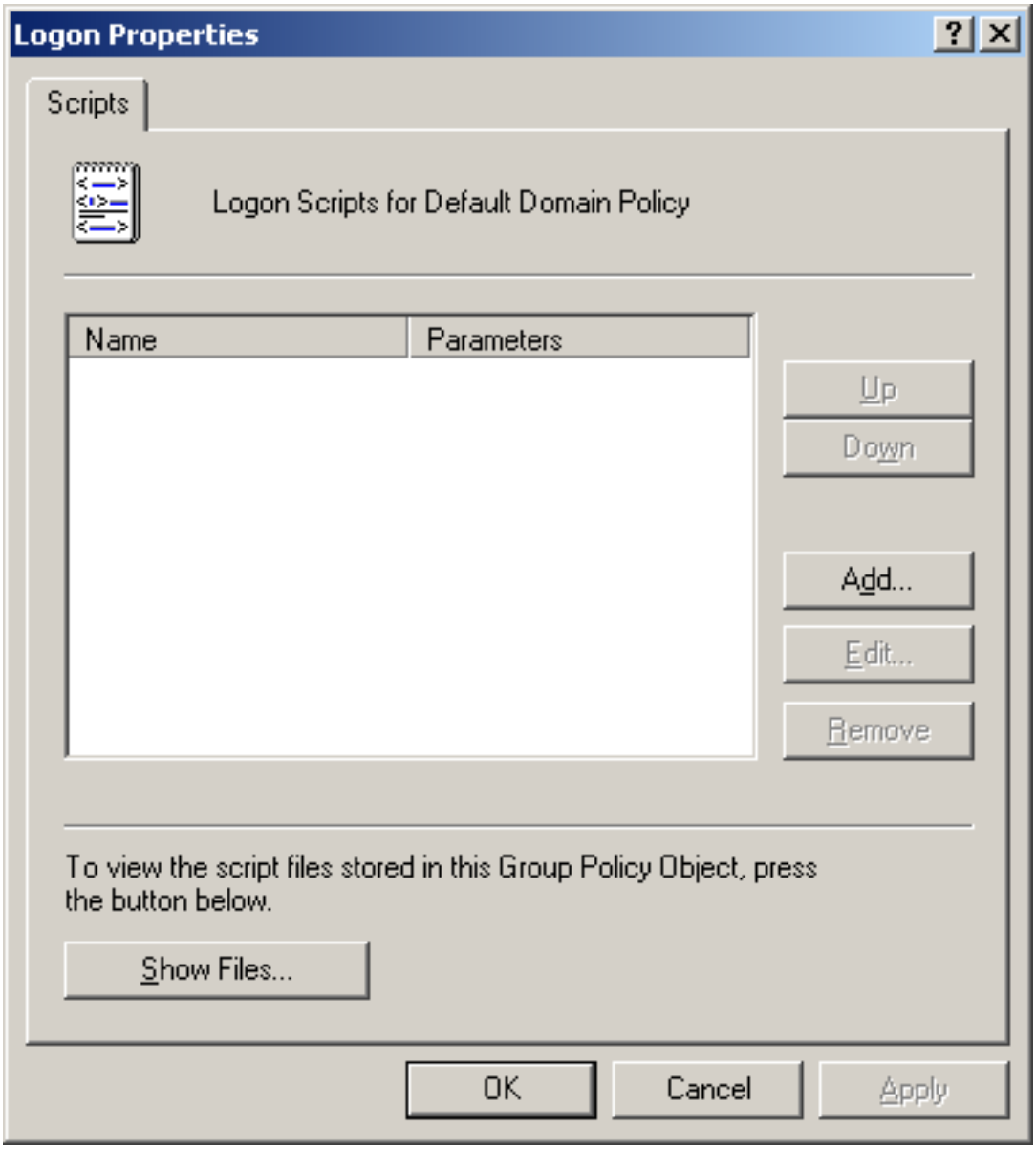
3. In the pop-up <Active Directory User and Computer> dialog box, right-click the domain which will apply SSO to select **Properties**, and then click <Group Policy> tab.



4. In the Group Policy list, double-click the group policy which will apply SSO. In the pop-up <Group Policy Object Editor>dialog box, select **User Configuration > Windows Settings> Script (Logon/Logout)**.



5. Double-click **Logon** on the right window, and click **Add** in the pop-up <logon properties> dialog box.



6. In the **Add a Script** dialog box, click **Browse** and select a script:

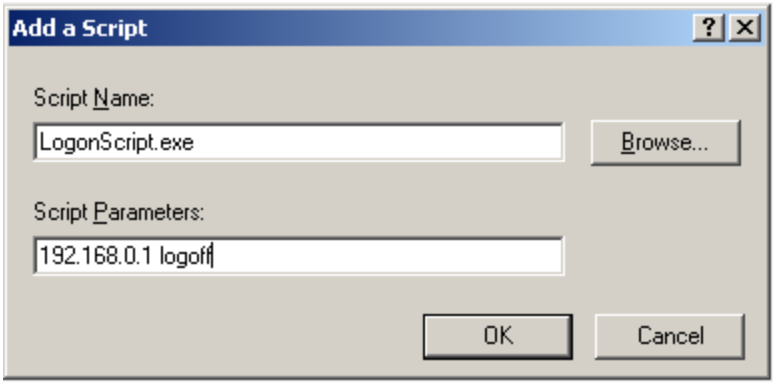
   - When you select "Logonscript.exe", enter *ip-adddress***logon** in the Script Parameter field. *ip-adddress* is used to specify the IP address of the authentication interface of

StoneOS, which can send login requests to multiple devices. You can configure up to 20 IP addresses. Multiple IP addresses need to be separated by ",".

- When you select "Logonscript.exe", enter *ip-adddress***logon daemon** [**cycle***cycle-times*] in the Script Parameter field. **daemon** indicates that user IP changes can be tracked. **cycle***cycle-times* is used to specify the track interval for user IP changes, which ranges from 1 to 300 seconds and defaults to 5 seconds.
- When you select "adscripting-dispatch.bat", modify the *ip-adddress***logon daemon** [**cycle***cycle-times*] parameter in "adscripting-startup.bat".

If there are a large number of clients, we recommend that you use "adscripting-dispatch.bat"; If there are a small number of clients, we recommend that you use "Logonscript.exe".

7. Similarly, import the script into the logout setting. In the **Add a Script** dialog box, click **Browse** and select the script (Logonscript.exe). In the Script Parameter field, enter *ip-adddress***logoff**. You can configure up to 20 IP addresses. Multiple IP addresses need to be separated by ",".



Notes: The directory of saving the script should be accessible to all domain users, otherwise, when a user who does not have privilege will not trigger the script when logs in or out.

Step 2: Configuring AD Scripting for StoneOS

After the AD Scripting is enabled, the user can log in Hillstone device simultaneously when logging in the AD server successfully. System only supports AD Scripting of Active Directory server.

To configure the AD Scripting function, take the following steps:

1. Click **Object> SSO Server > AD Scripting** to enter the AD Scripting page. The AD Scripting function is disabled by default.



2. Select the **Enable** button of AD Scripting to enable the function.
3. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
4. Specify the Idle Interval, which specifies the longest time that the authentication user can keep online without any traffic. After the interval timeout, StoneOS will delete the user authentication information. The value range is 0 to 1440 minutes. 0 means always online.
5. Allow or disable users with the same name to log in depends on needs.
    - **Enable** : Click to permit the user with the same name to log in from multiple terminals simultaneously.

- **Disable**: Click to permit only one user with the same name to log in, and the user logged in will be kicked out by the user logging in.

6. Click **Apply** to save the changes.

After completing the above two steps, the script can send the user information to StoneOS in real time. When users log in or out, the script will be triggered and send the user behavior to StoneOS.

For more information, refer to the **User Authentication** > **Single Sign-On** topic in *StoneOS_WebUI_User_Guide*. FR40651

Obtaining the System-Wide Power Consumption by Using SNMP

MIB

HILLSTONE-POWER-MIB

The following tables is the parsing results of HILLSTONE-POWER-MIB.

Name	OID	Value
hillstonePowerNumber	.1.3.6.1.4.1.28557.2.27.1.1	Data type: Integer32 Description: Total power supply number in the system
hillstonePowerTable: Power supply information		
hillstonePowerIndex	.1.3.6.1.4.1.28557.2.27.1.2.1.1	Data type: Integer Description: Power supply index
hillstonePowerDescr	.1.3.6.1.4.1.28557.2.27.1.2.1.2	Data type: String Description: Power supply description

Name	OID	Value
hillstonePowerState	.1.3.6.1.4.1.28557.2.27.1.2.1.3	Data type: Integer Description: Power supply status • 0 - Good • 1 - Not installed • 2 - Warning • 3 - Failure • 4 - Failure or powered off • 5 - System does not support obtaining power supply status
hillstoneInputPower	.1.3.6.1.4.1.28557.2.27.1.3.0	Date type: DisplayString Description: System-wide power consumption

For more information, refer to *StoneOS SNMP Private MIB Reference Guide*. FR 41735

Viewing the PN of the Power/Fan/Transceiver Module

CLI

Viewing the Information of Transceiver Module

To view the information of transceiver module, including serial number, power, temperature, voltage, module type, wavelength and max transmission distance. In any in any mode, use the following commands:

show transceiver [*interface-name*]

- *interface-name* – Specifies the interface name of transceiver module.

Example:

```
SG-6000# show transceiver
Transceiver status information is shown as below:
================ xethernet0/6 ======================
SFP+/XFP information: FINISARCORP / 111230
Part Number:  FTLF8519P2BNL (Displays the PN of the transceiver module.)
Serial Number: PLT4PH9  (Displays the serial number of the transceiver module.)
Transmission media: Multi-mode  (Displays the transmission mode of the transceiver module, including Single-mode and Multi-mode.)
Module temperature: 32.38  (Displays the current temperature of the transceiver module.)
Module temperature warning range:[-30.00 , 93.00 ]  (Displays the temperature range of the transceiver module.)
Tx supply voltage: 3.34 V  (Displays the transmit supply voltage of the transceiver module.)
Tx supply voltage warning range:[ 2.90 , 3.70 ]  (Displays the transmit supply voltage range of the transceiver module.)
```

Tx bias current: 5.59 mA (Displays the transmit bias current of the transceiver module.)

Tx bias current warning range:[2.00 , 14.00] (Displays the transmit bias current range of the transceiver module.)

Tx optical power: -5.55 dBm (Displays the transmit power of the transceiver module.)

Tx optical power warning range:[-11.00 ,-2.00] (Displays the transmit power range of the transceiver module.)

Rx optical power: -6.69 dBm (Displays the receive power of the transceiver module.)

Rx optical power warning range:[-18.01 , -1.00] (Displays the receive power range of the transceiver module.)

Module Wavelength: 850.00 nm (Displays the wavelength of the transceiver module.)

single module max transmit distance: 0 km (Display the max transmission distance of single mode.)

OM1 max transmit distance: 150 m (Display the max transmission distance of OM1 fiber.)

OM2 max transmit distance: 300 m (Display the max transmission distance of OM2 fiber.)

OM3 max transmit distance: 0 m (Display the max transmission distance of OM3 fiber.)

copper max transmit distance: 0 m (Displays the max transmission distance of the copper cable.)

==========

For more information, refer to **System Management** in *StoneOS_CLI_User_Guide*. FR 41747

Supporting to Aggregate Session Logs by Source/Destination IP Address

WebUI

Session Log

Session logs can be generated under the conditions that:

- Session logging in the Logging feature is enabled. Refer to Managing Logs.
- The logging function has been enabled for policy rules. Refer to Security Policy.

To view session logs, select **Monitor > Log > Session log**.



- Click Filter to specify filter conditions. The session logs that meet the filter conditions are displayed in the list.
  - Time - Displays session logs within the specified time range (last 60 minutes, last 24 hours, last 7 days, last 30 days, and custom). By default, last 24 hours is selected.
  - Policy ID - Displays session logs of policy rule of the specified ID.
  - Source IP - Displays session logs of the specified source IP address.
  - AAA: user@host - Displays session logs of user of the specified AAA server.
  - Source Port - Displays session logs of the specified source port.
  - Destination IP - Displays session logs of the specified destination IP address.

- Destination Port - Displays session logs of the specified destination port.
- Protocol - Displays session logs of the specified protocol.
- Action - Displays session logs of the specified action.
- Application - Displays session logs of the specified application.
- Source Interface - Displays session logs of the specified source interface.
- Destination Interface - Displays session logs of the specified destination interface.
- Close Reason - Displays session logs of the specified termination reason.

- Configure: Click this button to configure session logs.
- Aggregate Type: Select an aggregate type from the drop-down list, including Do Not Aggregate, Threat Name, Source IP, and Destination IP.
- Clear: Click this button to clear all session logs stored in the system. (Note: The **Clear** option is not supported for devices that support sending log information to the local database.)
- Export: Export all session logs stored in the system or filtered results (filter first, and then export) as a TXT or CSV file. You can add an encryption password to the exported file so that the users need to enter the password to view the file.

Notes:

- For ICMP session logs, the system will only record the ICMP type value and its code value. As ICMP 3, 4, 5, 11 and 12 are generated by other communications, not a complete ICMP session, system will not record such kind of packets.
- For TCP and UDP session logs, system will check the packet length first. If the packet length is 20 bytes (i.e., with IP header, but no loads), it will be defined as

a malformed packet and be dropped; if a packet is over 20 bytes, but it has errors, system will drop it either. So, such abnormal TCP and UDP packets will not be recorded.

- Specify the number of session logs to be displayed: Select a number from the **Data Limit** drop-down list to specify the number of session logs that meet the filter conditions. Valid values: 1000, 10000, 50000, and 100000. Default value: 1000.

For more information, see the **Monitor** > **Log** > **Session Log** topic in *StoneOS_WebUI_User_Guide*. FR 41773

Supporting to View Hit Statistics of NAT Rule by Using SNMP

MIB

HILLSTONE-NAT-MIB

The following tables is the parsing results of HILLSTONE-NAT-MIB.

Name	OID	Value
hillstoneSnatRuleId	.1.3.6.1.4.1.28557.2.33.1.1.1.1.1	Data type: Unsigned32 Description: SNAT Resource Index
hillstoneSnatTotalTcpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.2	Data type: Unsigned32 Description: Total TCP

Name	OID	Value
		resource
hillstoneSnatUsedTcpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.3	Data type: Unsigned32 Description: Used TCP resource
hillstoneSnatTotalUdpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.4	Data type: Unsigned32 Description: Total UDP resource
hillstoneSnatUsedUdpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.5	Data type: Unsigned32 Description: Used UDP resource
hillstoneSnatTotalIcmpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.6	Data type: Unsigned32 Description: Total ICMP resource
hillstoneSnatUsedIcmpResource	.1.3.6.1.4.1.28557.2.33.1.1.1.1.7	Data type: Unsigned32 Description: Used ICMP resource

Name	OID	Value
hillstoneSnatHitinfoTable: SNAT rule hit information		
hillstoneSnatRuleId	.1.3.6.1.4.1.28557.2.33.1.1.2.1.1	Data type: Integer Description: SNAT rule ID
hillstoneSnatHitCount	.1.3.6.1.4.1.28557.2.33.1.1.2.1.2	Data type: Integer Description: The number of hits of SNAT rules
hillstoneSnatFirstHitTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.3	Data type: Octet String Description: The time when the SNAT rule was first hit
hillstoneSnatLastHitTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.4	Data type: Octet String Description: The time when the SNAT rule was last hit
hillstoneSnatCreateTime	.1.3.6.1.4.1.28557.2.33.1.1.2.1.5	Data type: Octet String

Name	OID	Value
		Description: The time when the SNAT rule was created
hillstoneDnatServerTable: DNAT server information		
hillstoneDnatServerIndex	.1.3.6.1.4.1.28557.2.33.1.2.1.1.1	Data type: Integer Description: SLB server index
hillstoneDnatServerIPAndPort	.1.3.6.1.4.1.28557.2.33.1.2.1.1.2	Data type: DisplayString Description: IP address and port information of SLB server
hillstoneDnatServerName	.1.3.6.1.4.1.28557.2.33.1.2.1.1.3	Data type: DisplayString Description: VRouter of SLB server
hillstoneDnatServerConnectionNum	.1.3.6.1.4.1.28557.2.33.1.2.1.1.4	Data type: Integer Description: Connection number

Name	OID	Value
		of SLB server
hillstoneDnatServerStatus	.1.3.6.1.4.1.28557.2.33.1.2.1.1.5	Data type: Integer Description: Status of SLB server • 0 - Unknown • 1 - OK • 2 - Failed • 3 - Full load
hillstoneDnatServerGroup	.1.3.6.1.4.1.28557.2.33.1.2.1.1.6	Data type: Integer Description: HA group of SLB server
hillstoneDnatHitinfoTable: DNAT rule hit information		
hillstoneDnatRuleId	.1.3.6.1.4.1.28557.2.33.1.2.2.1.1	Data type: Integer Description: DNAT rule ID

Name	OID	Value
hillstoneDnatHitCount	.1.3.6.1.4.1.28557.2.33.1.2.2.1.2	Date type: Integer Description: The number of hits of DNAT rules
HillstoneDnatFirstHitTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.3	Date type: Octet String Description: The time when the DNAT rule was first hit
HillstoneDnatLastHitTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.4	Date type: Octet String Description: The time when the DNAT rule was last hit
hillstoneDnatCreateTime	.1.3.6.1.4.1.28557.2.33.1.2.2.1.5	Date type: Octet String Description: The time when the DNAT rule was created

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 29630

Supporting to Enable/Disable the Function of Using External IP on FTP Server to Establish Data Connection

WebUI

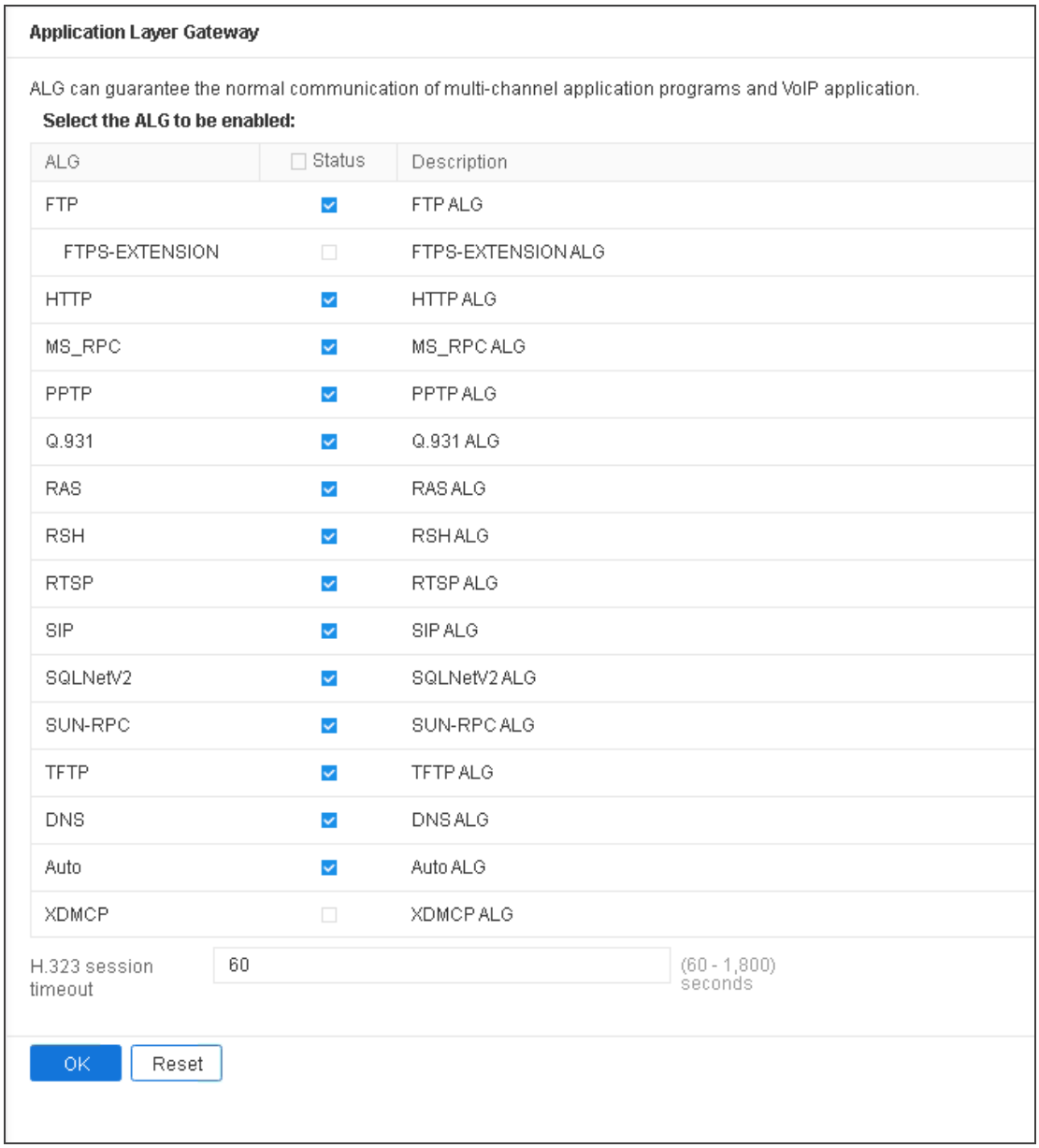
Enabling ALG

The system allows you to enable or disable ALG for different applications. Devices support ALG for the following applications: FTP, HTTP, MSRPC, PPTP, Q.931, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, TFTP, DNS, Auto and XDMCP. You can not only enable ALG for applications, but also specify H323's session timeout.

To enable the ALG for applications, take the following steps:

1. Select **Network> Application Layer Gateway**.

2. In the Application Layer Gateway dialog, select the applications that require ALG.



3. To modify H323's session timeout, type the value into the **H323 session timeout** box. The value range is 60 to 1800 seconds. The default value is 60.

4. Click **OK** to save your changes.

Notes: Only when the FTP ALG is enabled can the FTPS ALG be selected. When FTP ALG is enabled, you can enable FTPS ALG and use the external IP address on the server to establish the data connection function.

Enable/Disable the Function of Using External IP on FTP Server to Establish Data Connection

In certain business scenarios, if there is a device that supports NAT but does not support ALG between the FTP server and the firewall, and the transmission mode of the FTP server is the passive mode, the device that does not support ALG cannot modify the application layer IP after performing NAT translation at the network layer. This results in that the firewall cannot establish FTP data sessions, leading to the FTP data communication and processing issue. To address this issue, the system supports to enable or disable the use of the server's external IP to establish data connection. By default, this function is disabled.

To enable/disable using the external IP address on the FTP server to establish data connection, take the following steps:

1. Select **Network** > **Application Layer Gateway**.
2. Select FTP ALG to enable this function. After this function is enabled, the "EXTERNAL-IP-ON-SERVER" option is displayed below.
3. Select/Unselect "EXTERNAL-IP-ON-SERVER" to enable the function of using external IP address on FTP server to establish data connection.

Notes: This function can take effect only when the transmission mode of the FTP server is the passive mode.

For more information, refer to the **Network** > **Application Layer Gateway (ALG)** topic in *StoneOS_WebUI_User_Guide*. FR 35041

CLI

Enabling/Disabling the ALG FTPS funtion

To enable or disable the ALG FTPS function, in global configuration mode, use the following command:

Enable: **alg ftp ftps-extension**

Disable: **no alg ftp ftps-extension**

> **Notes:** Before you enable this function, make sure that the FTP ALG function is enabled.
>
> For more information, see Enabling/Disabling the ALG Control Function for Applications.

Enable/Disable the Function of Using External IP on FTP Server to Establish Data Connection

In certain business scenarios, if there is a device that supports NAT but does not support ALG between the FTP server and the firewall, and the transmission mode of the FTP server is the passive mode, the device that does not support ALG cannot modify the application layer IP after performing NAT translation at the network layer. This results in that the firewall cannot establish FTP data sessions, leading to the FTP data communication and processing issue. To address this issue, the system supports to enable or disable the use of the server's external IP to establish data connection. By default, this function is disabled.

To enable or disable the function of using the external IP address of the FTP server to establish data connection, in global configuration mode, use the following command:

Enable: **alg ftp external-IP-on-server**

Disable: **no alg ftp external-IP-on-server**

Notes:

- This function can take effect only when the transmission mode of the FTP server is the passive mode.
- Before you enable this function, make sure that the FTP ALG function is enabled. For more information, see Enabling/Disabling the ALG Control Function for Applications.

For more information, refer to the **Firewall** > **Application Layer Identification and Control** topic in *StoneOS_CLI_User_Guide*. FR 35041

Supporting Automatic Verification of Whether the Platform Model Matching the Product Model of License When Installing the V3 License for CloudEdge

WebUI

Platform Models	Minimum Configuration
SG-6000-VM01/VM01-KL	2 vCPU,2 GB memory
SG-6000-VM02/VM02-KL	2 vCPU,4 GB memory
SG-6000-VM04/VM04-KL	4 vCPU,8 GB memory
SG-6000-VM04/VM08-KL	8vCPU,16GB memory

Installing a License

You can install both V2 and corresponding V3 licenses for CloudEdge whose platforms are not developed by China.

If the V3 license of a non-corresponding model is installed on CloudEdge, you need to perform the following operations based on the actual situation.

- When installing the V3 license of a higher-specification CloudEdge platform model on a lower-specification CloudEdge platform, the system can function normally.
- When installing the V3 license of a lower-specification CloudEdge platform model on a higher-specification CloudEdge platform, you cannot perform configuration operations on the WebUI and in the global configuration mode of the CLI. You need to use the **exec license uninstall***license-name* command to uninstall the license of the lower-specification model and then reinstall the V3 license of the corresponding model.

After obtaining the license, you must install it to the device.

To install a license, take the following steps:

1. Select **System** > **License** , and click **Import**.
2. On the **Import License** page, configure options below.
   - Upload License File: Select **Upload License File**. Click **Browse** to select the license file, using the TXT format, and then click **OK** to upload it.
   - Manual Input: Select **Manual Input**. Type the license string into the box.
3. Click **OK**.
4. Go to **System > Device Management** > **Settings & Options**, and click the **System Options** tab.
5. Click **Reboot**, and select **Yes** in the prompt.
6. System will reboot. When it starts again, installed license(s) will take effect.

For more information, refer to the **System Management** > **License** topic in *StoneOS_WebUI_User_Guide*. FR 40832, FR 41871

CLI

Installing/Uninstalling a License

You can install both V2 and corresponding V3 licenses for CloudEdge whose platforms are not developed by China.

If the V3 license of a non-corresponding model is installed on CloudEdge, you need to perform the following operations based on the actual situation.

- When installing the V3 license of a higher-specification CloudEdge platform model on a lower-specification CloudEdge platform, the system can function normally.
- When installing the V3 license of a lower-specification CloudEdge platform model on a higher-specification CloudEdge platform, you cannot perform configuration operations on the WebUI and in the global configuration mode of the CLI. You need to use the **exec license uninstall***license-name* command to uninstall the license of the lower-specification model and then reinstall the V3 license of the corresponding model.

After obtaining the license, to install it, in any mode, use the following command:

exec license install*license-string*

- *license-string* - Pastes the license string.

To uninstall a license, in any mode, use the following command:

exec license uninstall*license-name*

- *license-name* - Specifies the name of the license you want to uninstall.

After installing some licenses, you need to type the command **reboot** to reboot system.

The following licenses will take effect after the reboot and other licenses will take effect directly.

- After installing the following licenses for the first time, you need to reboot the system: Platform Trial, Platform, AV, AV Trial, IPS, IPS Trial, Botnet C&C Prevention, Botnet C&C Prevention Trial, Stoneshield, URL, Sandbox, Virtual CPU, LLB, IP Reputation.
- The system needs to be rebooted each time the following licenses are installed: AEL, VSYS.

For more information, refer to the **System Management** > **License Management** topic in *StoneOS_CLI_User_Guide*. FR 40832, FR 41871

Supporting to Configure the ESB Protocol Subtype for the HTTP(S) SMS Gateway

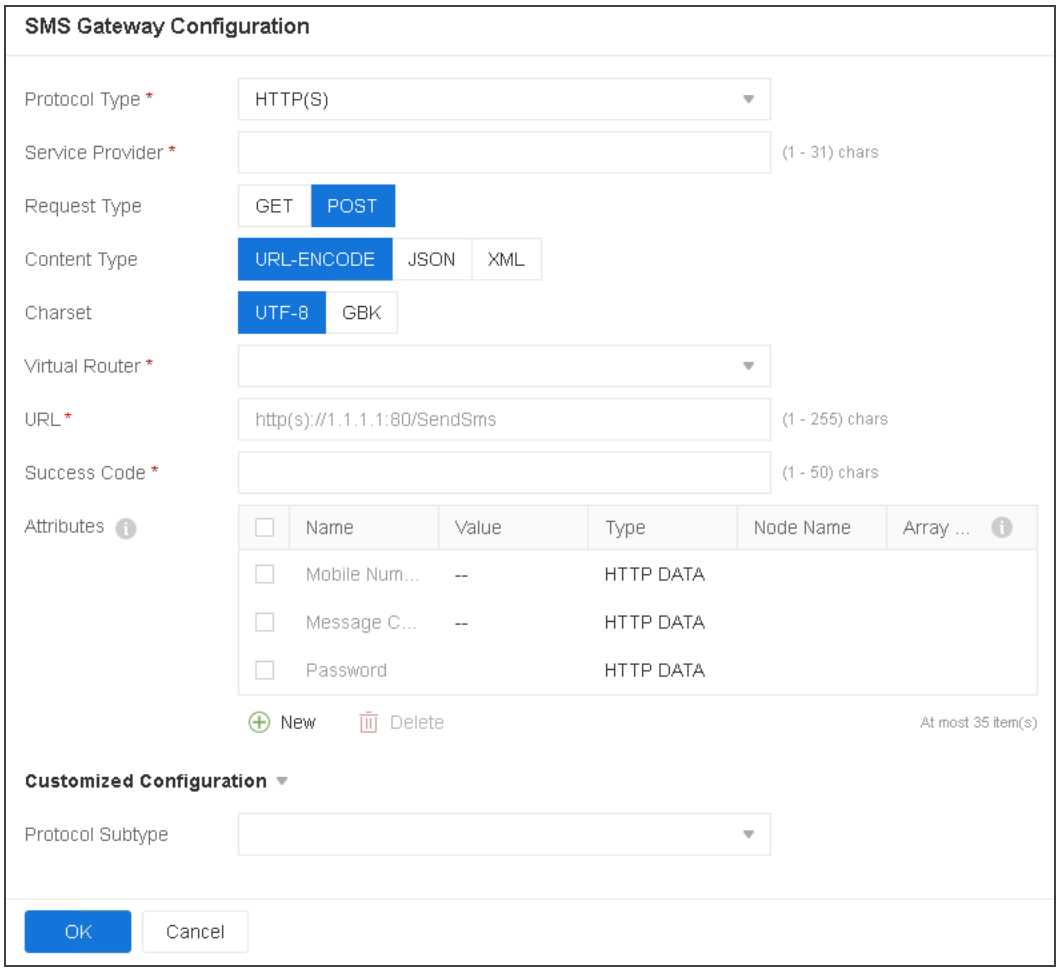
WebUI

Configuring SMS Gateway

To configure the SMS gateway, take the following steps:

1. Select **System > SMS Parameters >SMS Gateway**.

2. Click **New**.



Option	Description
Protocol Type	Specifies the protocol of SMS gateway. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU indicates the Xuanwu Technology SMS service platform. CAS indicates the

Option	Description
	12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. ChinaMobileMusic indicates the SMS platform of China Mobile Music. HTTP(S) indicates HTTP/HTTPS protocol.
Service Provider	Specifies the service provider name. The value range is 1 to 31.
Request Method	When the HTTP (S) protocol type is specified for the SP instance, you can specify the request method of HTTP(S). The default request method is POST.
Content Type	When the HTTP (S) protocol type is specified for the SP instance, you can specify the content type of HTTP Post requests sent to the SMS gateway. By default, URL-ENCODE is selected. • URL-ENCODE - Sets the content type of HTTP POST requests to application/x-www-from-urlencode. • JSON - Sets the content type of HTTP POST requests to application/json. • XML - Sets the content type of HTTP POST requests to XML.
Charset	When the HTTP (S) protocol type is specified for the SP instance, you can specify the charset of HTTP(S). The default charset is UTF-8.
UMS Protocol	When the protocol type is specified as "UMS", users can specify the UMS protocol type. The default protocol type is

Option	Description
	HTTPS.
Protocol	When the protocol type is specified as "ACC", "ALIYUNSMS", "CAS" or BEIKE, users can specify the protocol type. When the protocol type is specified as "CAS", the default protocol type is HTTPS. The default protocol type is HTTP for ACC and ALIYUNSMS, and HTTPS for BEIKE.
Virtual Router	Specifies the VRouter which gateway belongs to. The system supports multi-VR, and the default VR is trust-vr.
URL	When the HTTP (S) or the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the URL of HTTP(S). You need to enter a complete access path, such as "http(s)://1.1.1.1:80/SendSms". The system requests to communicate with the SMS gateway based on the specified URL address. The range is 1 to 255 characters.
Source Mobile Number	When the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the mobile number used to send verification code messages. The value can be an 8-digit to 21-digit number.
Platform ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. The ID is a 4-digit number.

Option	Description
Platform Password	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the password used to log in to China Mobile Music SMS Platform. The password is provided by China Mobile Music SMS Platform. The password is 1 to 64 characters.
Confirm Password	Re-type the password into the **Confirm Password** box.
Platform Subsystem ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the subsystem ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. The ID is a 3-digit number or 7-digit number.
Template ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the template ID of verification code messages, which is provided by China Mobile Music SMS Platform. The ID is a 1-digit to 21-digit number.
Success code	When the HTTP (S) protocol type is specified for the SP instance, you can specify the success code of HTTP(S). Success code is used to determine whether the SMS gateway successfully sent an authentication message. Refer to the status code in the SMS gateway manual. For example, if an SMS gateway sent an authentication message successfully, the status code returned is "OK: 325689", and if failed, the status number returned is "ERROR: eUser". In this instance, you can specify the success code as "OK". The range is 1 to 50 characters.

Option	Description
Root Node	When the protocol type is specified as HTTP(S), request method is specified as POST, and content type is specified as XML, specify the name of the root node of the XML messages sent from the system to the SMS gateway. The name can be 1 to 20 characters in length.
Attributes	When the HTTP (S) protocol type is specified for the SP instance, you can configure attributes to communicate with the SMS gateway. • The mobile number field specifies the parameter name of the mobile number. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The message content field specifies the parameter name of the authentication message. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The password field specifies the parameters of password to log in the SMS gateway. The parameter name and parameter value must exist at the same time or be empty. This is an optional attribute. The range of parameter name is 1 to 20 characters and the range of parameter value is 1 to 255 characters. You can also configure Node Name and Array Object for the field. • Click **New** and configure the parameter name, parameter value, parameter type, node name, and array object of

Option	Description
	the custom attribute of the user to log in to the SMS gateway. • Name: The range is 1 to 20 characters. • Value: The range is 1 to 255 characters. • Type: You can set the type to HTTP DATA or HTTP HEADER. If the type is set to HTTP DATA, the attribute will be used as data content of HTTP. If the type is set to HTTP HEADER, the attribute will be added to the header of HTTP. • Node Name: Enter the node name, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system constructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON or XML format. You can configure 10 different node names. • Array Object: Sets the attribute to array object. This way, the parameter values are stored in array. To do this, click ×. When ✓ is displayed, it indicates that the attribute is set to array object. You can create new attributes as needed, with up to 32 at the same time. Select the check box of the attributes bar and click "Delete".

Option	Description
	Note: • Node name and array object can be configured only when the method is POST, content type is JSON, and parameter type is HTTP DATA. • For the attribute fields with the same node name, the array object configurations need to be consistent. • The parameter name of the mobile number field, message content field, and password field can be the same. For other attributes, the parameter name can be the same only if the parameter types are different.

Protocol Subtype	If the protocol type is set to HTTP(s), you can select MAS, EMAY, ZGC, or ESB from the drop-down list to connect the Hillstone device to the mobile cloud MAS SMS platform, EMAY SMS, ZGC SMS, or ESB SMS platform.
	• To specify the MAS protocol subtype, you need to configure the following attributes in the Attributes section above:
	  • mobiles: Sets the name of the mobile number field to mobiles. This attribute is required.
	  • content: Sets the name of the SMS content field to content. This attribute is required.
	  • secretKey: Specifies the name and value of the password used to log in to the SMS gateway. The

Option	Description
	name needs to be "secretKey" and the value can be 1 to 255 characters in length. This attribute is required. • apId: Click **New** and specify the name, value, and type of the username used to log in to the SMS gateway. The name needs to be "apId", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • ecName: Click **New** and specify the name, value, and type of the enterprise name field. The name needs to be "ecName", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • sign: Click **New** and specify the name, value, and type of the signature code field. The name needs to be "sign", the value is provided by China Mobile Cloud MAS SMS Platform, and the type needs to be "HTTP DATA". This attribute is required. • addSerial: Click **New** and specify the name, value, and type of the extension code field. The name needs to be "addSerial", the value is provided by China Mobile Cloud MAS SMS Platform, and the

Option	Description

	type needs to be "HTTP DATA". This attribute is optional.
	• To specify the ESB protocol subtype, you need to configure the following attributes in the Attributes section above:
	  • MOBILE: Sets the name of the mobile number field to MOBILE. This attribute is required.
	  • MSG: Sets the name of the SMS content field to MSG. This attribute is required.
	  • Password: Sets the parameter name and value of the password field of the ESB SMS platform. You can customize the parameter name, and the parameter value is provided by the ESB SMS platform. This attribute is optional.
	  • CHANNEL_CODE: Click **New** and specify the parameter name, value, and type of the channel name. The parameter name needs to be specified as "CHANNEL_CODE", the parameter value is provided by the ESB SMS platform, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required.
	  • SYS_HEAD: Click **New** and specify the node name "SYS_HEAD" that needs to be included in

Option	Description
	the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value is filled based on the requirements, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required. • BODY: Click **New** and specify the node name "BODY" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value is filled based on the requirements, and the parameter type is specified as "HTTP DATA" or "HTTP HEADER". This attribute is required. **Note**: • When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the charset needs to be

Option	Description
	"UTF-8". • When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON". • When you specify the ESB protocol subtype, to connect the Hillstone device to the ESB SMS platform, the request type needs to be "POST" and the content type needs to be "XML".
Host	Specifies the gateway address.
Port	Specifies the port number of the gateway. When the protocol type is specified as "SGIP", the default port number is 8801; When the protocol type is specified as "ACC", the default port number is 80; When the protocol type is specified as "BEIKE", the default port number is 8086; When the protocol type is specified as "UMS", the default port number is 9600. When the protocol type is specified as "XUANWU" or "CAS", the default port number is 8080.
Device Code	Specifies the device code, the range is 1 to 4294967295. When the protocol type is specified as "SGIP", and before configuring the SMS gateway, you have to ask your supplier to provide the device ID of SP, which sends the SMS messges.
Source Number	When the protocol type is specified as "SGIP", and aftering enabling the SMS Authentication function, the system will send an Auth-message to the mobile phone number. Specifies the user's phone number, the range is 1 to 21.

Option	Description
Company Code	When the protocol type is specified as "UMS", users can specify the enterprise code registered on the UMS platform. The range is 1 to 31 digits.
Username	Specifies the username to log in SMS gateway. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Password	Specifies the password for the user. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Template Name	Specifies the template parameter of BEIKE SMS gateway.
Confirm Password	Re-type the password into the **Confirm Password** box to confirm.
Change Password	When you edit the SMS gateway, you can see the Change Password function. After you enable this function, the Password field is displayed. To change the password, enter a new one in this field and save the configuration.
SMS Limit/hour	Defines the maximum message number the gateway can send in one hour.
SMS Limit/day	Defines the maximum messages number the gateway can send in one day.
AccessKeyId	Specifies the AccessKeyId which will be used as the username for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the

Option	Description
	template AccessKeyId applied in the SMS of Alibaba Cloud.
AccessKeySecret	Specifies the AccessKeySecret which will be used as the password for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the template AccessKeySecret applied in the SMS of Alibaba Cloud.
Confirm AccessKeySecret	Re-type the AccessKeySecret to confirm.
Trading Code	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the trading code. The range is 1-7.
Channel	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the channel. The range is a-z.
Request Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the request type. The range is 1-6.
Organization Code	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the organization code. The range is 1-31.
SMS Service Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the SMS service type. The range is 1-31.
Send Sign Code	When the protocol type is specified as "ACC", select the

Option	Description
	Enable check box to enable the Send Sign Code function. When this function is enabled, the ACC SMS gateway will add a sign code field when sending a request to the ACC server, which will prevent the content of the SMS from being tampered with.

For more information, refer to the **System Management** > **SMS Parameters** > **SMS Gateway** topic in *StoneOS_WebUI_User_Guide*. FR 39815

CLI

SMS Gateway Authentication

Introduction to Configuring an SP Instance

In the SP instance configuration mode, you can configure as follows:

- Specifying the VRouter
- Specifying the Request Method
- Specifying the Charset
- Specifying the UMS/ACC/ALIYUNSMS/CAS/BEIKE Protocol
- Specifying the URL
- Specifying Source Mobile Number
- Configuring Platform ID
- Configuring Platform Password
- Configuring Platform Subsystem ID

- Configuring Template ID
- Specifying the Success Code
- Configuring the root node
- Specifying the Attributes
- Configuring the protocol subtype

……

Specifying the Content Type of the HTTP(S) Packets

When the HTTP(S) protocol type is specified for the SP instance, you can specify the content type of HTTP POST request packets. The default content type is URL-ENCODE. To specify the content type of HTTP POST request packets, in the SP instance configuration mode, use the following command:

content-type { **url-encode** | **json** | **xml**}

- **url-encode**-Indicates that the content type of HTTP POST request packets is application/x-www-from-urlencode.
- **json** - Indicates that the content type of HTTP POST request packets is application/json.
- **xml** - Indicates that the content type of HTTP POST request packets is XML.

To restore to the default content type of HTTP POST request packets, use the command **nocontent-type**.

Configuring the Root Node

When the HTTP (S) protocol type, POST request method, and XML content type are specified for the SP instance, you can specify the name of the root node of the XML messages sent from the system to the SMS gateway.

To configure the root node, in SP instance configuration mode, use the following command:

xml-root*value*

- *value* – Specifies the name of the root node, which needs to be 1 to 20 characters in length.

To delete the specified root node, use the **no xml-root** command.

Specifying the Attributes

When the HTTP (S) protocol type is specified for the SP instance, you can configure attributes to communicate with the SMS gateway. Attributes including the parameter name of the mobile number field, the parameter name of the message content field, the password filed, and the username filed, etc. You can configure up to 32 attributes. The parameter name of the mobile number field and the parameter name of the message content field are default attributes and must be specified. The password field and other custom fields about user are optional.

Notes:

- Node name and array object can be configured only when the method is POST, content type is JSON, and parameter type is HTTP DATA.
- For the attribute fields with the same node name, the array object configurations need to be consistent.

To specify the parameter name of the mobile number field and the parameter name of the message content field, in SP instance configuration mode, use the following command:

default-attribute {**phone-attr-name***phone-attr-name* | **msg-content-attr-name***msg-content-name*} [**node***node-name*] [**add-to-array**]

- **phone-attr-name***phone-attr-name* – Specifies the parameter name of the mobile number field, such as phone. This is the default attribute and the range is 1 to 20 characters.
- **msg-content-attr-name***msg-content-name* – Specifies the parameter name of the message content field, such as msg. This is the default attribute and the range is 1 to 20 characters.

- **node** *node-name* - Specifies the node name of the mobile number field or message content field, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names.
- **add-to-array**- Sets the mobile number field or message content field to array object. After you specify this parameter, the parameter values are stored in array.

The system will obtain the parameter values of the mobile number field and the parameter values of the message content field when SMS gateway and the system is communicating.

When the SMS gateway and the system communicate, the SMS gateway can obtain the parameter values of the mobile number field and the parameter values of the message content field from the system. To delete the parameter name of the specified mobile number field and the parameter name of the message content field, use the command **nodefault-attribute** {**phone-attr-name** | **msg-content-attr-name**}.

To specify the parameters of password to log in SMS gateway, which is an optional attribute, in SP instance configuration mode, use the following command:

password-attribute {*password-name password-value*} [**node***node-name*] [**add-to-array**]

- *password-name* – Specifies the parameter name of the password, such as password. The range is 1 to 20 characters.
- *password-value* – Specifies the parameter value of the password, such as 123456. The range is 1 to 255 characters.
- **node***node-name* - Specifies the node name of the password field, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names.

- **add-to-array**- Sets the password field to array object. After you specify this parameter, the password field value is stored in array.

To delete the specified parameters of password, use the command **nopassword-attribute**.

To specify the custom parameter of user to log in SMS gateway, which is optional, in SP instance configuration mode, use the following command:

user-attribute {*parameter-name value*} [**add-to-header** | **node** *node-name*] [**add-to-array**]

- *parameter-name* – Specifies the parameter name of the custom parameter, such as username. The range is 1 to 20 characters.
- *value* – Specifies the value of the custom parameter, such as user1. The range is 1 to 255 characters.
- **add-to-header** – Specifies to add the custom parameter of the user to the HTTP header. If not specified, the parameter will be used as the data content of HTTP (HTTP DATA).
- **node***node-name* - Specifies the node name of the custom parameter, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system reconstructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON or XML format. You can configure 10 different node names.
- **add-to-array** - Sets the custom parameter of the user to array object. After you specify this parameter, the custom parameter value is stored in array.

To delete the specified custom parameter of user, use the command **nouser-attribute** {*parameter-name*} [**add-to-header**. If **add-to-header** is specified when you configure the user attribute, you need to specify **add-to-header** when you delete the user attribute.

Configuring the Protocol Subtype

When the SP instance uses the HTTP(s) protocol type, you can configure the MAS, EMAY, ZGC, or ESB protocol subtype to connect the Hillstone device to the mobile cloud MAS SMS platform,

EMAY SMS platform, ZGC SMS, or ESB SMS platform. To configure the protocol subtype, run the following command in SP instance configuration mode:

subtype { **mas** | **emay** | **zgc** | **esb**}

In SP instance configuration mode, run the **no subtype** command to delete the MAS, EMAY, ZGC, or ESB protocol subtype configuration.

When you specify the MAS protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- mobiles: In SP instance configuration mode, run the **default-attribute phone-attr-name mobiles** command to set the name of the mobile number field to mobiles. This attribute is required.
- content: In SP instance configuration mode, run the **default-attribute msg-content-attr-name content** command to set the name of the SMS content field to content. This attribute is required.
- secretKey: In SP instance configuration mode, run the **password-attribute secretKey** *password-value* command to set the name of the password used to log in to the SMS gateway to secretKey. The *password-value* can be 1 to 255 characters in length. This attribute is required.
- apId: In SP instance configuration mode, run the **user-attribute apId** *value* command to set the username used to log in to the SMS gateway to apId. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.
- ecName: In SP configuration mode, run the **user-attribute ecName** *value* command to set the name of the enterprise name field to ecName. The *value* can be 1 to 255 characters in length. By default, the field type is HTTP DATA. This attribute is required.
- sign: In SP instance configuration mode, run the **user-attribute sign** *value* command to set the name of the signature code field to sign. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is required.

- addSerial: In SP instance configuration mode, run the **user-attribute addSerial** *value* command to set the name of the extension code field to addSerial. The *value* is provided by China Mobile Cloud MAS SMS Platform. By default, the field type is HTTP DATA. This attribute is optional.

To specify the ESB protocol subtype, you need to configure the following attributes. For more information, see Configuring Attributes:

- MOBILE: In SP instance configuration mode, use the **default-attribute phone-attr-name MOBILE** command to set the parameter name of the mobile number field to "MOBILE". This attribute is required.
- MSG: In SP instance configuration mode, use the **default-attribute msg-content-attr-name MSG** command to set the parameter name of the SMS content field to "MSG". This attribute is required.
- Password: In SP instance configuration mode, use the **password-attribute***password-name password-value* command to specify the parameter name and parameter value of the password field of the ESB SMS platform. You can customize the parameter name *password-name*, and the parameter value *password-value* is provided by the ESB SMS platform. This attribute is optional.
- CHANNEL_CODE: In SP instance configuration mode, use the **user-attribute CHANNEL_CODE***value* command to specify the parameter name "CHANNEL_CODE" of the channel name; the parameter value *value* is provided by the ESB SMS platform; the parameter type is "HTTP DATA" by default. This attribute is required.
- SYS_HEAD: In SP instance configuration mode, use the **user-attribute** {*parameter-name value*} [**node SYS_HEAD**] command to specify the node name "SYS_HEAD" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name *parameter-name* is provided by the ESB SMS platform and needs to be capitalized

when configuring, the parameter value *value* is filled based on the requirements, and the parameter type is specified as "HTTP DATA" by default. This attribute is required.

- BODY: In SP instance configuration mode, use the **user-attribute** {*parameter-name value*} [**node BODY**] command to specify the node name "BODY" that needs to be included in the XML message sent from the system to the ESB SMS platform, and configure the parameter name, value, and type of the attribute belonging to this node name. The parameter name *parameter-name* is provided by the ESB SMS platform and needs to be capitalized when configuring, the parameter value *value* is filled based on the requirements, and the parameter type is specified as "HTTP DATA" by default. This attribute is required.

Notes:

- When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the chartset needs to be "UTF-8".
- When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON".
- When you specify the ESB protocol subtype, to connect the Hillstone device to the ESB SMS platform, the request type needs to be "POST" and the content type needs to be "XML".

For more information, refer to the **VPN** > **SSL VPN** > **Two-Step Verification** > **SMS Gateway Authentication** section in *StoneOS_CLI_User_Guide*. FR 39815

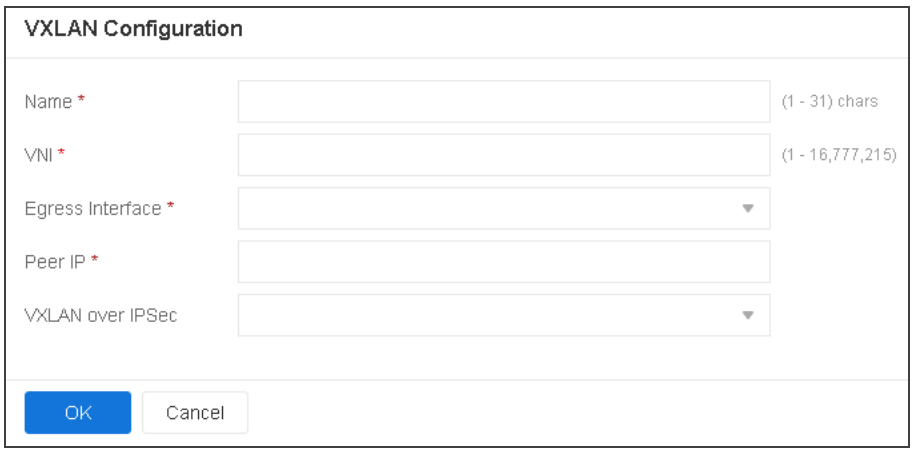
Supporting to Transmit VXLAN Packets by Using the IPSec Tunnel

WebUI

Creating VXLAN Static Tunnel

To creating VXLAN static tunnel, take the following steps:

1. Click **Network > VPN > VXLAN**.
2. Click **New**.



Option	Description
Name	Specified the name of the VXLAN static tunnel.
VNI	Specified the ID as the global network identity of the VXLAN network. The value range is 1 to 16777215.
Egress Interfaces	Select the egress interface of the VXLAN network in the drop-down list. **Notes:** When binding the VXLAN instance to the tunnel

Option	Description
	interface, you need to bind the tunnel interface to Layer 2 zone.
Peer IP	Specified the destination VTEP IP address.
VXLAN over IPSec	Select the IPSec tunnel that you want to reference from the drop-down list. This way, you can encrypt and encapsulate VXLAN packets in IPSec packets, ensuring the security of data transmitting in the VXLAN tunnel. For more information about how to create an IPSec VPN tunnel, see Configuring IPSec VPN. **Notes:** • The IPSec tunnel whose peer type is "User Group" cannot be referenced. • Only the HA Active-Passive (A/P) mode is supported.

3. Click **OK**.

For more information, refer to the **VPN** > **VXLAN** topic in *StoneOS_WebUI_User_Guide*.
FR38128

Viewing IPSec VPN Entry

To view an IPSec VPN entry of specified filter condition, take the following steps:

1. Select **Network** > **VPN** > **IPSec VPN**.
2. In the IPSec VPN tab, enter the name of the IPSec VPN entry or the peer name in the text boxes at the top of the toolbar to view the IPSec VPN entry under the specified conditions.

3. Click the value in the "Referenced by" column to view the details of the configuration items associated with an IPSec VPN entry.
4. Click the value in the **Referenced by** column to view details about the reference of the IPSec VPN entry.
    - Click the object name to view detailed configuration about the object.
    - Click **Unreference** to cancel the reference of the IPSec tunnel from the object.
    - Click **Delete** to delete the object and cancel the reference of the IPSec tunnel from the object.

For more information, refer to the **VPN** > **IPSec VPN** > **Configuring an IPSec VPN** topic in *StoneOS_WebUI_User_Guide*. FR38128

CLI

Configuring VXLAN Static Tunnel

Specifying the Referenced IPSec Tunnel

The system supports to encrypt and encapsulate VXLAN packets in IPSec packets, ensuring the security of data transmitting in the VXLAN tunnel. To specify the referenced IPSec tunnel, in VXLAN tunnel configuration mode, use the following command:

next-tunnel ipsec*tunnel-name*

- *tunnel-name* - Specifies the IPSec tunnel name referenced by the VXLAN static tunnel.

In VXLAN tunnel configuration mode, use the **no next-tunnel** command to cancel the configuration.

Notes:

- The IPSec tunnel whose peer type is "User Group" cannot be referenced.
- Only the HA Active-Passive (A/P) mode is supported.

For more information, refer to the **VPN** > **VXLAN** topic in *StoneOS_CLI_User_Guide*. FR38128

Specifying the Device as the NTP Server

WebUI

System Time

Describes how to configure the system time, including configuring the system time and synchronizing the system time via the NTP server. In addition, the device can function as the server to synchronize the system time for other clients. A device can act as both the server and the client at the same time, and it can provide services to multiple devices at the same time.

Configuring the System Time Manually

To configure the system time manually, take the following steps:

1. Select **System** > **Device Management** > **System Time**.
2. Under System Time Configuration in the System Time tab, configure the following.

Option	Description
Sync with Local PC	Specifies the method of synchronize with local PC. You can select **Sync Time** or **Sync Zone&Time**. • Sync Time: Synchronize the system time with local PC. • Sync Zone&Time: Synchronize the system zone&time with local PC.

Option	Description
Specified the system time.	Configure parameter of system time. • Time Zone: Select the time zone from the drop-down list. • Date: Specifies the date. • Time: Specifies the time.

3. Click **OK**.

Specifying the Device as the NTP Client

The system time may affect the establishment time of VPN tunnel and the schedule, so the accuracy of the system time is very important. To ensure the system is able to maintain an accurate time, the device allows you to synchronize the system time with a NTP server on the network via NTP protocol.

To specify the device as the NTP client, take the following steps:

1. Select **System** > **Device Management** > **System Time**.
2. Under NTP Configuration in the System Time tab, configure the following.

Option	Description
Enable	Select the **Enable** check box to enable the NTP function. By default, the NTP function is disabled.
Authentication	Select the **Authentication** check box to enable the NTP Authentication function.
Server	Specifies the NTP server that device need to synchronize with. You can specify at most 3 servers. • IP: Type IP address of the server .

Option	Description
	• Key: Select a key from the **Key** drop-down list. If you enable the NTP Authentication function, you must specify a key. • Virtual Router: Select the Virtual Router of interface for NTP communication from the drop-down list. • Source interface: Select an interface for sending and receiving NTP packets. • Specify as a preferred server: Click **Specify as a preferred server** to set the server as the first preferred server. The system will synchronizate with the first preferred server.
Sync Interval	Type the interval value. The device will synchronize the system time with the NTP server at the interval you specified to ensure the system time is accurate.
Time Offset	Type the time value. If the time difference between the system time and the NTP server's time is within the max adjustment value you specified, the synchronization will succeed, otherwise it will fail.

3. Click **OK**.

Specifying the Device as the NTP Server

When the device synchronizes its clock by using other NTP servers or specifies the local clock as the primary clock, the device's own clock is in the synchronized state. At this time, the device can serve as the NTP server to provide synchronized clock services to other clients.

To specify the device as the NTP server, take the following steps:

1. Select **System** > **Device Management** > **System Time**.

2. In the Enable NTP Server Service section, configure the following options:

Option	Description
Enable	Turn on the switch to enable the NTP server function. By default, this function is disabled.
Listening Interface	The listening interface is used to receive synchronization requests from the client and provide synchronization services to the client. Specify the interface on the device that receives and sends NTP packets. Up to 32 interfaces can be configured, and only Layer 3 interfaces are supported.
Set Local Clock As Primary	Click the button to specify the device's local time as the reference clock to provide synchronization services to the client. By default, this is disabled. Note: Before setting the local clock as the primary clock, calibrate the device time.
Stratum Of Local Time	After enabling the local clock as the primary clock, specify the stratum of local time. Valid values: 1 to 14. Default value: 8. The stratum indicates clock precision, with a smaller value indicating higher precision. When the device is configured with other servers as time sources: • If the local clock's stratum is greater than the stratum provided by the server, the device will use the time server as a reference; • If the local clock's stratum is less than the stratum provided

Option	Description
	by the server, the device will use the local clock as a reference.
NTP Server Key	Specifies the trusted key for the device as the server, used for authentication with other clients. For more information about how to create an NTP key, see NTP Key.

3. Click **OK**.

NTP Key

After enabling NTP Authentication function, you need to configure MD5 key ID and keys. The device will only synchronize with the authorized servers.

Creating an NTP Key

To create an NTP key:

1. Select **System** > **Device Management** > **NTP Key**.
2. Click **NEW**.

Option	Description
Key ID	Type the ID number into the Key ID box. The value range is 1 to 65535.
Password	Type a MD5 key into the **Password** box. The value range is 1 to 31.
Confirm Password	Re-type the same MD5 key you have entered into the **Confirm** box.

3. Click **OK**.

For more information, refer to the **System Management** > **Device Management** > **System Time** topic in *StoneOS_WebUI_User_Guide*. FR38570

CLI

Specifying the Device as the NTP Client

By configuring the NTP client, you can synchronize the system time of the device with the clock server. The system supports the following NTP client configurations:

- Enabling/Disabling NTP Client Service
- Configuring an NTP Sever
- Configuring the Max Adjustment Value
- Configuring the Query Interval
- Enabling/Disabling NTP Authentication
- Configuring NTP Authentication

Enabling/Disabling NTP Client Service

By default, NTP client service on Hillstone devices is disabled.

To enable/disable NTP client service, in the global configuration mode, use the following commands:

- Enable: **ntp enable**
- Disable: **no ntp enable**

Configuring an NTP Server

You can specify up to three NTP servers, one of which with keyword "prefer" is the primary NTP server, or, if no "prefer" is specified, the earliest configured NTP server is the first one for time synchronization.

To configure an NTP server, in the global configuration mode, use the following command:

ntp server {*ip-address* | *host-name*} [**key***number*] [**source***interface-name*] [**prefer**] [**vrouter***vrouter-name*]

- *ip-address* | *host-name*- Specifies the IP address or host name of the NTP server. The length of the host name can be 1 to 127 characters.
- **key***number* - Specifies the password of the NTP server if it requires so.
- **source***interface-name* - Specifies the interface on which the security device sends and receives NTP packets.
- **prefer**- If more than one NTP servers are specified, use this keyword to determine the primary server.
- *vrouter-name* - Specifies NTP server for the specified VRouter.

To cancel the NTP server settings, use the command **no ntp server** {*ip-address* | *host-name*}.

Here is an example of configuring a NTP server:

```
hostname(config)# ntp server 10.160.64.5 prefer
```

Configuring the Max Adjustment Value

The maximum time adjustment value represents the acceptable time difference between the device system clock and the time received from an NTP server. The device only adjusts its clock with the NTP server time if the time difference between its clock and the NTP server time is within the maximum time adjustment value.

To set the maximum adjustment value, in the global configuration mode, use the following command:

ntp max-adjustment*time-value*

- *time-value* - Specifies the time value. The value range is 0 to 3600 seconds. The value of 0 means no adjustment time. The default value is 400.

To restore to the default value, use the command **no ntp max-adjustment**.

Configuring the Query Interval

The device updates its clock with NTP servers at intervals of the value you set here.

To configure the query interval, in the global configuration mode, use the following command:

ntp query-interval*time-interval*

- *time-interval* - The query interval. The value range is 1 to 60 minutes. The default value is 5.

To restore to the default value, use the command **no ntp query-interval**.

Enabling/Disabling NTP Authentication

By default, NTP authentication is disabled.

To enable/disable NTP authentication, in the global configuration mode, use the following commands:

- Enable: **ntp authentication**
- Disable: **no ntp authentication**

Configuring NTP Authentication

If you choose to use NTP authentication, the security device only interact with servers that pass the authentication.

To configure NTP authentication key ID and key, in the global configuration mode, use the following command:

ntp authentication-key*number***md5***string*

- *number* - Specifies the key ID number. The value range is 1 to 65535.
- *string* - Specifies MD5 authentication key. The length is 1 to 31 characters.

To cancel the authentication private key settings, in the global configuration mode, use the command **no ntp authentication-key***number*.

Specifying the Device as the NTP Server

By configuring the NTP server, you can synchronize the system time for other clients. A device can act as both the server and the client at the same time, and it can provide services to multiple devices at the same time. When the device synchronizes its clock by using other NTP servers or specifies the local clock as the primary clock, the device's own clock is in the synchronized state. At this time, the device can serve as the NTP server to provide synchronized clock services to other clients. The system supports the following NTP server configurations:

- Enabling/Disabling NTP Server Service
- Configuring the Listening Interface
- Setting Local Clock As Primary
- Configuring NTP Server Key

Enabling/Disabling NTP Server Service

By default, NTP server service on Hillstone devices is disabled. To enable/disable NTP server service, in the global configuration mode, use the following commands:

- Enable: **ntp server-service enable**
- Disable: **no ntp server-service enable**

Configuring the Listening Interface

The listening interface is used to receive synchronization requests from the client and provide synchronization services to the client. To specify the listening interface, in global configuration mode, use the following command:

ntp server-service listening-interface*interface-name*

- *interface-name* - Specifies the interface on the device that receives and sends NTP packets. Up to 32 interfaces can be configured, and only Layer 3 interfaces are supported.

In global configuration mode, use the **no ntp server-service listening-interface***interface-name* command to cancel the configuration.

Setting Local Clock As Primary

You can specify the device's local time as the reference clock to provide synchronization services to the client. By default, this is disabled. To set the local clock as primary, in global configuration mode, use the following command:

ntp refclock local [**stratum***stratum-value*]

- *stratum-value* - Specifies the stratum of local time. Valid values: 1 to 14. Default value: 8. The stratum indicates clock precision, with a smaller value indicating higher precision. When the device is configured with other servers as time sources:
    - If the local clock's stratum is greater than the stratum provided by the server, the device will use the time server as a reference;
    - If the local clock's stratum is less than the stratum provided by the server, the device will use the local clock as a reference.

In global configuration mode, use the **no ntp refclock local** command to cancel the configuration.

Configuring NTP Server Key

You can specify the trusted key for the device as the server, used for authentication with other clients. To specify the NTP server key, in global configuration mode, use the following command:

ntp server-service key *key-id*

- *key-id* - Specifies the ID of the NTP server key. To create an NTP key, see Configuring NTP Authentication.

In global configuration mode, use the **no ntp server-service key** command to cancel the configuration.

Viewing NTP Status

To view the current NTP configurations, in any mode, use the command **show ntp status**.

Viewing/Clearing Statistics about Sending NTP Packets

After specifying the device as the NTP server, in any mode, use the **show ntp server-service packets statistics** command to view the statistics about sending/receiving/handling/dropping NTP packets of the current device.

In any mode, use the **show ntp server-service packets statistics clear** command to clear the statistics about sending/receiving/handling/dropping NTP packets of the current device.

For more information, refer to the **System Management** > **Network Time Protocol (NTP)** > **Configuring NTP** topic in *StoneOS_CLI_User_Guide*. FR38570

Log

ID:	0x43200522
Type:	Event
Severity:	Notifications
Message:	The NTP server fails to send packets to *client-address*.
Description:	The device fails to send NTP packets to the client as the NTP server.
Solution:	N/A

For more information, refer to the **NTP** topic in *StoneOS Log Messages Reference Guide*. FR38570

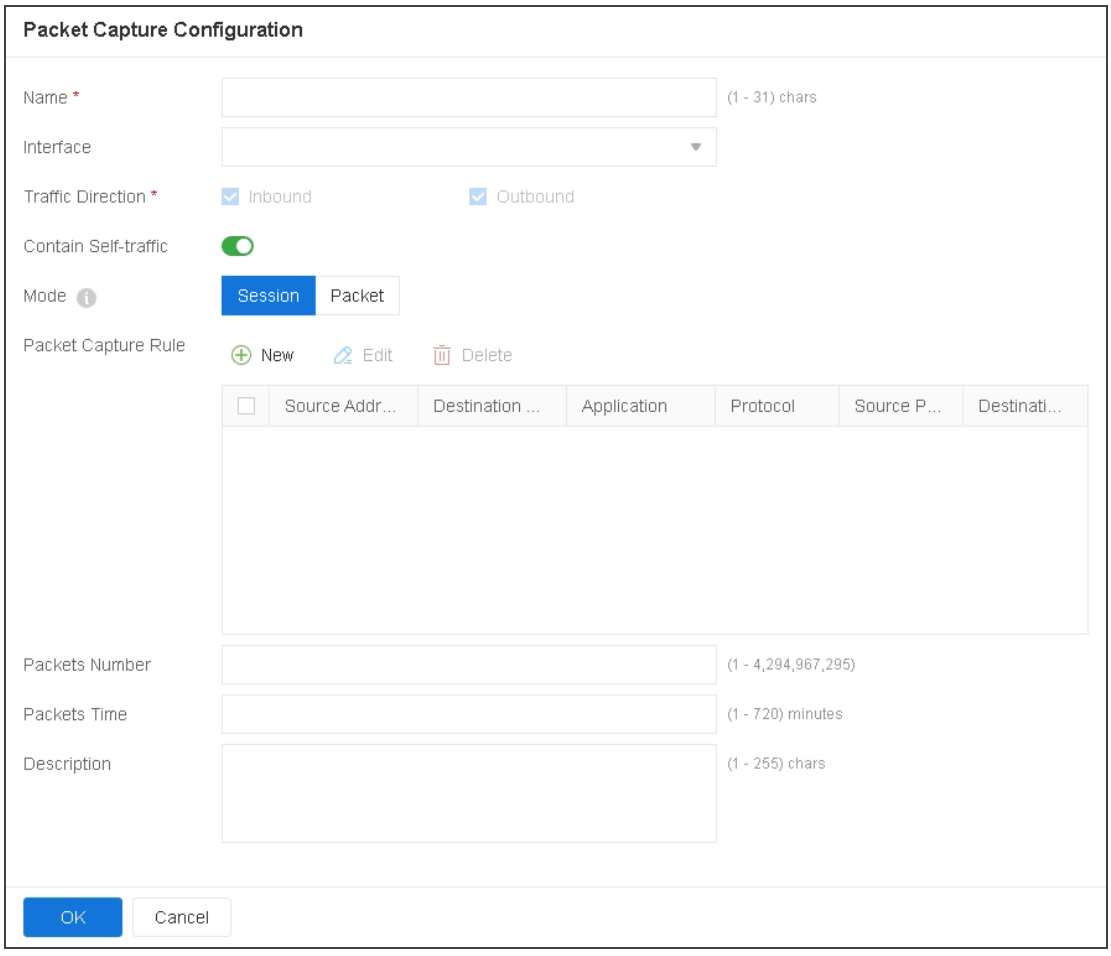
Supporting to Capture All Packets of Interface

WebUI

Configuring Packet Capture Tools

To capture packets, take the following steps:

1. Select **System > Diagnostic Center > Packet Capture Tool**.
2. Click **New**.

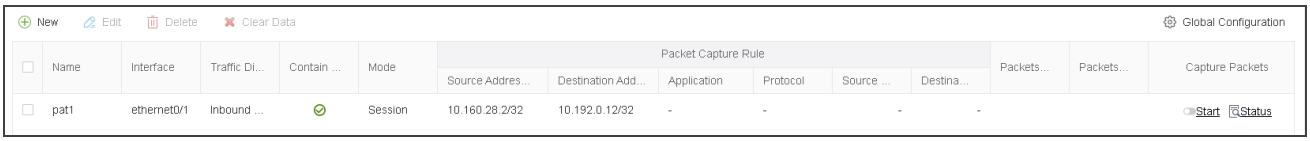


Option	Description
Name	Enter the name of the packets capture entry.
Interface	Select the interface used for the online packet capture task from the drop-down list.
Traffic Direction	Specifies the traffic direction of the interface. Valid values: Inbound and Outbound. By default, both Inbound and Outbound are selected. • Inbound: The online packet capture task captures packets that flow from the specified interface into the device. If fails, the packets may be blocked by the firewall or not flow into the firewall. If no packets flow into the firewall, you can troubleshoot the upstream link or upstream device as needed. • Outbound: The online packet capture task captures packets that flow out from the specified interface. If succeeds, you can troubleshoot the downstream link or downstream device as needed. • Inbound+Outbound: You can select both inbound and outbound and determine the actual traffic direction of the interface based on captured packets.
Mode	Specifies the mode of capturing packets, including the session mode and packet mode. By default, the session mode is selected. • Session: In this mode, the system can efficiently capture packets that have established sessions and meet the packet

Option	Description
	capture rule. ◦ Contain Self-traffic: Turn on the switch to enable the Contain Self-traffic function. This way, captured packets contain traffic sent and received by the device itself. By default, this function is enabled. ◦ Packet Capture Rule: Click **New**, and configure the packet capture rules in the **Packet Capture Rules** page. For the configuration method, refer to Create a Packet Capture Rule. Select the check box of the packet capture rule in the list and click the **Edit** button to edit the configuration of the packet capture rule again. Select the check box of the packet capture rule in the list and click the **Delete** button to delete the packet capture rule. • Packet: When the system resources are sufficient, in this mode, the system can capture packets of all traffic. Notes: • In session mode, you cannot capture packets of hardware fast forward. • In packet mode, you cannot capture packets of hardware fast forward and IOM card fast forward.

Option	Description
Packets Number	Specifies the total number of packets that can be captured for the packet capture task. Valid values: 1 to 4294967295. During the effective period (packets time) of the packet capture task, if the number of packets captured reaches the configured number, the system automatically stops capturing packets.
Packets Time	Enter the packets time in the text box. Valid values: 1 to 720 minutes. Default value: 30 minutes.
Description	Enter the entry description in the text box.

3. Click **OK**.



4. For each task, click **Start** button in the Capture Packets column to start capturing packets, and **Start** button will change to **Capturing**. Click the **Status** to view the current size/number of packets captured.

5. To stop capturing packets, click **Capturing** button in the Capture Packets column.

6. After you stop capturing packets or the capturing is completed, click **Download** at the top-right corner of the Capture Grid List to save the captured packets to a specified location.

7. You can select one or more file entries, and click **Export** at the top right corner of the list to export the package files. The exported grab package files are in compressed format.

8. To clear packet capture data, select a packet capture task and click the **Clear Data** button. All files captured under this task will be cleared.

Notes:

- At most 5 online packet capture tasks can be created.
- An online packet capture task cannot capture packets based on the tunnel interface and MGT0 interface.
- We recommend that the packet you capture at a time does not exceed 500 MB because a larger packet may fail to be exported caused by timeout.
- At most 5 packet capture tasks can be configured within each VSYS.
- You can start only one packet capture task within a single VSYS each time, and start a packet capture task within multiple VSYSes at the same time.
- When you delete a non-root VSYS, the packet capture tasks and packet capture files within the VSYS are deleted at the same time.

For more information, refer to the **Diagnostic Center > Packet Capture Tool** topic in *StoneOS_WebUI_User_Guide*. FR 36021

CLI

Configuring Packet Capture Task

Including configuration capture tasks, capture rules, start/stop capture, export capture files, clear capture files.

packet-capture task

Create an online packet capture task and enter the packet capture task configuration mode. Use the no form of the command to delete the specified online packet capture task.

Command:

packet-capture task*task-name*

no packet-capture task*task-name*

Description:

task-name - Specifies the name of the online packet capture task and enter the packet capture task configuration mode.

Default values:

None

Mode:

Global configuration mode

Guidance:

At most 5 packets capture tasks can be configured within each VSYS.

Example:

```
hostname(config)# packet-capture task task1
```

include-self-traffic

Enable the Contain Self-traffic function so that captured packets contain traffic sent and received by the device itself. Use the no form of the command to disable this function.

Command:

include-self-traffic

no include-self-traffic

Description:

None

Default values:

Enable

Mode:

Packet capture task configuration mode

Guidance:

You can configure this function when the packet capture mode is session mode.

Example:

hostname(config-pkt-task)# include-self-traffic

interface

Configure the interface used for the online packet capture task. Use the no form of the command to delete the specified interface.

Command:

interface*interface-name*

no interface

Description:

interface-name - Specifies the name of the interface used for the online packet capture task, which cannot capture packets based on the tunnel interface and management interface.

Default values:

None

Mode:

Packet capture task configuration mode

Guidance:

None

Example:

hostname(config-pkt-task)# interface ethernet0/0

direction

Configure the traffic direction of the interface. Use the no form of the command to delete the specified traffic direction.

Command:

direction {**in** | **out**}

no direction

Description:

in - Specifies to capture packets that flow from the interface into the device. If fails, the packets may be blocked by the firewall or not flow into the firewall. If no packets flow into the firewall, you can troubleshoot the upstream link or upstream device as needed.

out - Specifies to capture packets that flow out from the interface. If succeeds, you can troubleshoot the downstream link or downstream device as needed.

If **direction** is not configured, both inbound and outbound are specified. In this case, you can determine the actual traffic direction based on captured packets.

Default value:

None

Mode:

Packet capture task configuration mode

Guidance:

None

Example:

```
hostname(config-pkt-task)# direction in
```

task-info

Configure the packet capture task.

Command:

task-info [mode {session-mode | packet-mode}] [pacp-num*number-value***] [pacp-time***time-value***] [description***description***]**

no task-info

Description:

mode {session-mode | packet-mode} - Specifies the mode of capturing packets, including the session mode and packet mode. By default, the session mode is selected.

- **session-mode** - The session mode. In this mode, the system can efficiently capture packets that have established sessions and meet the packet capture rule.

- **packet-mode** - The packet mode. When the system resources are sufficient, in this mode, the system can capture packets of all traffic.

Notes:

- In session mode, you cannot capture packets of hardware fast forward.
- In packet mode, you cannot capture packets of hardware fast forward and IOM card fast forward.

pacp-num*number-value* - Specifies the total number of packets that can be captured for the packet capture task. The value ranges from 1 to 4294967295. During the effective period (pacp-time) of the packet capture task, if the number of packets captured reaches the configured number, the system automatically stops capturing packets.

pacp-time*time-value* - Specifies the effective duration of the capture task, the range is 1 to 720 minutes.

description*description* - Specifies the description information of the packet capture task. The range is 1 to 255 characters.

Default values:

None

Mode:

Packet capture task configuration mode

Guidance:

None.

Example:

```
hostname(config-pkt-task)# task-info pacp-time 20
```

filter-rule

Configure the packet capture rule.

Command:

filter-rule id *id* [**src-ip***ipv4-address/mask* | **src-ipv6***ipv6-address/prefix* | **src-ip-min***min-ipv4***src-ip-max***max-ipv4* | **src-ipv6-min***min-ipv6***src-ipv6-max***max-ipv6* | **user***aaa-server user-name* | **user-group***aaa-server user-name*] [**src-port***port-num*] [**dst-ip***ipv4-address/mask* | **dst-ipv6***ipv6-address/prefix* | **dst-ip-min***min-ipv4***dst-ip-max***max-ipv4* | **dst-ipv6-min***min-ipv6***dst-ipv6-max***max-ipv6* | **url***url*] [**dst-port***port-num*] [**proto** {**tcp** | **udp** | **icmp** | *proto-num*}] [**application***app-name*]

no filter-rule id*id*

Description:

filter-rule id *id* -Specifies the ID of packet capture rule. The range is 1-8.

src-ip*ipv4-address/mask* - Specifies the source IPv4 address and its mask of the packet.

src-ipv6*ipv6-address/prefix* - Specifies the source IPv6 address and its range of the packet.

src-ip-min*min-ipv4***src-ip-max***max-ipv4* - Specifies the source IPv4 range of the packet.

src-ipv6-min*min-ipv6***src-ipv6-max***max-ipv6*- Specifies the source IPv6 range of the packet.

user*aaa-serveruser-name* - Specifies the user of the packet.

user-group*aaa-serveruser-name* - Specifies the user group of the packet.

src-port *port-num* -Specifies the source port number of the packet.

dst-ip*ipv4-address/mask* - Specifies the destination IPv4 address and its mask of the packet.

dst-ipv6*ipv6-address/prefix* - Specifies the destination IPv6 address and its range of the packet.

dst-ip-min*min-ipv4***dst-ip-max***max-ipv4* - Specifies the destination IPv4 range of the packet.

dst-ipv6-min*min-ipv6***dst-ipv6-max***max-ipv6*- Specifies the destination IPv6 range of the packet.

url*url*- Specifies the destination URL of the packet.

dst-port*port-num* -Specifies the destination port number of the packet.

proto {**tcp** | **udp** | **icmp** | *proto-num*} -Specifies the protocol type or the protocol number of the packet.

application*app-name* -Specifies the application type of the packet.

Default values:

any.

Mode:

Packet capture task configuration mode

Guidance:

You can configure this function when the packet capture mode is session mode.

A maximum of 8 packet capture rules can be created in the same packet capture task.

Example:

hostname(config-pkt-task)# **filter-rule id 1 src-ip 1.1.1.1 src-port 23 dst-ip 2.2.2.2 dst-port 23 application http**

For more information, refer to the **Monitor** > **Diagnostic Tool** topic in *StoneOS_CLI_User_Guide*. FR 36021

Configuring the Number of Times of Automatically Detecting ARP Table Entries

WebUI

Configuring the Timeout Detection Times

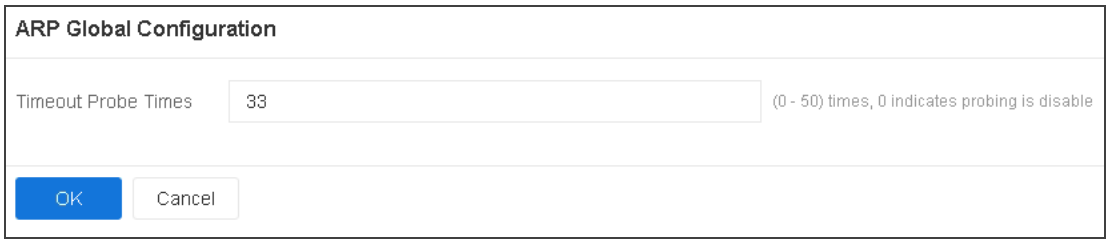
By default, the system automatically detects ARP entries after they have aged. Entries that do not respond within the specified number of detections will be deleted. You can configure the number of detection attempts. Setting the value to 0 disables automatic detection. When disabled, ARP entries will be directly deleted after they have aged.

Notes:

- The configuration applies to ARP entries on all interfaces.
- Non-root VSYS will inherit the configuration from the root VSYS, but this function cannot be configured in non-root VSYS.

To configure the number of times of automatically detecting ARP table entries, take the following steps:

1. Select **Policy** > **ARP Defense** > **Configuration**.



2. In the **Timeout Probe Times** field, enter the number of times of automatic detection. Valid values: 0 to 50. Default value: 33. A value of "0" indicates that automatic detection is disabled.

3. Click **OK**.

For more information, refer to the **Policy** > **ARP Defense** > **Configuring ARP Defense** topic in *StoneOS_WebUI_User_Guide*. FR38671

CLI

IP-MAC Binding

Hillstone devices support IP-MAC binding, MAC-port binding and IP-MAC-port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings. Besides, the Hillstone devices are also designed with the ARP inspection function.

Configuring the Timeout Detection Times

By default, the system automatically detects ARP entries after they have aged. Entries that do not respond within the specified number of detections will be deleted. You can configure the number of detection attempts. Setting the value to 0 disables automatic detection. When disabled, ARP entries will be directly deleted after they have aged.

Notes:

- The configuration applies to ARP entries on all interfaces.
- Non-root VSYS will inherit the configuration from the root VSYS, but this function cannot be configured in non-root VSYS.

To configure the number of times of automatic detection of ARP table entries, in global mode, use the following command:

arp timeout-probe times *times*

- *times* - Specifies the the number of times of automatic detection. Valid values: 0 to 50. Default value: 33. A value of "0" indicates that automatic detection is disabled.

To restore the default value of automatic detection, in global configuration mode, use the following command:

no arp timeout-probe times

Viewing the Number of Times of Automatic Detection of ARP Table Entries

To view the number of times of automatic detection of ARP table entries, in any mode, use the following command:

show arp timeout-probe times

For more information, refer to the **Policy** > **ARP Defense** topic in *StoneOS_CLI_User_Guide*.
FR38671

Supporting to Configure the PIM Passive Mode for the Interface

WebUI

Configuring PIM

The configuration of PIM includes basic configuration and the configuration of PIM-SM on different interfaces.

Notes:

- The PIM-SM function cannot be configured with the static multicast routing function or the IGMP Proxy function at the same time.
- PIM-SSM function is on the basis of the PIM-SM function. Configure PIM-SM mode before configuring the PIM-SSM.
- In HA environment, PIM-SSM only supports Active-Passive (A/P) mode.
- The PIM-SM function can only be enabled on the Layer 3 interface.

To configure PIM, take the following steps:

1. Select **Network** > **Routing** > **PIM**
2. Select a virtual router where the new PIM belongs from the **Virtual Router** drop-down list.
3. Select the **Configuration** tab to specify basic parameters.

   On the Configuration tab, configure the following options.

Option	Description
Multicast	Turn on the switch button to enable global multicast routing.

Option	Description
Route	
PIM-SM	Turn on the switch button to enable PIM-SM.
Candidate RP	Select PIM devices in the PIM-SM domain to configure them as the candidate RP (Rendezvous Point). RP will be elected from the candidates. Candidate BSR should be configured at the same time and BSR will be elected from the candidate BSR (BootStrap Router). BSR is responsible for collecting and distributing RP information in the network. Candidate RP includes the following configuration: • Interface: Select the interface where the candidate RP resides from the drop-down list. The interface must be enabled with PIM-SM. • Interval: Specifies the interval for sending candidate RP messages. The range is 1 to 16,383 seconds. The default value is 60 seconds. • Priority: Specifies the priority. The smaller the value is, the higher the priority will be. In the RP election, the candidate RP with a higher priority will be elected as the RP. The range is 0 to 255 and the default priority is 0. **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is 224.0.0.0/4.

Option	Description
Candidate BSR	In a PIM-SM domain, you need to configure one or more candidate BSRs. BSR will be automatically generated among candidate BSRs. The BSR will collect and distribute the RP information. Candidate BSR includes the following configuration: • Interface: Select the interface where the candidate BSR resides from the drop-down list. The interface must be enabled with PIM-SM • Priority: Specifies the priority. The larger the value is, the higher the priority will be. If there is only one candidate BSR in the PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255 and the default priority is 0. **Notes:** When a dynamic RP is used, the candidate BSR must be configured and at least one candidate BSR must be configured in the PIM-SM domain.
Static RP	When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP to save the bandwidth occupied by frequent message exchange between the Candidate RP and the BSR. In the PIM-SM domain, the static RP configured on all the devices should be the same. Click **New**. Enter the IP address of the interface where the static RP resides in the **Interface IP** textbox and the multicast address in the **Multicast Address** textbox.

Option	Description
RPT to SPT Switchover	Click the switch button to enable RPT to SPT Switchover. Since the RPT (Rendezvous Point Tree) in the PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.
PIM-SSM	By default, PIM-SSM is disabled. Click the switch button to enable PIM-SSM and specify the address range of PIM-SSM multicast group in the **Multicast Group Range** textbox. Ensure that the address range of PIM-SSM group configured on all PIM devices in the network are consistent. By default, the address range of PIM-SSM is 232.0.0.0/8.

4. Click **OK**.
5. To delete configured PIM, select a virtual router from the **Virtual Router** drop-down list. Click Delete PIM to delete PIM configuration in this VR

To configure PIM-SM on interfaces, take the following steps:

1. Select **Network** > **Routing** > **PIM**.
2. Click **Interface Configuration** in the upper-right corner.
3. Double-click the interface or select the check box before the interface and click **Edit**.

Option	Description
Interface	Displays the name of the interface.

Option	Description
PIM-SM	Turn on the switch button to enable PIM-SM.
Passive Mode	Turn on the switch to enable the PIM passive mode of the interface. When the PIM-SM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets. The PIM passive mode is used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding. **Note:** • Before enabling this function, ensure that both the PIM-SM function and multicast routing function are enabled. • This function is only available to the PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment. • After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.

Option	Description
DR Priority	Specifies the priority of DR. The larger the value is , the higher the priority will be. The default value is 1. The value range is 0 to 4,294,967,294. The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). All routers in the PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority is the same, the one with a larger IP address will be selected.
Hello Interval	With PIM-SM enabled, the interface periodically sends Hello packets. You can specify the interval for sending Hello packets on the interface as needed. The value range is 1 to 65,535 seconds. The default value is 30 seconds.
IGMP Query Interval	Specifies the interval for sending IGMP general query messages. The range is 1 to 18,000 seconds, and the default value is 60 seconds. The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain IGMP group membership of the interface. After the PIM-SM function is enabled for the interface, the querier will send IGMP general query messages to learn about the entry and exit of multicast group members.
IGMP Querier Timeout	Specifies the timeout value for IGMP general query. The range is 30 to 300 seconds, and the default value is 120 seconds. If the multicast router in the network does not receive IGMP general query messages within the specified timeout period, multicast

Option	Description
	routers will elect a querier again.
IGMP Query Max Response Time	Specifies the maximum response time for IGMP general query. The range is 1 to 25 seconds, and the default value is 10 seconds. You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the IGMP general query message twice and no response from the receiver host within the specified maximum response time, the system will delete this receiver in the multicast routing table.
Non-direct Multicast Source	Specifies the non-direct multicast source address. The system cannot establish the neighbor relationship with a multicast source as the muticast source DR across different network segments, and the muticast source DR will discard multicast packets whose network segment is different from the ingress interface. Therefore, you can configure the non-direct multicast source address to ensure that the multicast source DR and multicast source multicast across network segments when unicast routing of the multicast source is reachable for all PIM devices within the multicast domain. Click **New** and configure the multicast source address and subnet mask of non-direct multicast source. You can configure at most 10 non-direct multicast source entries. **Note**: Only root-VSYS supports to configure the multicast source address of non-direct multicast source.
Interface joins Multicast	Configures the IGMP Join-group on the interface. This allows the interface of the system to join the multicast group and receive data

Option	Description
Groups	traffic from the multicast group. You can configure at most 100 multicast groups. • IGMPv2: Select "IGMPv2" and configure the multicast group address. This way, the interface will join the specified multicast group over IGMPv2. • IGMPv3: Select "IGMPv3" and configure the multicast group address and multicast source address. This way, the interface will join the specified multicast group over IGMPv3. **Note**: To use the MSR function, you need to configure the IGMP Join-group function on the Vif interface.
Multicast Service Reflection	The MSR function supports to process multicast data forwarded to the Vif interface by converting the source address and multicast group address of the original multicast stream into a new multicast stream. When multicast traffic matches the ingress interface and pre-reflection destination IP address in the MSR entry, it can be converted to the post-reflection destination IP address and source IP address in the MSR entry. You can configure at most 100 MSR entries. To do this, click **New** and configure the following parameters: • Ingress Interface: Select the ingress interface of the original multicast stream from the drop-down list. • Destination IP (Before Reflection): Specifies the multicast group address of the original multicast stream.

Option	Description
	• Destination IP (After Reflection): Specifies the post-reflection multicast group address. • mask (After Reflection): Specifies the post-reflection subnet mask of the multicast group address. • Source IP (After Reflection): Specifies the post-reflection multicast source address, which needs to be in the same network segment as the IP address of the Vif interface. **Note:** • Only root VSYS supports the MSR function. • When you use the MSR function, if unicast route performs route advertisement learning combined with the OSPF protocol, the OSPF network type on the Vif interface needs to be set to **point-to-point**. This allows the neighbor device to learn non-host routes. For more information about how to configure OSPF on the interface, see Configuring OSPF.

4. Click **OK**.

For more information, refer to the **Advanced Routing** > **PIM** topic in *StoneOS WebUI User Guide*. FR 38562

Configuring PIMv6

The configuration of PIMv6 includes basic configuration and the configuration of IPv6 PIM-SM on different interfaces.

Notes:

- To configure PIMv6, the current system version should be IPv6.
- The IPv6 PIM-SM function cannot be configured with the IPv6 static multicast routing function at the same time.
- IPv6 PIM-SM function can only be enabled on the Layer 3 interface.

To configure PIMv6, take the following steps:

1. Select **Network** > **Routing** > **PIMv6**.
2. Select a virtual router where the new PIMv6 belongs from the **Virtual Router** drop-down list.
3. Select the **Configuration** tab to specify basic parameters.

Option	Description
Multicast Route	Turn on the switch button to enable IPv6 global multicast routing.
PIM-SM	Turn on the switch button to enable IPv6 PIM-SM.
Candidate RP	Select PIM devices in the IPv6 PIM-SM domain to configure them as the candidate RP (Rendezvous Point). RP will be elected from the candidates. Candidate BSR should be configured at the same time and BSR will be elected from the candidate BSR (BootStrap Router). BSR is responsible for collecting and distributing RP information in the network. Candidate RP includes the following configuration: • IPv6 Address: Specifies the IPv6 address of the candidate RP interface. The address cannot be the link-local address.

Option	Description
	The interface must be enabled with IPv6 PIM-SM. • Interval: Specifies the interval for sending candidate RP messages. The range is 1 to 16,383 seconds. The default value is 60 seconds. • Priority: Specifies the priority. The smaller the value is, the higher the priority will be. In the RP election, the candidate RP with a higher priority will be elected as the RP. The range is 1 to 192 and the default priority is 192. **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is FF00::/8.
Candidate BSR	In a IPv6 PIM-SM domain, you need to configure one or more candidate BSRs. BSR will be automatically generated amongcandidate BSRs. The BSR will collect and distribute the RP information. Candidate BSR includes the following configuration: • IPv6 Address: Specifies the IPv6 address of the candidate BSR interface. The address cannot be the link-local address. The interface must be enabled with IPv6 PIM-SM. • Priority: Specifies the priority. The larger the value is, the higher the priority will be. If there is only one candidate BSR in the IPv6 PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The

Option	Description
	range is 0 to 255 and the default priority is 0. **Notes:** When a dynamic RP is used, the candidate BSR must be configured and at least one candidate BSR must be configured in the IPv6 PIM-SM domain.
Static RP	When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP to save the bandwidth occupied by frequent message exchange between the Candidate RP and the BSR. In the IPv6 PIM-SM domain, the static RP configured on all the devices should be the same. Click **New**. Enter the IPv6 address of the interface where the static RP resides in the **Interface IP** textbox and the multicast address in the **Multicast Address** textbox.
RPT to SPT Switchover	Click the switch button to enable RPT to SPT Switchover. Since the RPT (Rendezvous Point Tree) in the IPv6 PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.

4. Click **OK**.
5. To delete configured PIMv6, select a virtual router from the **Virtual Router** drop-down list. Click **Delete PIMv6** to delete PIMv6 configuration in this VR.

To configure IPv6 PIM-SM on interfaces, take the following steps:

1. Select **Network** > **Routing** > **PIMv6**.
2. Click **Interface Configuration** in the upper-right corner.
3. Double-click the interface or select the check box before the interface and click **Edit**.

Option	Description
Interface	Displays the name of the interface.
PIM-SM	Turn on the switch button to enable IPv6 PIM-SM.
Passive Mode	Turn on the switch to enable the IPv6 PIM passive mode of the interface. When the IPv6 PIM-SM function is enabled on the interface, if a malicious host simulates IPv6 PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the IPv6 PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any IPv6 PIM packets, all IPv6 PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of MLD packets. **Note:** • efore enabling this function, ensure that both the IPv6 PIM-SM function of the interface and IPv6 multicast routing function are enabled. • This function is only available to the IPv6 PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment.

Option	Description
	• After configuring this function, the interface will no longer receive or forward any IPv6 PIM packets, which indicates that other IPv6 PIM functions configured on the interface will be disabled. Please use this function with caution. • The IPv6 PIM passive mode cannot be used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding.
DR Priority	Specifies the priority of DR. The larger the value is , the higher the priority will be. The default value is 1. The value range is 0 to 4,294,967,294. The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). All routers in the IPv6 PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority is the same, the one with a larger IP address will be selected.
Hello Interval	With IPv6 PIM-SM enabled, the interface periodically sends Hello packets. You can specify the interval for sending Hello packets on the interface as needed. The value range is 1 to 3600 seconds. The default value is 30 seconds.
MLD Query Interval	Specifies the interval for sending MLD general query messages. The range is 1 to 1,800 seconds, and the default value is 125 seconds. The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a

Option	Description
	router as the querier automatically to maintain MLD group membership of the interface. After the IPv6 PIM-SM function is enabled for the interface, the querier will send MLD host query messages to learn about the entry and exit of multicast group members.
MLD Querier Timeout	Specifies the timeout value for MLD querier. The range is 3 to 3,620 seconds, and the default value is 260 seconds. If the multicast router in the network does not receive MLD query messages within the specified timeout period, multicast routers will elect a querier again.
MLD Query Max Response Time	Specifies the maximum response time for MLD general query. The range is 1 to 32 seconds, and the default value is 10 seconds. You can specify the maximum response time after the receiver host receives the general query message. If no response from the receiver host within the specified maximum response time, the system will delete this receiver in the multicast routing table.

4. Click **OK**.

For more information, refer to the **Advanced Routing** > **PIMv6** topic in *StoneOS WebUI User Guide*. FR 38562

CLI

Configuring the PIM Passive Mode of the Interface

When the PIM-SM function is enabled on the interface, if a malicious host simulates PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the PIM passive mode can be enabled on the interface. Once enabled, the interface will no

longer receive or forward any PIM packets, all PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of IGMP packets.

The PIM passive mode is used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding.

Before you start

Before you configure the PIM passive mode of the interface, complete the following tasks:

- In interface configuration mode, use the **ip pim sparse-mode** command to enable the PIM-SM function of the interface.
- In VRouter configuration mode, use the **ip multicast-routing** command to enable the multicast routing function.

Notes

- This function is only available to the PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment.
- After configuring this function, the interface will no longer receive or forward any PIM packets, which indicates that other PIM functions configured on the interface will be disabled. Please use this function with caution.

Procedure

By default, the PIM passive mode of the interface is disabled. To enable this mode, in interface configuration mode, use the following command:

ip pim passive

To disable this mode, in interface configuration mode, use the following command:

no ip pim passive

Check configuration results

After you configure the PIM passive mode of the interface, in interface configuration mode, you can use the **show this** command to view whether the configuration is successful.

Sample response:

```
hostname(config-if-eth0/3)#show this
interface ethernet0/3
ip pim passive
exit
```

Configuring the IPv6 PIM Passive Mode of the Interface

When the IPv6 PIM-SM function is enabled on the interface, if a malicious host simulates IPv6 PIM Hello packets and sends a large number of them, it could cause the device to crash. To avoid this security issue, the IPv6 PIM passive mode can be enabled on the interface. Once enabled, the interface will no longer receive or forward any IPv6 PIM packets, all IPv6 PIM neighbors on the interface will be deleted, and the interface will automatically become the DR. Enabling PIM passive mode on the interface will not affect its processing of MLD packets.

Before you start

Before you configure the IPv6 PIM passive mode of the interface, complete the following tasks:

- In interface configuration mode, use the **ipv6 pim sparse-mode** command to enable the IPv6 PIM-SM function of the interface.
- In VRouter configuration mode, use the **ipv6 multicast-routing** command to enable the multicast routing function.

Notes

- This function is only available to the IPv6 PIM device interface directly connected to the user host segment, and only one PIM device can be connected to the segment.
- After configuring this function, the interface will no longer receive or forward any IPv6 PIM packets, which indicates that other IPv6 PIM functions configured on the interface will be disabled. Please use this function with caution.

- The IPv6 PIM passive mode cannot be used in conjunction with Interface joins Multicast Groups to control multicast traffic forwarding.

Procedure

By default, the IPv6 PIM passive mode of the interface is disabled. To enable this mode, in interface configuration mode, use the following command:

ipv6 pim passive

To disable this mode, in interface configuration mode, use the following command:

no ipv6 pim passive

Check configuration results

After you configure the PIM passive mode of the interface, in interface configuration mode, you can use the **show this** command to view whether the configuration is successful.

Sample response:

```
hostname(config-if-eth0/3)#show this
interface ethernet0/3
ip pim passive
exit
```

Adding Multicast Router Interface to Multicast Group

In a multicast environment, multicast receivers indicate their interest of receiving multicast data by sending an IGMP report to the routers in the network. The routers are then responsible for delivering the data from the source to the receivers. However, if the routers do not connect to multicast receivers or the connected multicast receivers cannot send an IGMP report, data from the source fails to reach the routers. To solve this issue, you can add the interface of multicast routers to the multicast group by configuring join-group. The interface can be added to a specified multicast group based on the IGMPv2 protocol or IGMPv3 protocol.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv2, run the following command in the interface configuration mode:

ip pim igmp join-group*group-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv2 protocol.

In the interface configuration mode, run the **no ip pim igmp join-group***group-address* command to remove the interface from the specified multicast group.

To set the type of protocol based on which the interface is added to a specified multicast group to IGMPv3, run the following command in the interface configuration mode:

ip pim igmpv3 join-group*group-addresssource-address*

- *group-address* - Specifies the IP address of the multicast group to which the interface is added based on the IGMPv3 protocol.
- *source-address* - Specifies the IP address of multicast source data traffic that the interface receives.

In the interface configuration mode, run the **no ip pim igmp join-group***group-addresssource-address* command to remove the interface from the specified multicast group.

Notes:

- Only layer-3 interfaces can be added to the multicast group.
- To add an interface to the multicast group, the following requirements need to be met:
  - The PIM-SM function is enabled for the interface. For more information, refer to Enabling/Disabling the PIM-SM for Interfaces.
  - The device where the interface resides is receiver DR and has the highest priority. For more information about how to configure the priority of DR, refer to Configuring the Priority of DR.
  - The PIM-SM function is also enabled for the upstream device of the device where the interface resides.

For more information, refer to the **Routing** > **PIM** topic in *StoneOS CLI User Guide*. FR 38562

Optimizing Docker Management

CLI

Docker Management

Docker is an open-source platform that allows developers to package applications and their dependencies into lightweight, portable containers. By utilizing containerization, Docker enables developers to isolate applications, eliminate environment inconsistencies, and streamline the deployment process.

StoneOS supports the Docker management function. By using this function, you can create a Docker, allocate system resources in the system, import Docker image files, and run container applications based on Docker.

Device Supported: :

- A-series devices (except A2200/A1800/A1600/A200/A200G4B/A200W) support the Docker management function.
- CloudEdge whose software version is StoneOS 5.5R10F6 and later F versions support the Docker management function.

Docker Management Functions

You can perform the following operations about Docker management:

- Creating a Docker
- Allocating Resources for Docker
- Specifying Access Interfaces

- Managing Image Files
- Managing Containers
- Docker Global Configuration
- Viewing Information about Docker
- Viewing Docker Global Configuration
- Viewing Occupied Storage of Docker

Viewing Occupied Storage of Docker

When the memory occupied by Docker files exceeds the threshold, the device will stop running the container. In any mode, use the following command to view occupied storage of Docker:

show docker-info

Example:

```
hostname# show docker-info
Storage Limit of containers:
threshold : 1374MB
current used : 0MB(0.0%)
Total size of user imported image files: 0MB
```

For more information, refer to the **System Management** > **Docker Management** topic in *StoneOS_CLI_User_Guide*. FR38556

Log

ID:	0x44f40404
Type:	Event
Severity:	Warnings
Message:	Storage used by docker exceeds 90 percent of threshold *storage-*

	threshold MB, please clean unused files in container, if used storage exceeds threshold, system may stop container to recycle storage.
Description:	The storage used by Docker exceeds 90% of the threshold. Please clean unused files in the container, if the used storage exceeds the threshold, the system may stop container to recycle storage.
Solution:	N/A

ID:	0x44f40205
Type:	Event
Severity:	Critical
Message:	Alarm! Storage used by docker exceeds threshold *storage-threshold* MB, system will stop container of docker *docker-name* to recycle storage.
Description:	Alarm! The storage used by Docker exceeds the threshold, and the system will stop the container of docker *docker-name* to recycle storage.
Solution:	Clear unused files in the container.

ID:	0x44f40206
Type:	Event
Severity:	Critical
Message:	Alarm! Storage used by docker exceeds threshold *storage-threshold* MB, please clean unused files in container, if storage keeps increasing, system may run in fault.
Description:	Alarm! The storage used by Docker exceeds the threshold. Please clean unused files in the container. If the storage keeps increasing, the system may fail.

Solution:	Clear unused files in the container.

For more information, refer to the **Docker_ agent** topic in *StoneOS Log Messages Reference Guide*. FR38556

Support to Retrieve the Total Number of Session Resource Allocation Failures for the Entire Device by Using the SNMP

MIB

HILLSTONE-SYSTEM-MIB

The following tables is the parsing results of HILLSTONE-SYSTEM-MIB.

Name	OID	Value
sysSerialNumber	.1.3.6.1.4.1.28557.2.2.1.1	Data type: String Description: Product serial number
sysSoftware	.1.3.6.1.4.1.28557.2.2.1.2	Data type: String Description: Software version
sysCPU	.1.3.6.1.4.1.28557.2.2.1.3	Data type: Integer Description: CPU utilization
sysTotalMemory	.1.3.6.1.4.1.28557.2.2.1.4	Data type:

Name	OID	Value
		Gauge32 Description: Total memory
sysCurMemory	.1.3.6.1.4.1.28557.2.2.1.5	Data type: Gauge32 Description: Used memory
sysTotalSession	.1.3.6.1.4.1.28557.2.2.1.6	Data type: Counter Description: Maximum session number of the system
sysCurSession	.1.3.6.1.4.1.28557.2.2.1.7	Data type: Gauge32 Description: Active session number
sysHAStatus	.1.3.6.1.4.1.28557.2.2.1.8	Data type: Integer Description: HA status • 0 - Invalid • 1 - Started • 2 - Hello

Name	OID	Value
		• 3 - Backup device • 4 - Primary device • 15 - Failure
sysSnmpStackStatus	.1.3.6.1.4.1.28557.2.2.1.9	Data type: Integer Description: SNMP running status
sysTr069StackStatus	.1.3.6.1.4.1.28557.2.2.1.10	Data type: Integer Description: TR069 running status
sysVedorOUI	.1.3.6.1.4.1.28557.2.2.1.11	Data type: String Description: Provider name
sysLogStackStatus	.1.3.6.1.4.1.28557.2.2.1.12	Data type: Integer Description: Syslog running status
sysLogServerAddress1	.1.3.6.1.4.1.28557.2.2.1.13	Data type: String

Name	OID	Value
		Description: Syslog server IP address 1
sysLogServerAddress2	.1.3.6.1.4.1.28557.2.2.1.14	Data type: String Description: Syslog server IP address 2
sysDeviceReloadAction	.1.3.6.1.4.1.28557.2.2.1.15	Data type: Integer Data type: String Description: Device reloading. When the value equals 2, the device will reboot.
sysStatisticsPeriod	.1.3.6.1.4.1.28557.2.2.1.16	Data type: Integer Description: Statistic interval. Default value is 24 hours.
sysMemRatio	.1.3.6.1.4.1.28557.2.2.1.17	Data type: Gauge32 Description:

Name	OID	Value
		Memory usage ratio.
sysSessionRampupRate	.1.3.6.1.4.1.28557.2.2.1.18	Data type: Gauge32 Description: New session connection ratio(used for Statistics).
sysOverallThroughput	.1.3.6.1.4.1.28557.2.2.1.19	Data type: Counter64 Description: Root VSYS throughput.
sysCTWapStat	.1.3.6.1.4.1.28557.2.2.1.20	Data type: String Description: WAP status information
sysRamupRate	.1.3.6.1.4.1.28557.2.2.1.21	Data type: Integer Description: New session connection ratio(not related to Statistics).
sysL4SynCheckDrop	.1.3.6.1.4.1.28557.2.2.1.22	Data type:

Name	OID	Value
		Integer Description: Number of the dropped packets during TCP snchronous message error
sys L4SynBitCheckDrop	.1.3.6.1.4.1.28557.2.2.1.23	Data type: Integer Description: Number of the dropped packets during syc bit of TCP message error
sysL4SeqCheckDrop	.1.3.6.1.4.1.28557.2.2.1.24	Data type: Integer Description: Number of the dropped packets during serial number error
sysL4HwCPUError	.1.3.6.1.4.1.28557.2.2.1.25	Data type: Integer Description: Number of the dropped pack-

Name	OID	Value
		ets during Octeon chip error
sysHistoryMaxSessNum	.1.3.6.1.4.1.28557.2.2.1.26	Data type: Gauge32 Description: Maximum number of sessions in history.
sysTCPSessNum	.1.3.6.1.4.1.28557.2.2.1.27	Data type: Gauge32 Description: Number of current TCP sessions.
sysUDPSessNum	.1.3.6.1.4.1.28557.2.2.1.28	Data type: Gauge32 Description: Number of current UDP sessions.
sysICMPSessNum	.1.3.6.1.4.1.28557.2.2.1.29	Data type: Gauge32 Description: Number of current ICMP sessions.

Name	OID	Value
sysCurSessionIPv4	.1.3.6.1.4.1.28557.2.2.1.31	Data type: Gauge32 Description: Total number of concurrent IPv4 sessions
sysCurSessionIPv6	.1.3.6.1.4.1.28557.2.2.1.32	Data type: Gauge32 Description: Total number of concurrent IPv6 sessions
sysRampupRateIPv4	.1.3.6.1.4.1.28557.2.2.1.33	Data type: Integer Description: Total rate of new IPv4 sessions
sysRampupRateIPv6	.1.3.6.1.4.1.28557.2.2.1.34	Data type: Integer Description: Total rate of new IPv6 sessions
sysPeerHAStatus	.1.3.6.1.4.1.28557.2.2.1.36	Data type: Integer Description: HA

Name	OID	Value
		status of the peer device • 0 - none • 1 - init • 2 - hello • 3 - backup • 4 - master • 15 – failed
sysHAGroupStatus	.1.3.6.1.4.1.28557.2.2.1.37	Data type: Integer Description: HA status of the master device and backup device in the HA group • 0 - normal • 1 - abnormal
sysHAStatusChangeTimes	.1.3.6.1.4.1.28557.2.2.1.38	Data type: Integer Description:

Name	OID	Value
		Number of master/backup status changes in the HA group
sysOverallIPv4Throughput	.1.3.6.1.4.1.28557.2.2.1.39	Data type: Counter64 Description: IPv4 throughout of root VSYS
sysOverallIPv6Throughput	.1.3.6.1.4.1.28557.2.2.1.40	Data type: Counter64 Description: IPv6 throughout of root VSYS
sysAllocFailedSessNum	.1.3.6.1.4.1.28557.2.2.1.41	Data type: Gauge32 Description: Total number of failed attempts to allocate session resources when establishing new sessions on the device.

Name	OID	Value
sysCurSessionNat	.1.3.6.1.4.1.28557.2.2.1.42	Data type: Gauge32 Description: Number of concurrent connections of current NAT sessions
sysRampupRateNat	.1.3.6.1.4.1.28557.2.2.1.43	Data type: Gauge32 Description: New connection rate of current NAT sessions
sysTopAppthroughputTable: Throughput information of the TOP application		
hillstoneAppIndex	.1.3.6.1.4.1.28557.2.2.1.30.1.1	Data type: Integer Description: The index of the TOP 10 Application.
hillstoneAppthroughput	.1.3.6.1.4.1.28557.2.2.1.30.1.2	Data type: DisplayString Description: The throughput of the

Name	OID	Value
		TOP 10 application in last 24 hours.
sysPendingSessionQueueFullDrop	.1.3.6.1.4.1.28557.2.2.1.35	Data type: Integer Description: Number of packets dropped caused by full cache queue of sessions.

For more information about the private MIB, refer to *StoneOS SNMP MIB Reference Guide*. FR 33389