Hillstone Networks

StoneOS WebUI Guide - E-Pro Series

Version 5.5R8

TechDocs | docs.hillstonenet.com

Contact Information:

US Headquarters:

Hillstone Networks
5201 Great America Pkwy, #420
Santa Clara, CA 95054
Phone: 1-408-508-6750
https://www.hillstonenet.com/about-us/contact/

About this Guide:

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

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

To provide feedback on the documentation, please write to us at: TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-WUG-UNI-E-Pro-5.5R8-EN-V1.0-5/31/2021

Contents

Welcome

Thanks for choosing Hillstone products!

This part introduces how you get user guides of Hillstone products.

Getting Started Guide:

- Getting Started Guide (Download PDF)

Cookbook (recipes):

- StoneOS 5.5 Cookbook (Download PDF)

OS Operation Guides:

- StoneOS Command Line Interface User Guide (Download PDF)
- StoneOS WebUI User Guide (Download PDF)
- StoneOS Log Messages Reference Guide (Download PDF)
- StoneOS SNMP Private MIB Reference Guide (Download PDF)
- StoneOS Addendum Book for P Releases (Download PDF)

Hardware Installation Guides:

- Hardware Reference Guide of all series platforms (Download PDF)
- Expansion Modules Reference Guide of all modules (Download PDF)

Other Support Links:

- Webiste: https://www.hillstonenet.com
- Download Documentations:https://docs.hillstonenet.com
- Technical Support: 1-800-889-9860

Chapter 1 Getting Started Guide

This guide helps you go through the initial configuration and the basic set-up of your Hillstone device. The intended reader is your company's network administrator.

This guide is used when you have finished mounting your device. After following the steps in this guide, your private network will be able to access the Internet. To set up security functions, you will need to read the User Guide (WebUI User Guide or CLI User Guide).

You may configure your firewall in the following sequence:

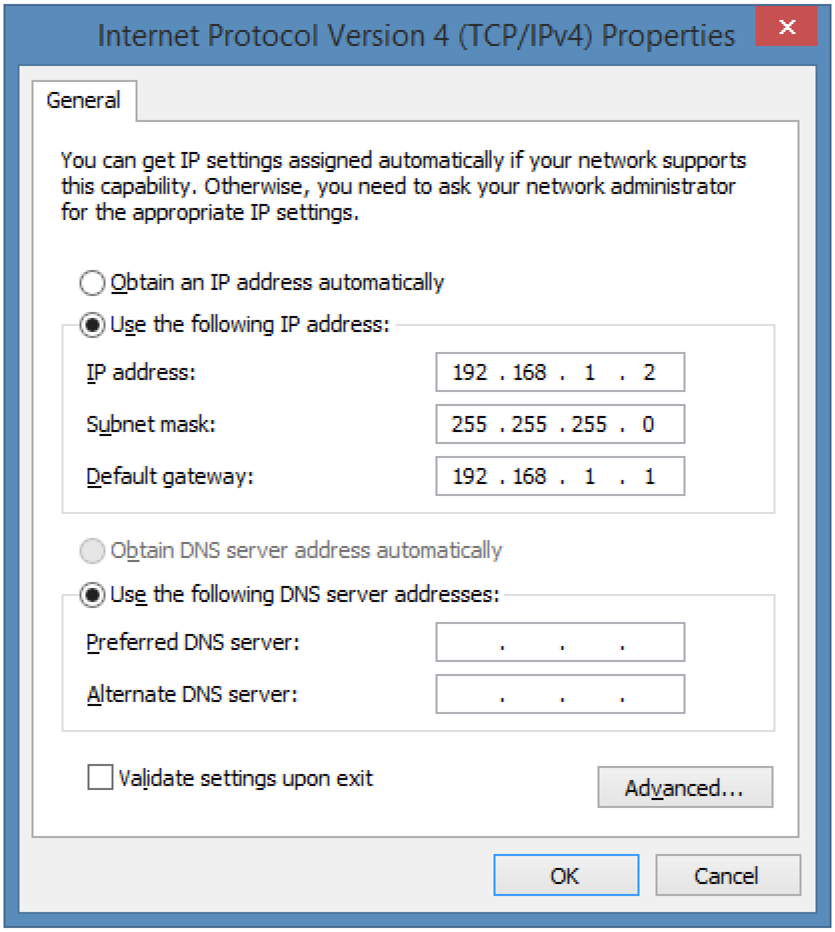
1. "Initial Visit to Web Interface" on Page 4
2. "Preparing the StoneOS System" on Page 6, including:
    - "Installing Licenses" on Page 6
    - "Creating a System Administrator" on Page 6
    - "Adding Trust Hosts" on Page 8
    - "Upgrading StoneOS Firmware" on Page 9
    - "Updating Signature Database" on Page 9
3. "Connecting to Internet Under Routing Mode" on Page 11
4. "Restoring Factory Settings" on Page 19

Initial Visit to Web Interface

Interface eth0/0 is configured with IP address 192.168.1.1/24 by default and it is open to SSH、PING、SNMP、HTTP connection types(except for some custom versions). For the initial visit, use this interface.

To visit the web interface for the first time, take the following steps:

1. Go to your computer's Ethernet properties and set the IPv4 protocol as below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

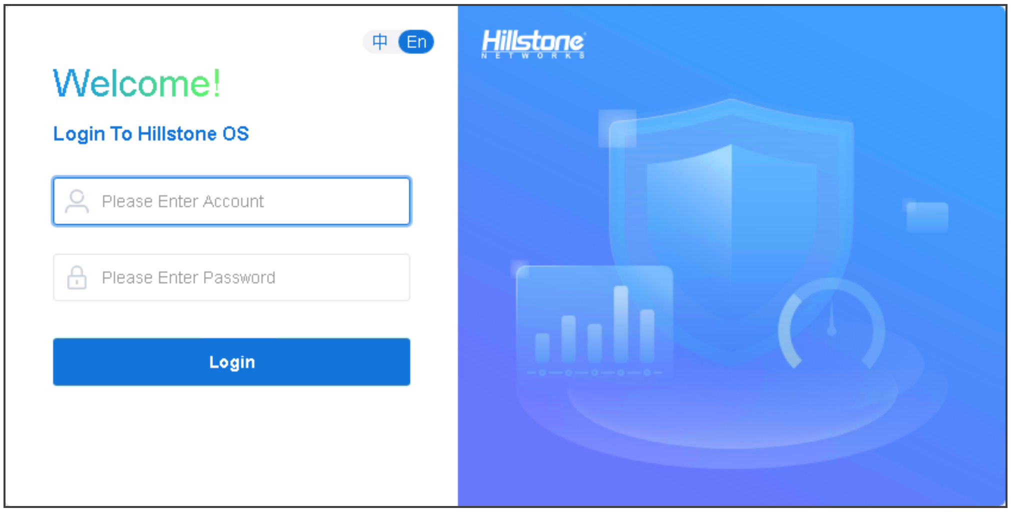
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2. Connect an RJ-45 Ethernet cable from your computer to the eth0/0 of the device.

3. In your browser's address bar, type "http://192.168.1.1" and press **Enter**.



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

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

6. Click **Login**, and the device's system will initiate.

Preparing the StoneOS System

Installing Licenses

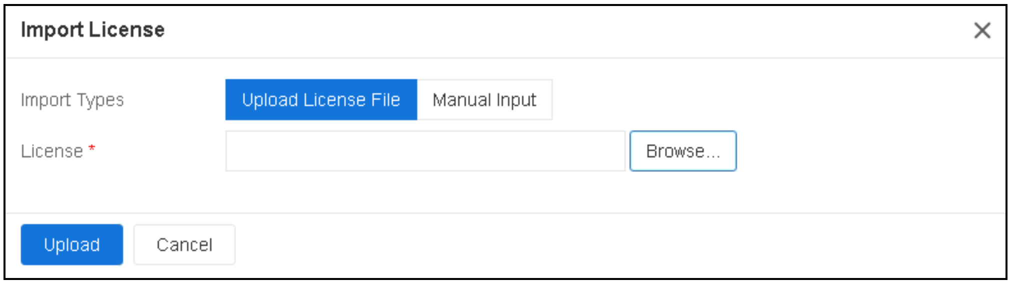
Licenses control features and performance.

Before installing any license, you must purchase a license code.

To install a license, take the following steps:

1. Go to **System** > **License**.

   Click Import to open Import License page.Choose one of the three ways to import a license:

2. 

   - **Upload License File:** Select the radio button, click **Browse**, and select the license file (a .txt file).
   - **Manual Input**: Select the radio button, and paste the license code into the text box.

3. Click **OK**.

4. To make the license take effect, reboot the system. Go to **System** > **Device Management** > **Options**, and click **Reboot**.

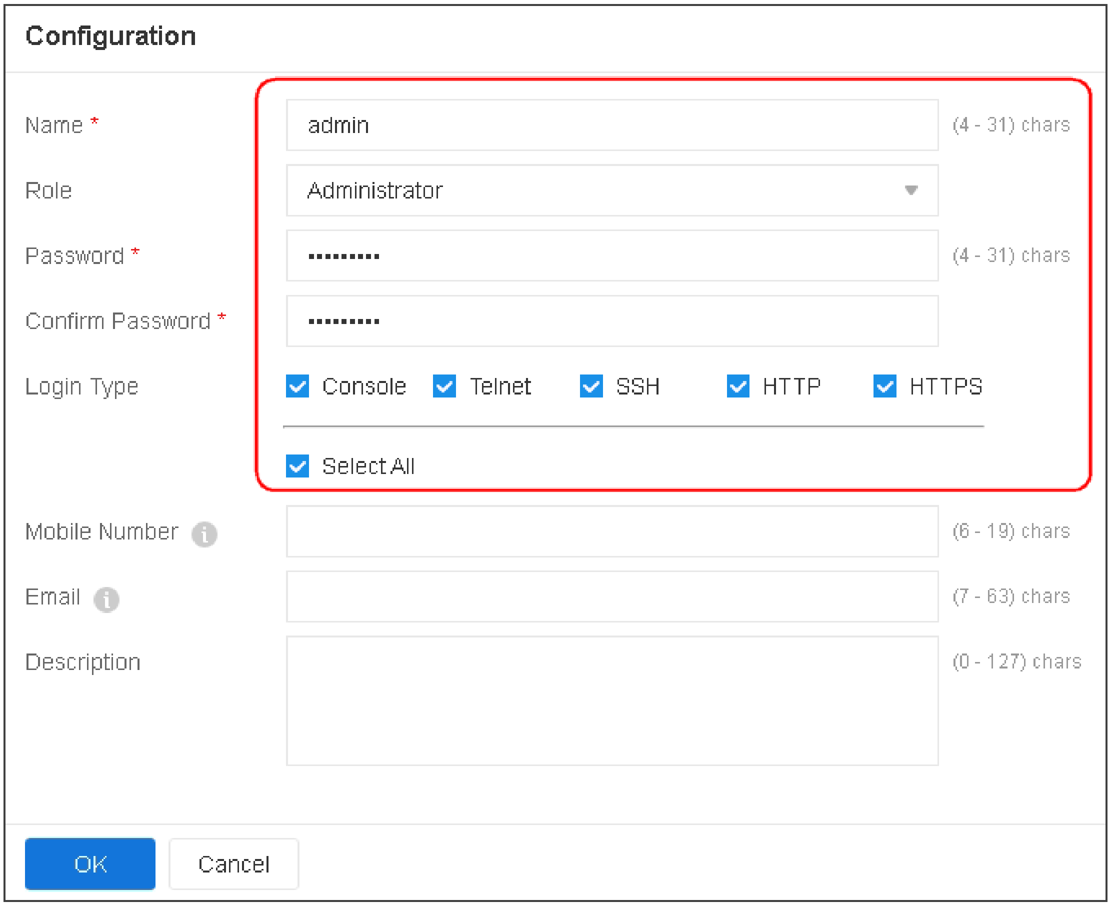
Creating a System Administrator

System administrator has the authority to read, write and execute all the features in system.

To create a system administrator, take the following steps:

1. Go to **System > Device Management > Administrator.**

2. Click **New.**



Configuration

Name * admin (4 - 31) chars

Role Administrator

Password * •••••••••• (4 - 31) chars

Confirm Password * ••••••••••

Login Type ☑ Console ☑ Telnet ☑ SSH ☑ HTTP ☑ HTTPS

☑ Select All

Mobile Number (6 - 19) chars

Email (7 - 63) chars

Description (0 - 127) chars

In the Admin Configuration dialog box, enter values

Option	Value
Name	Admin
Role	Administrator
Password	123456
Confirm Password	123456

Option	Value
Login Type	Select **Telnet**, **SSH**, **HTTP**and **HTTPS**.

3. Click **OK**.

Notes: The system has a default administrator "hillstone" , which cannot be deleted or renamed.

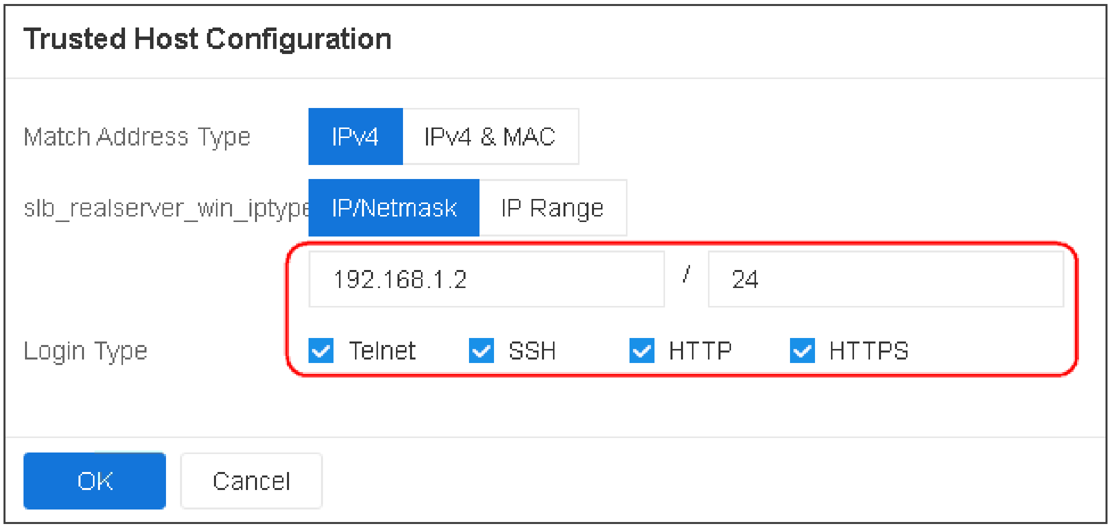
Adding Trust Hosts

The trust host is administrator's host. Only computers included in the trust hosts can manage system.

To add a trust host, take the following steps:

1. Go to **System > Device Management**.

2. Select **Trusted Host** tab, and click **New**.



Trusted Host Configuration

Match Address Type: IPv4 | IPv4 & MAC

slb_realserver_win_iptype: IP/Netmask | IP Range

192.168.1.2 / 24

Login Type: ☑ Telnet ☑ SSH ☑ HTTP ☑ HTTPS

In the Trust Host Configuration dialog box, enter value

Option	Value
Type	Select **IP/Netmask**
IP	192.168.1.2/24
Login Type	Select all: Telnet, SSH, HTTP and HTTPS

3. Click **OK**.

Upgrading StoneOS Firmware

Notes: Back up your configuration files before upgrading your system.

To upgrade your system firmware, take the following steps:

1. Go to **System > Upgrade Management**.
2. Select **Browse** and choose the new image from your local computer.
3. Click **Reboot to make new firmware take effect**, then click **Apply**.
4. System will automatically reboot when it finishes installing the new firmware.

Updating Signature Database

Features that require constant updates of signature are license controlled. You must purchase the license in order to be able to update the signature libraries. By default, the system will automatically update the databases daily.

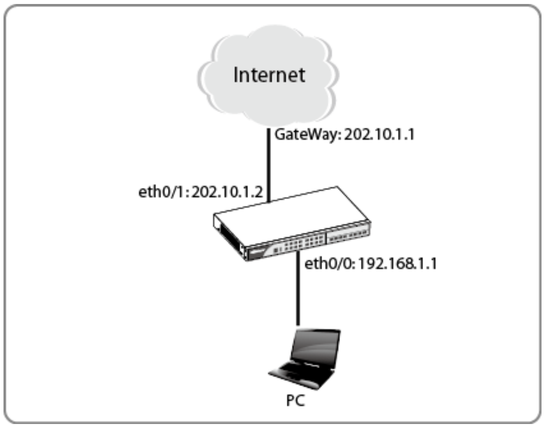
Toupdate a database, take the following steps:

1. Go to **System > Upgrade Management**, and click the <Signature Database Update> tab.
2. **Find your intended database, and choose one of the following two ways to upgrade.**
   - **Remote Update**: Click **Update** , and system will automatically update the database.

- **Local Update**: Select **Browse** to open the file explorer, and select your local signature file to import it into system.

Connecting to Internet Under Routing Mode

In routing mode, the device is working as a gateway and router between two networks. This section shows how to connect and configure a new Hillstone device in routing mode to securely connect the private network to the Internet.



To get your private network access to Internet through a Hillstone device, take the following steps:

Step 1: Connecting to the device

1. Connect one port (e.g. eth0/1) of Hillstone device to your ISP network. In this way, "eth0/1" is in the untrust zone.

2. Connect your internal network to another Ethernet interfaces (e.g. eth0/0) of the device. This means "eth0/0" is connected to the trust zone.

3. Power on the Hillstone device and your PCs.

4. If one of the internal interfaces already has been configured with an IP address, use a browser to visit that address from one of your internal PCs.

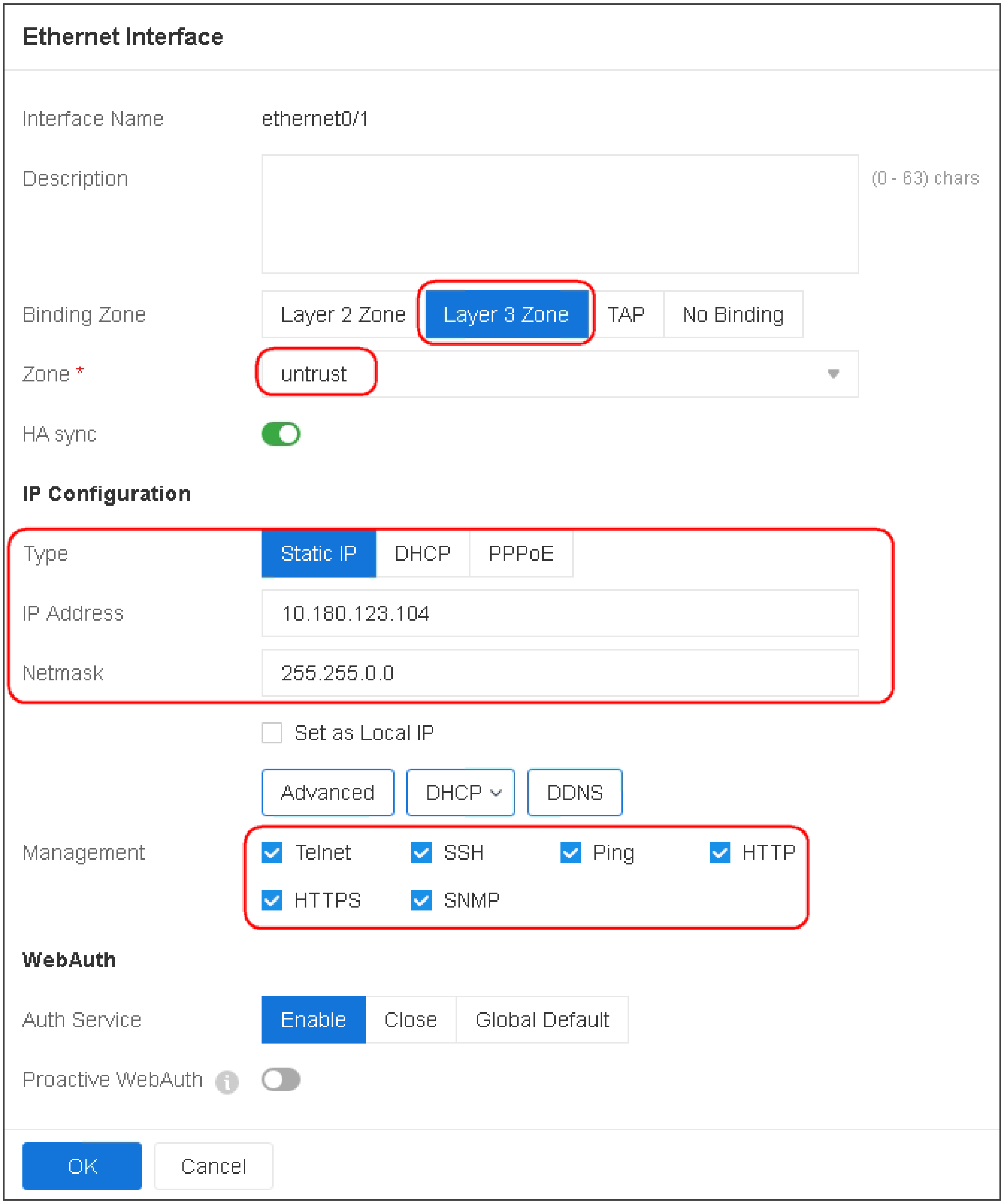
   If it is a new device, use the methods in "Initial Visit to Web Interface" on Page 4 to visit.

5. Enter "hillstone" for both the username and the password.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.

2. Double click **ethernet0/1**.



Ethernet Interface

Interface Name: ethernet0/1

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone | [✓ Layer 3 Zone] | TAP | No Binding

Zone *: untrust

HA sync: ●

IP Configuration

Type: [✓ Static IP] | DHCP | PPPoE

IP Address: 10.180.123.104

Netmask: 255.255.0.0

□ Set as Local IP

Management: ☑ Telnet ☑ SSH ☑ Ping ☑ HTTP ☑ HTTPS ☑ SNMP

WebAuth

Auth Service: [✓ Enable] | Close | Global Default

Proactive WebAuth: ○

In the Ethernet Interface dialog box, enter values

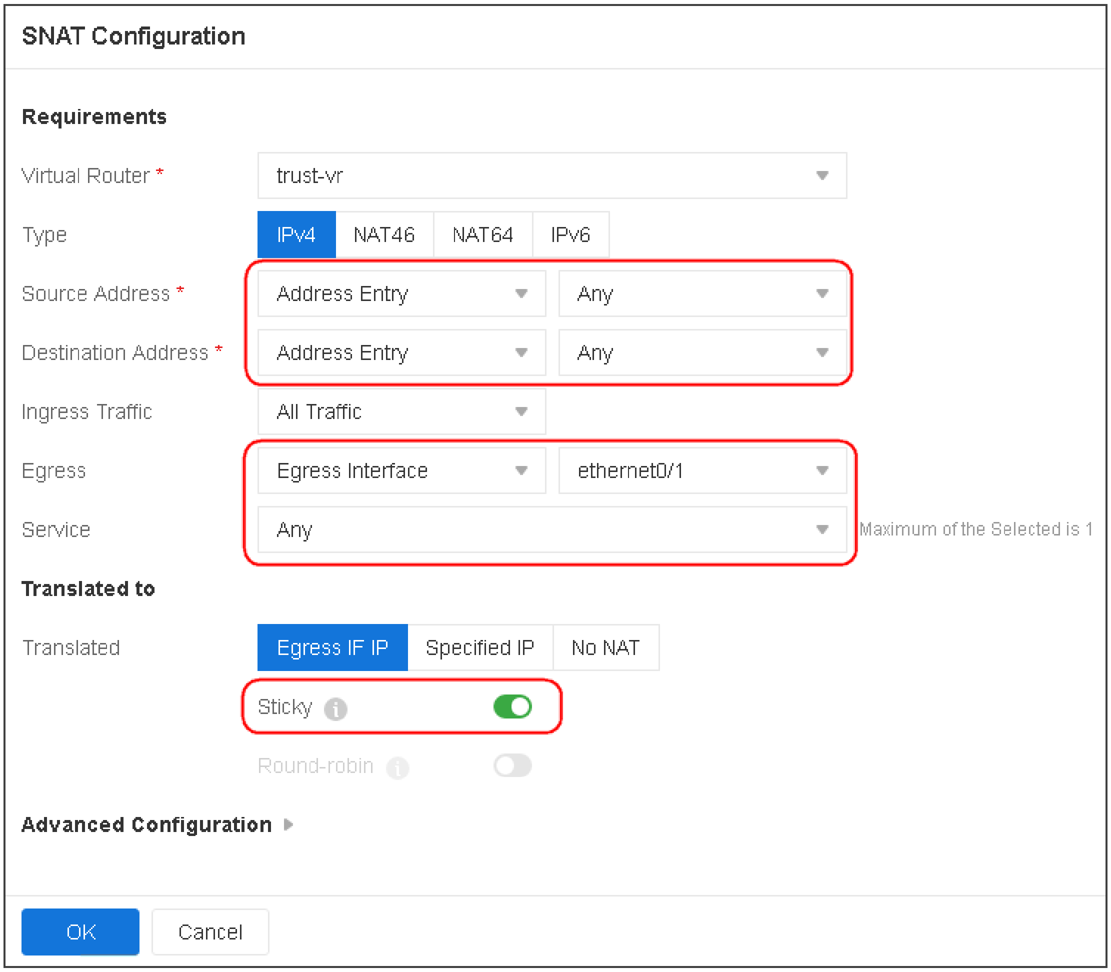
Option	Value
Binding Zone	L3-zone
Zone	untrust
Type	Static IP
IP Address	202.10.1.2 (public IP address provided by your ISP)
Netmask	255.255.255.0
Management	Select protocols that you want to use to access the device.

3. Click **OK**.

Step 3: Creating a NAT rule to translate internal IP to public IP

1. Go to **Policy** > **NAT** > **SNAT**.

2. Click **New**



SNAT Configuration

Requirements

Virtual Router * trust-vr

Type IPv4 | NAT46 | NAT64 | IPv6

Source Address * Address Entry | Any

Destination Address * Address Entry | Any

Ingress Traffic All Traffic

Egress Egress Interface | ethernet0/1

Service Any — Maximum of the Selected is 1

Translated to

Translated Egress IF IP | Specified IP | No NAT

Sticky ●

Round-robin ○

Advanced Configuration ▸

In the SNAT Configuration dialog box, enter values

Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any

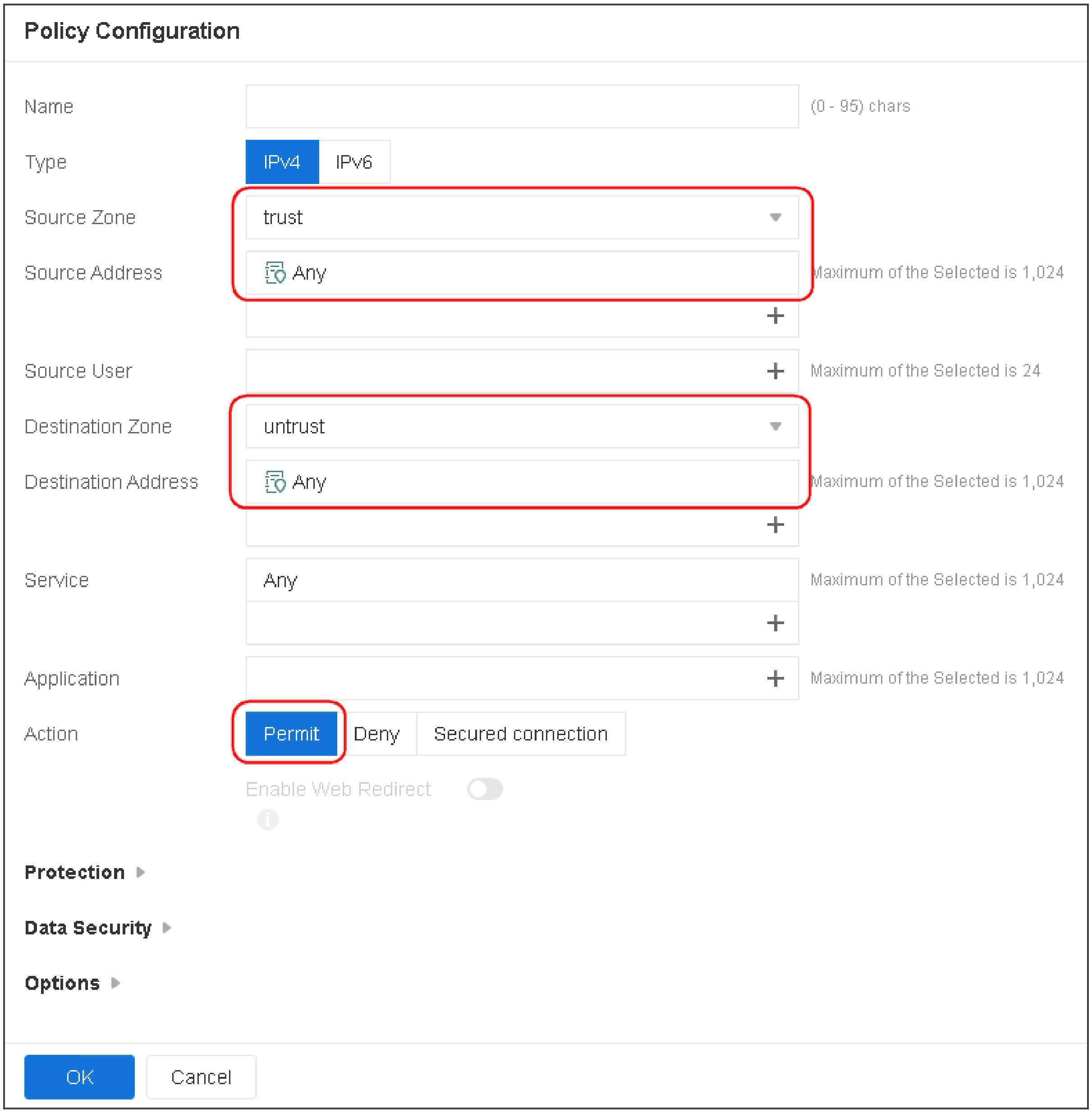
Option	Value
Egress	Egress interface, ethernet 0/1
Translated	Egress IP
Sticky	Enable

3. Click **OK**.

Step 4: Creating a security policy to allow internal users access Internet.

1. Go to **Policy > Security Policy>Policy**.

2. Click **New**,select **Policy** from the drop-down list.



Policy Configuration

Name (0 - 95) chars

Type: IPv4 IPv6

Source Zone: trust

Source Address: Any — Maximum of the Selected is 1,024

Source User — Maximum of the Selected is 24

Destination Zone: untrust

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application — Maximum of the Selected is 1,024

Action: Permit Deny Secured connection

Enable Web Redirect

In the Policy Configuration dialog box, enter values.

Source Information	
Zone	trust
Address	Any

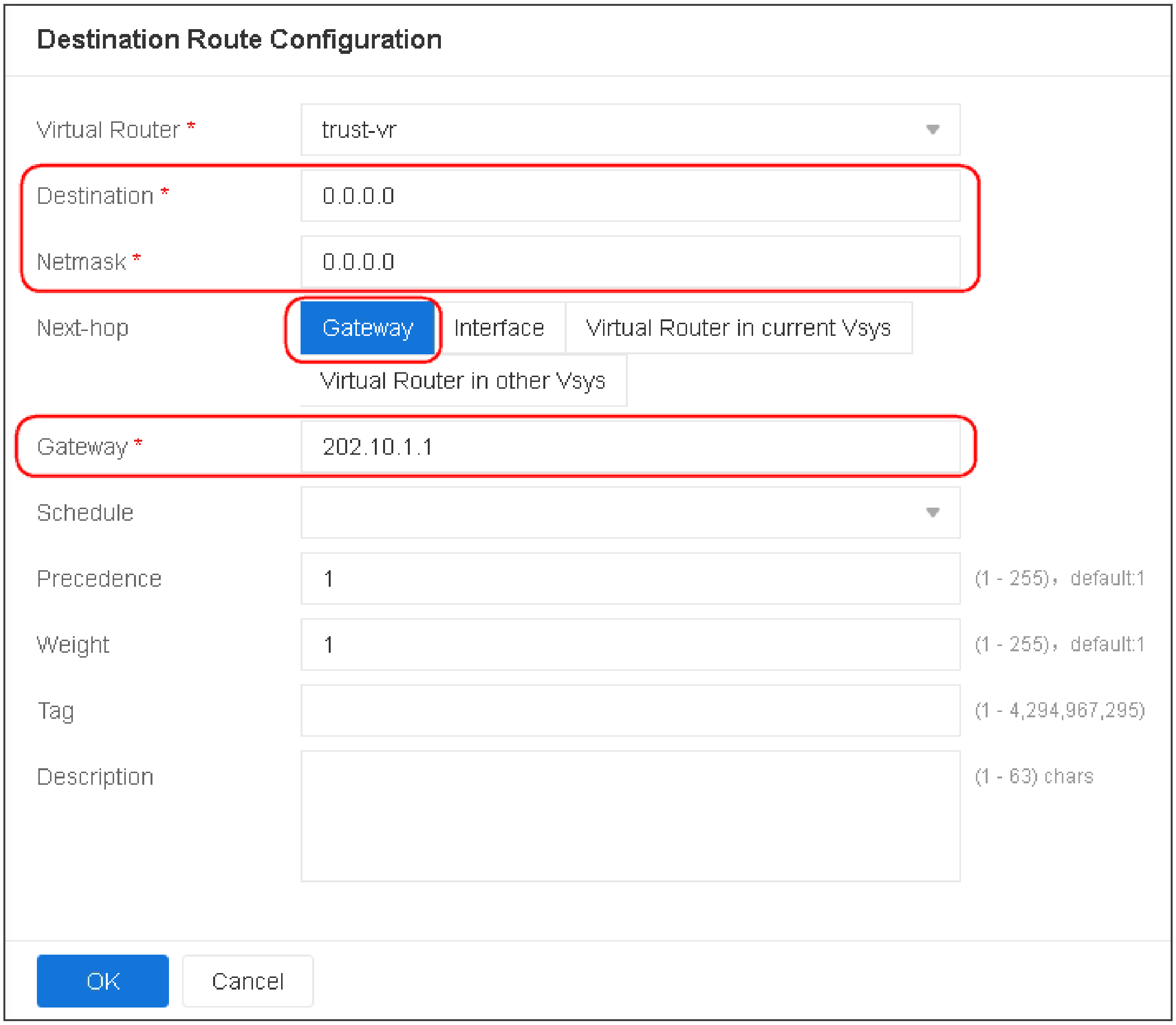
Destination Information	
Zone	untrust
Address	Any
Other Information	
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click OK.

Step 5: Configuring a default route

1. Go to **Network >Routing > Destination Route**.

2. Click **New**.



Destination Route Configuration

Virtual Router *	trust-vr	
Destination *	0.0.0.0	
Netmask *	0.0.0.0	
Next-hop	Gateway / Interface / Virtual Router in current Vsys / Virtual Router in other Vsys	
Gateway *	202.10.1.1	
Schedule		
Precedence	1	(1 - 255)，default:1
Weight	1	(1 - 255)，default:1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0 (means all network)
Subnet Mask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

3. Click **OK**.

Restoring Factory Settings

Notes: Resetting your device will erase all configurations, including the settings that have been saved. Please be cautious!

To restore the factory default settings, use one of the following ways:

- "Restoring using a pin" on Page 19
- "Restoring via WebUI" on Page 20

Restoring using a pin

To restore factory default settings using a pin, take the following steps:

Model	Step
SG-6000- C4000、SG-6000-C3100、SG-6000-C3000、SG-6000-C2100、SG-6000-C2000、SG-6000-C1500、SG-6000-C1300、SG-6000-C1200W、SG-6000-C1000、SG-6000-C600 SG-6000- E5960、SG-6000-E5760、SG-6000-E5660、SG-6000-E2800、SG-6000-E2800-GM、SG-6000-E2300、E2300-GM、SG-6000-E1700、SG-6000-E1700-GM、SG-6000-E1606、SG-6000-E1605、SG-6000-E1600、SG-6000-E1600-GM、SG-6000-E1500、SG-6000-E1100	Method 1: 1. Power off the device. 2. Use a pin to press the CLR button in the pinhole; keep pressing and power on the device. 3. Keep pressing until the STA and ALM LEDs turn solid red. System will start to reset itself. 4. When restoring is complete, system will reboot automatically. Method 2: 1. Keep the device powered on.

Model	Step
	2. With the STA LED blinking, use a pin to press the CLR button in the pinhole for 2 minutes. 3. Keep pressing until the STA and ALM LEDs turn solid red. System will start to reset itself. 4. When restoring is complete, system will reboot automatically.
SG-6000- E6368、SG-6000-E6360、SG-6000-E6168、SG-6000-E6160、SG-6000-E5960-GM、SG-6000-E5568、SG-6000-E5560、SG-6000-E5268、SG-6000-E5260、SG-6000-E5168、SG-6000-E3968、SG-6000-E3965、SG-6000-E3960、SG-6000-E3960-GM、SG-6000-E3668、SG-6000-E3662、SG-6000-E3660、SG-6000-E3660-GM、SG-6000-E2868、SG-6000-E2860 SG-6000-C6050、SG-6000-C5650、SG-6000-C5450、SG-6000-C5250、SG-6000-C5050、SG-6000-C4550、SG-6000-C4100	1. When the device is working, use a pin to press the CLR button in the pinhole and the device will restart. 2. After the device restarts, the CON port outputs the information of CLR button pressed and the STA and ALM LEDs turn solid red. After the LEDs turn off, the device will restart again.

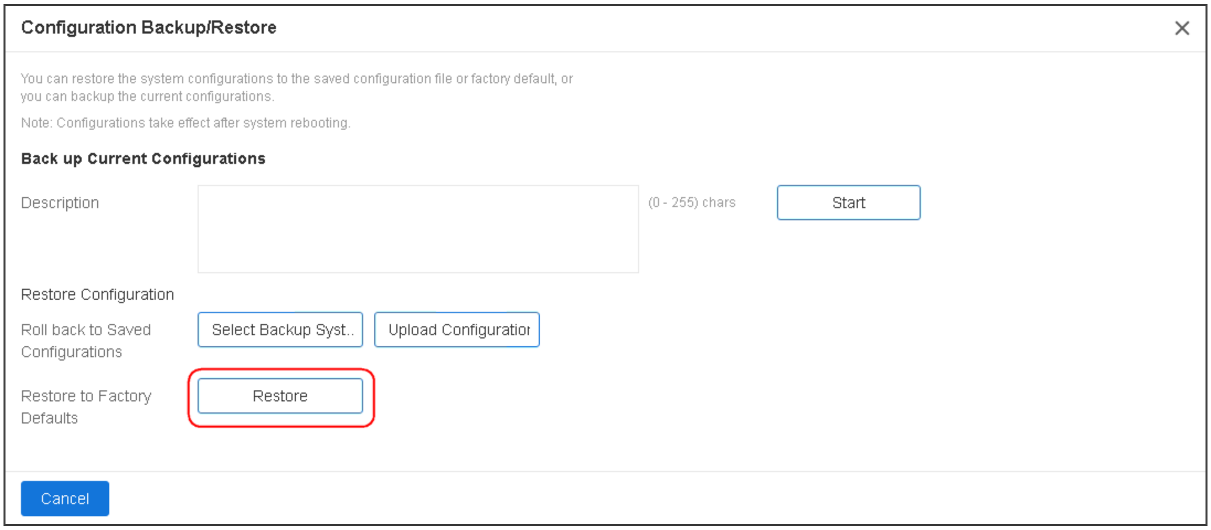
Restoring via WebUI

To restore factory default settings via WebUI, take the following steps:

1. Go to **System > Configuration File Management>Configuration File List**.

2. Click **Backup Restore**.

3. In the prompt, click **Restore**.



Configuration Backup/Restore

You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.

Note: Configurations take effect after system rebooting.

Back up Current Configurations

Description (0 - 255) chars

Restore Configuration

Roll back to Saved Configurations

Restore to Factory Defaults

4. Click **OK** to confirm.

5. The device will automatically reboot and be back to factory settings.

Chapter 2 Deploying Your Device

This chapter introduces how a firewall works and its most commonly used scenarios. Understanding the system structure, basic elements and flow chart will help you in better organizing your network and making the most of the firewall product.

- "How a Firewall Works" on Page 23

A firewall has more than one deployment scenario. Each scenario applies to one environment requirement. The usual deployment modes are:

- "Deploying Transparent Mode" on Page 32

  Transparent mode is a situation when the IT administrator does not wish to change his/her existing network settings. In transparent mode, the firewall is invisible to the network. Because no IP address configuration is needed, the firewall only provides security features.

- "Deploying Routing Mode" on Page 42

  Routing mode applies when the firewall offers both routing and NAT functions. In routing mode, the firewall connects two networks typically, an internal network and the Internet, and the firewall interfaces are configured with IP addresses.

- "Deploying Mix Mode" on Page 51

  If a firewall has Layer-2 interfaces and Layer-3 interfaces, it is in mix mode.

- "Deploying Tap Mode" on Page 52

  When an IT administrator only wants the monitor, IPS or statistic function of a firewall, while not a gateway device, using tap mode is the right choice. In tap mode, the firewall is not directly connected within the network.

How a Firewall Works

A firewall is a network security device. It protects a network by controlling the traffic that comes in and out of that network. The basic mechanism of how a firewall works is that allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, a firewall can also works as a bridging device to connect a trust zone (internal network) and untrust zone (external network).

StoneOS System Architecture

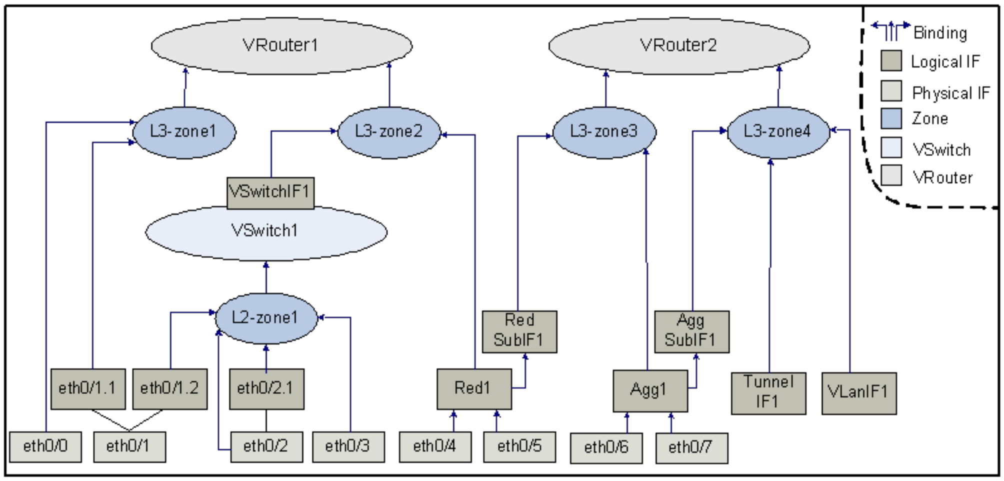
The elements that constitute StoneOS system architecture are:

- **Zone**: Zones divide network into multiple segments, for example, trust (usually refers to the trusted segments such as the Intranet), untrust (usually refers to the untrusted segments where security treats exist).
- **Interface**: Interface is the inlet and outlet for traffic going through security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.
- **VSwitch**: VSwitch is short for Virtual Switch. A VSwitch functions as a switch in Layer 2. After binding a Layer 2 zone to a VSwitch, all the interfaces in the zone are also bound to the VSwitch. There is a default VSwitch named VSwitch1. By default, all Layer 2 zones will be bound to VSwitch1. You can create new VSwitches and bind Layer 2 zones to VSwitches. Each VSwitch is a Layer 2 forwarding zone with its own MAC address table which supports the Layer 2 traffic transmission for the device. Furthermore, the VSwitchIF helps the traffic to flow between Layer 2 and Layer 3.

- **VRouter**: VRouter is Virtual Router and also abbreviated as VR. A VRouter functions as a router with its own routing table. There is a default VR named trust-vr. By default, all the Layer 3 zones will be bound to trust-vr automatically. The system supports the multi-VR function and the max VR number varies from different platforms. Multiple VRs make the device work as multiple virtual routers, and each virtual router uses and maintains its own routing table.The multi-VR function allows a device to achieve the effects of the address isolating in different route zones and the address overlapping in different VRs, as well as avoiding leakage of route to some extent and enhancing route security of network.

- **Policy**: Policy is used to control the traffic flow in security zones/segments. By default Hillstone devices will deny all traffic in security zones/segments, while the policy can identify which flow in security zones or segments will be permitted, and which will be denied, which is specifically based on policy rules.

For the relationships among interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationships among them are:

- Interfaces are bound to security zones. Interfaces bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; interface and its sub interface can belong to different security zones.

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

General Rules of Security Policy

By default, all interfaces, even in the same zone, cannot communicate. Traffic in different zones are not allowed to be transferred either. In order to change the rule, you need to set up new policy rules to allow traffic forwarding.

Notes: To allow bidirectional traffic, you need to set up two policies: one is from source to destination, the other is from destination to source. If there is only one-direction initiative access, the responsive direction only need to respond to that visit, you will need to create only one-way policy (from source to destination).

This part explains what policy is needed to allow interfaces in different zones, VSwitches, or VRouters to communicate. The rules are:

- **Interfaces in the same zone**

  To allow interfaces in the same zone to communicate, you need to create a policy whose source and destination are both the zone which the interfaces belong to.

  For example, to allow eth0/0 and eth0/1 to communicate, you need to create an "allowing" policy with source L3-zone and destination L3-zone.

- **Zones of two interfaces are under the same VSwtich**

  To allow communication of interfaces in different zones under the same VSwitch, you need to create two policies: one policy is to allow traffic from a zone to another; the other policy is to allow traffic in the opposite direction.

For example, to allow eth0/2 and eth0/3 to communicate, you should create a policy whose source is L2-zone1 and destination is L2-zone2, then create another policy to allow traffic from L2-zone2 to L2-zone1.

- **Zones of two interfaces are under different VSwitches**

  Each VSwtich has its VSwtich interface (VSwitchIF) which is bound to a Layer-3 zone. To allow interfaces in different zones under different VSwitches to communicate, you need to create an "allowing" policy where the source is the zone of one VSwitchIF and the destination is the zone of the other VSwitchIF. After that, create another policy of the opposite direction.

- **Zones of two L3 interfaces are under the same VRouter**

  To allow two L3 interfaces to communicate, you need to create a policy allowing one zone to the other zone.

  For example, to allow communication between eth0/0 and eth0/5, you should create a policy from L3-zone1 to L3-zone2, and then create an opposite direction policy.

- **Zones of two L3 interfaces are under different VRouters**

  To allow two L3 interfaces in two different zones of different VRouters, you need to create a policy with the source being one VRouter and the destination being the other VRouter. Then you create a policy of the opposite direction.

- **An L2 interface and an L3 interface under the same VRouter**

  To allow communication between an L2 interface and an L3 interface under the same VRouter, you will need to create a policy whose source is the zone which binds the VSwithIF of L2 interface and the destination is the zone of L3 interface. After that, create a policy of the opposite direction.

  For example, to allow eth0/0 and eth0/2 to communicate, create a policy from L3-zone1 to L2-zone1, and its opposite direction policy.

Packet Processing Rule

Forwarding Rule in Layer 2

Forwarding within Layer 2 means it is in one VSwitch. StoneOS system creates a MAC address table for a VSwitch by source address learning. Each VSwitch has its own MAC address table. The packets are forwarded according to the types of the packets, including IP packets, ARP packets, and non-IP-non-ARP packets.

The forwarding rules for IP packets are:

1. Receive a packet.

2. Learn the source address and update the MAC address table.

3. If the destination MAC address is a unicast address, the system will look up the egress interface according to the destination MAC address. And in this case, two situations may occur:

   - If the destination MAC address is the MAC address of the VSwitchIF with an IP configured, system will forward the packet according to the related routes; if the destination MAC address is the MAC address of the VSwitchIF with no IP configured, system will drop the packet.

   - Figure out the egress interface according to the destination MAC address. If the egress interface is the source interface of the packet, system will drop the packet. Otherwise, system will forward the packet from the egress interface.

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

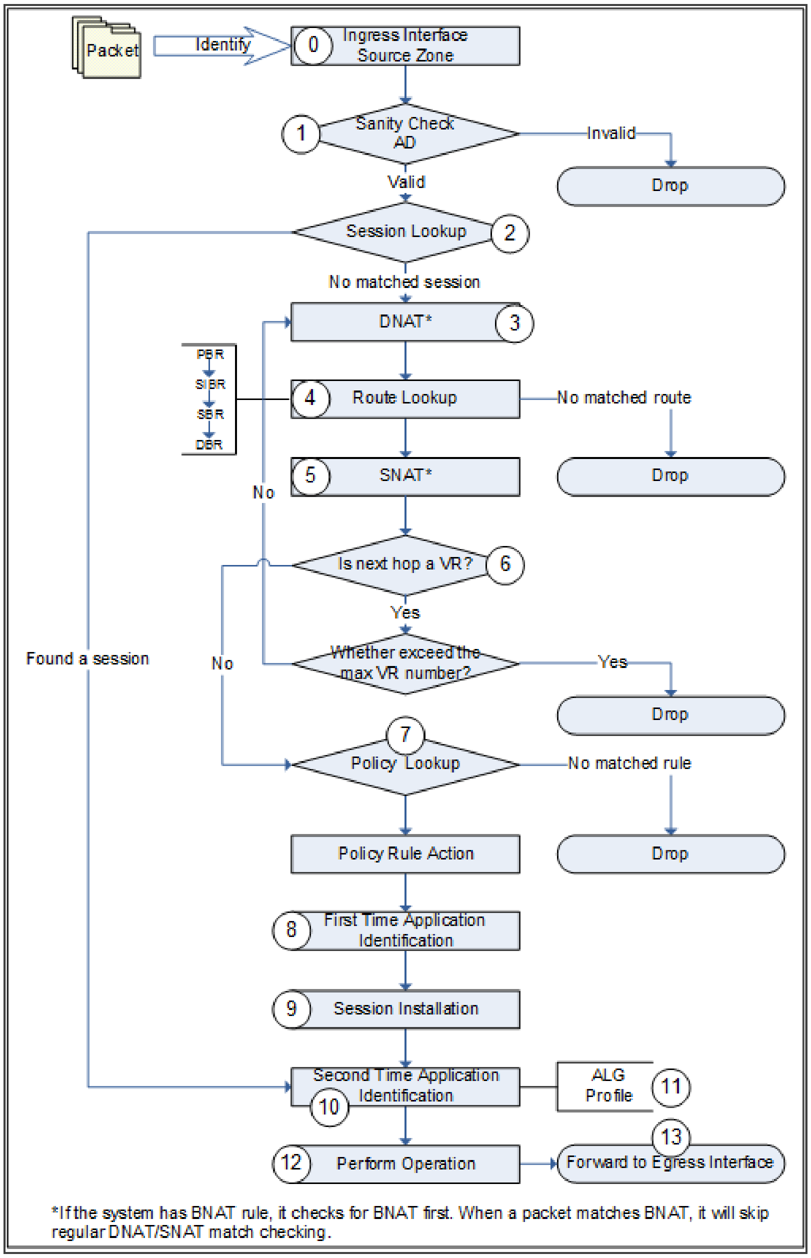
4. Figure out the source zone and destination zone according to the ingress and egress interfaces.

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

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

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

Forwarding Rule in Layer 3



*If the system has BNAT rule, it checks for BNAT first. When a packet matches BNAT, it will skip regular DNAT/SNAT match checking.

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

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

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

3. DNAT operation. If a DNAT rule is matched, system will mark the packet. The DNAT translated address is needed in the step of route lookup.
   *Note: If the system has static 1-to-1 BNAT rule, BNAT rule is checked before other NAT rules. If a packet matches BNAT, it will be processed in accordance with this rule's configuration. It will skip the regular DNAT rule checking.

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

5. SNAT operation. If a SNAT rule is matched, system will mark the packet.
   *Note: If the system has static 1-to-1 BNAT rule, BNAT rule is checked before other NAT rules. If a packet matches BNAT, it will be processed in accordance with this rule's configuration. It will skip the regular SNAT rule checking.

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

7. Policy lookup. System looks up the policy rules according to the packet’s source/destination zones, source/destination IP and port, and protocol. If no policy rule is matched, system will drop the packet; if any policy rule is matched, the system will deal with the packet as the rule specified. And the actions can be one of the followings:

- Permit: Forward the packet.
- Deny: Drop the packet.
- Tunnel: Forward the packet to the specified tunnel.
- Fromtunnel: Check whether the packet originates from the specified tunnel. System will forward the packet from the specified tunnel and drop other packets.
- WebAuth: Perform WebAuth on the specified user.

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

Deploying Transparent Mode

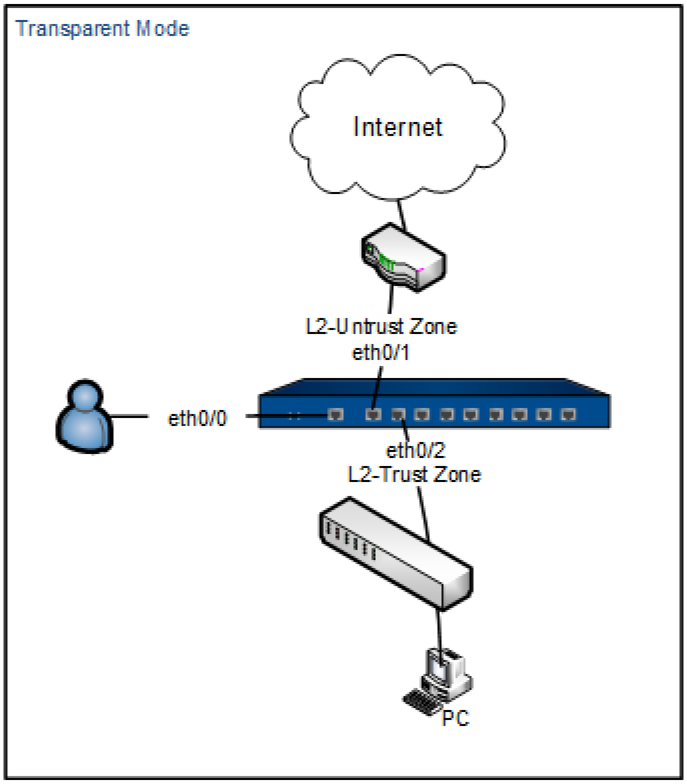
Transparent mode is also known as bridge mode or transparent bridging mode. Transparent mode is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. The firewall will be used as a security device.

Transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up NAT rule

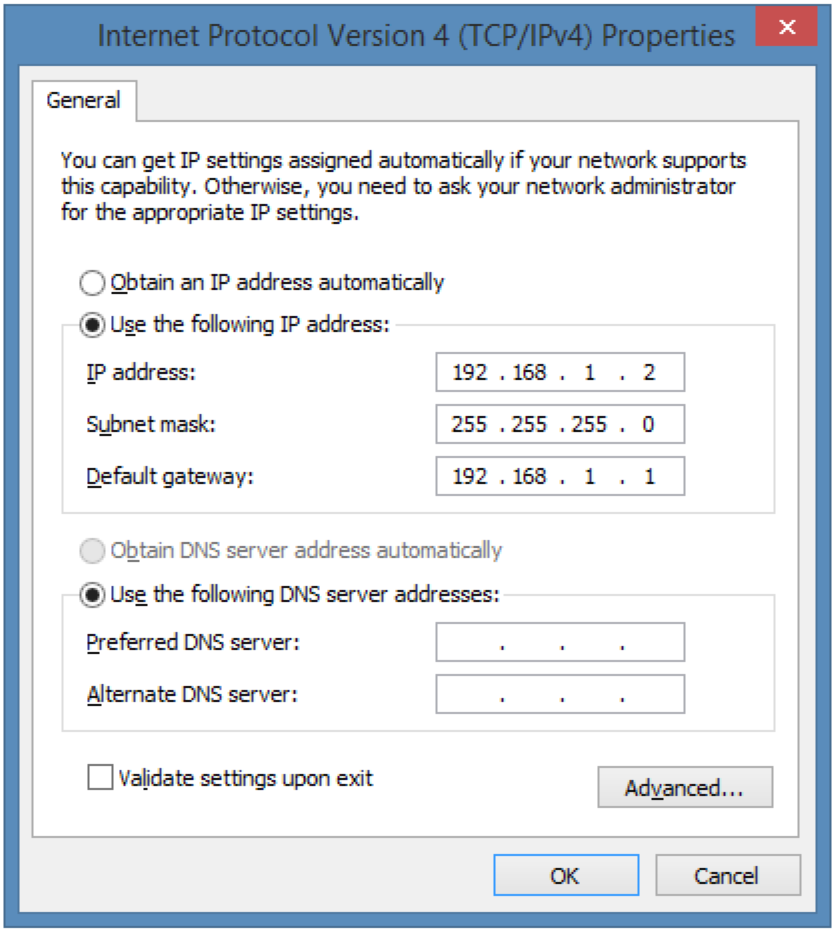
Under normal circumstances, the firewall in transparent mode is deployed between the router and the switch of the protected network, or it is installed between the Internet and a company's router. The internal network uses its old router to access the Internet, and the firewall only provides security control features.

This section introduces a configuration example of a firewall deployed between a router and a switch. In this example,the administrator uses eth0/0 to manage firewall. The firewall's eth0/1 is connected to router (which is connecting to the Internet) and eth0/2 is connected to a switch (which is connecting to internal network).



Step 1: Initial log in the firewall

1. In the administrator's Ethernet properties, set the IPv4 protocol as below.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2. Connect an RJ-45 Ethernet cable from the computer to the eth0/0 of the device.

3. In the browser's address bar, type "http://192.168.1.1" and press **Enter**.

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

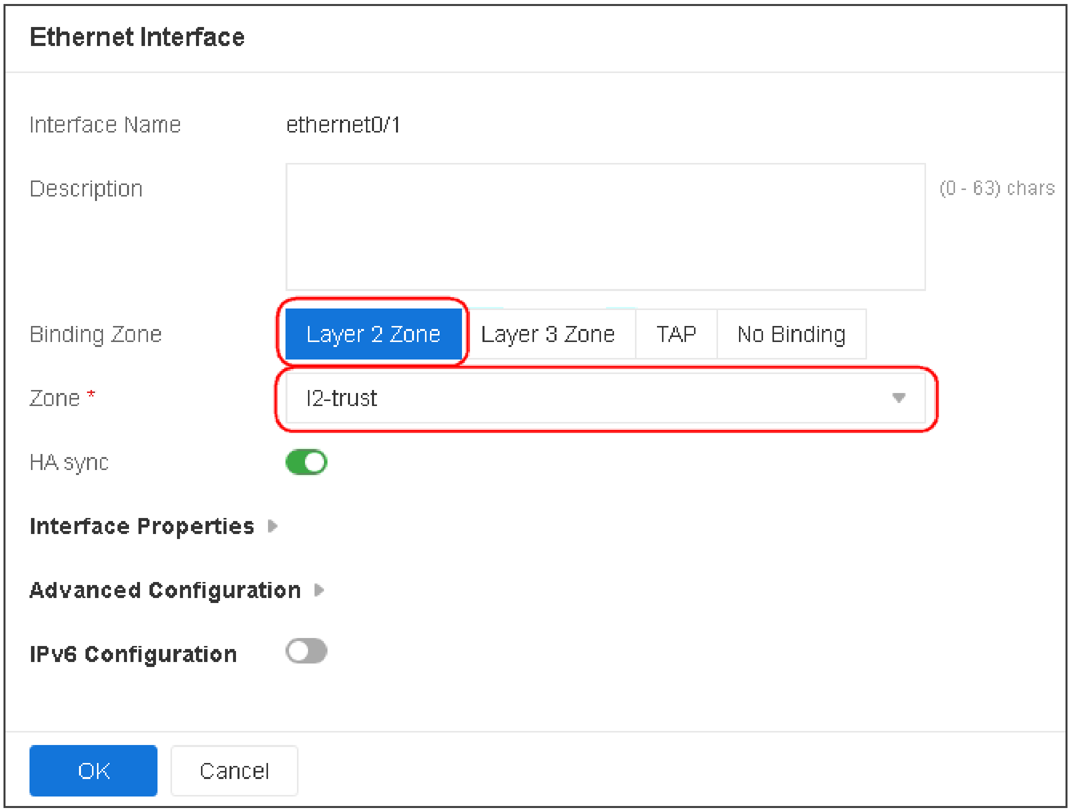
5. Click **Login**, and the device's system will initiate.

Step 2: Configure interface and zone

- Configure eth0/1 as an Internet connected interface.

1. Select **Network > Interface**.

2. Double click ethernet0/1, and configure in the prompt.



Ethernet Interface

Interface Name: ethernet0/1

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone | Layer 3 Zone | TAP | No Binding

Zone *: l2-trust

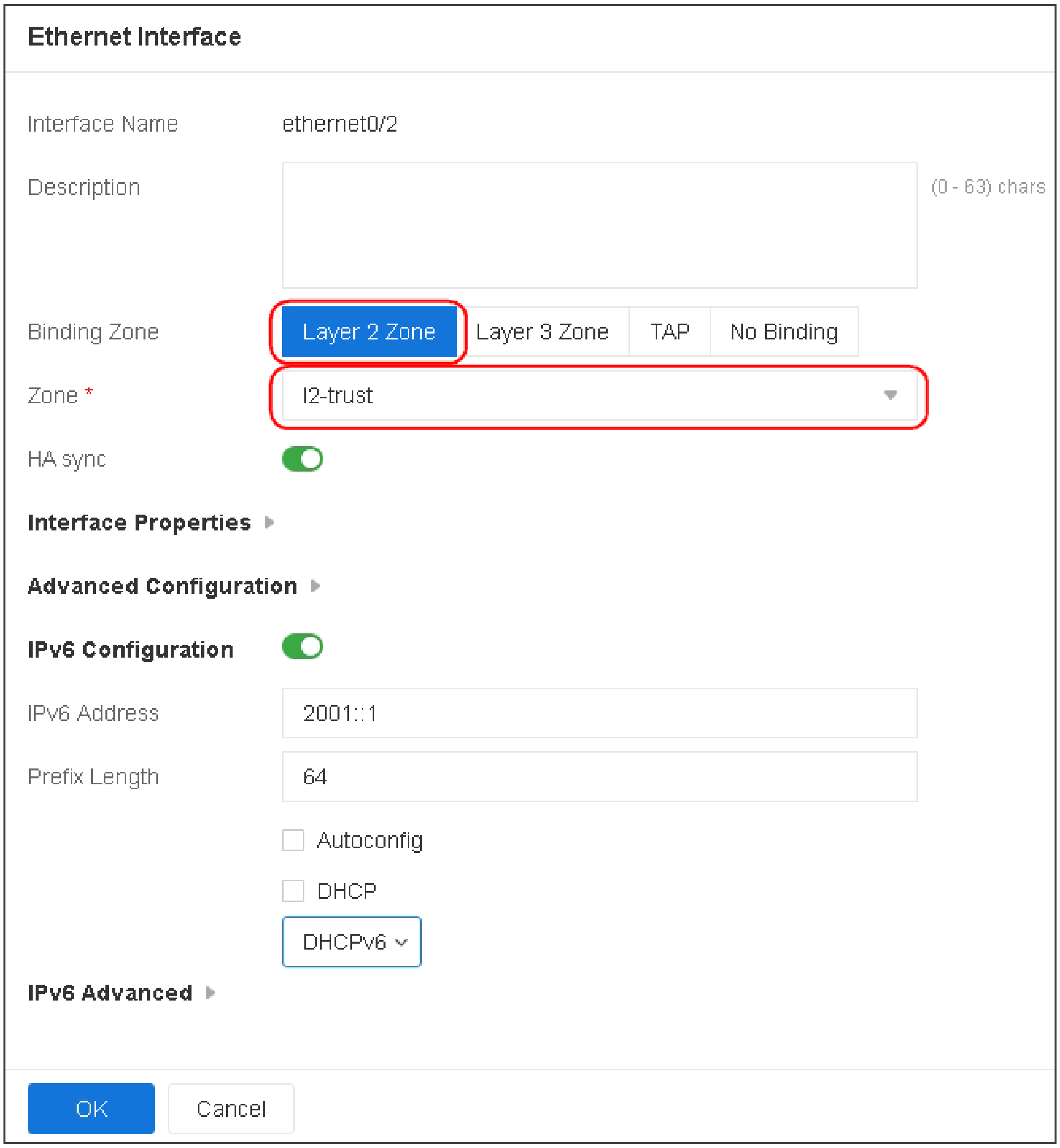
HA sync

3. Click **OK**.

- Configure eth0/2 as a private network connected interface.

1. Select **Network** > **Interface**.

2. Double click ethernet0/2, and configure in the prompt.



Ethernet Interface

Interface Name ethernet0/2

Description (0 - 63) chars

Binding Zone [✓ Layer 2 Zone] Layer 3 Zone TAP No Binding

Zone * l2-trust

HA sync ●

Interface Properties ▸

Advanced Configuration ▸

IPv6 Configuration ●

IPv6 Address 2001::1

Prefix Length 64

□ Autoconfig

□ DHCP

DHCPv6 ⌄

IPv6 Advanced ▸

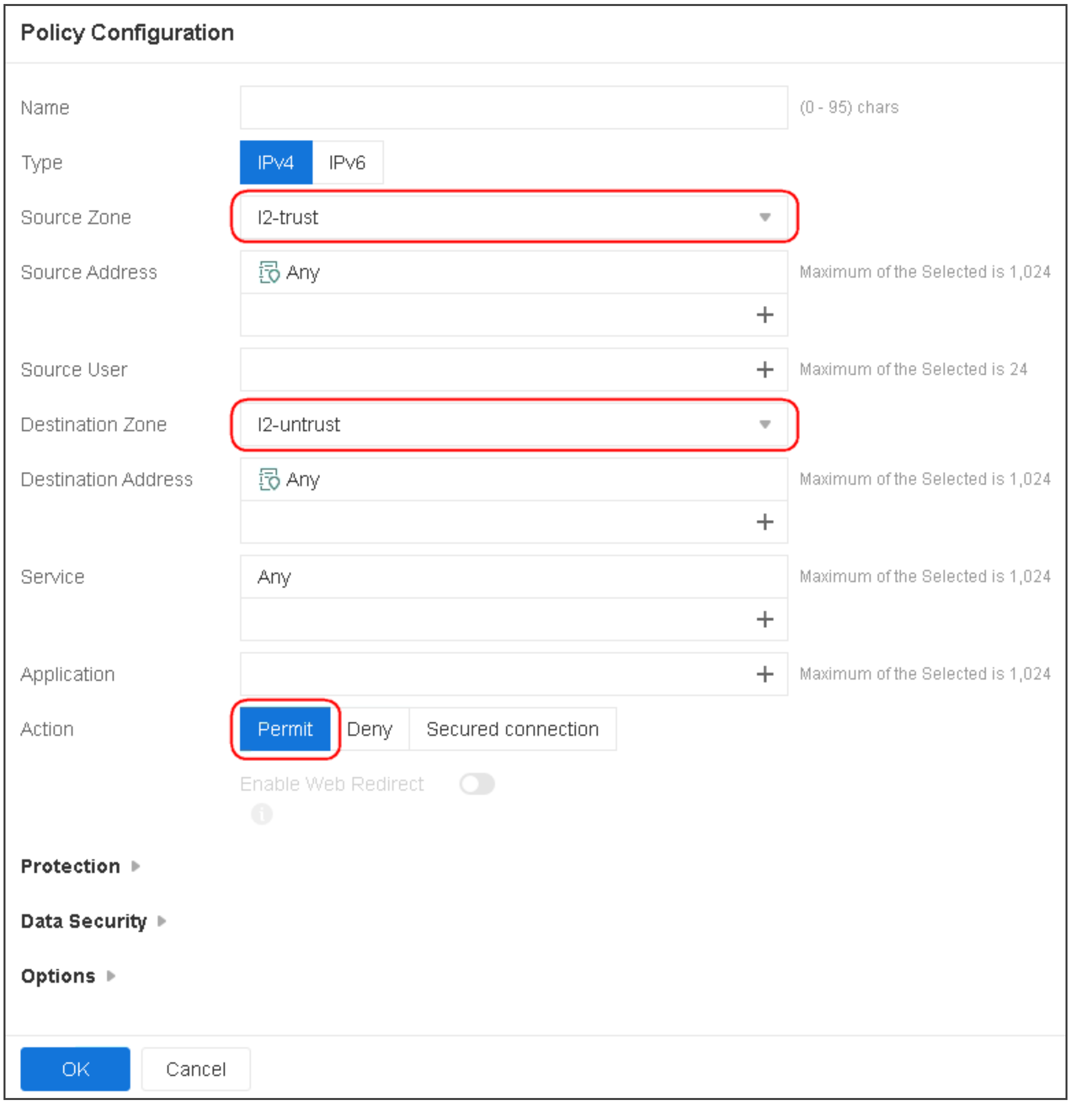
3. Click **OK**.

Step 3: Configuring policies

- Create a policy to allow visiting the Internet.

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

2. Click **New**,select Policy from the drop-down list.



Policy Configuration

Name: (0 - 95) chars

Type: IPv4 | IPv6

Source Zone: l2-trust

Source Address: Any — Maximum of the Selected is 1,024

Source User: Maximum of the Selected is 24

Destination Zone: l2-untrust

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application: Maximum of the Selected is 1,024

Action: Permit | Deny | Secured connection

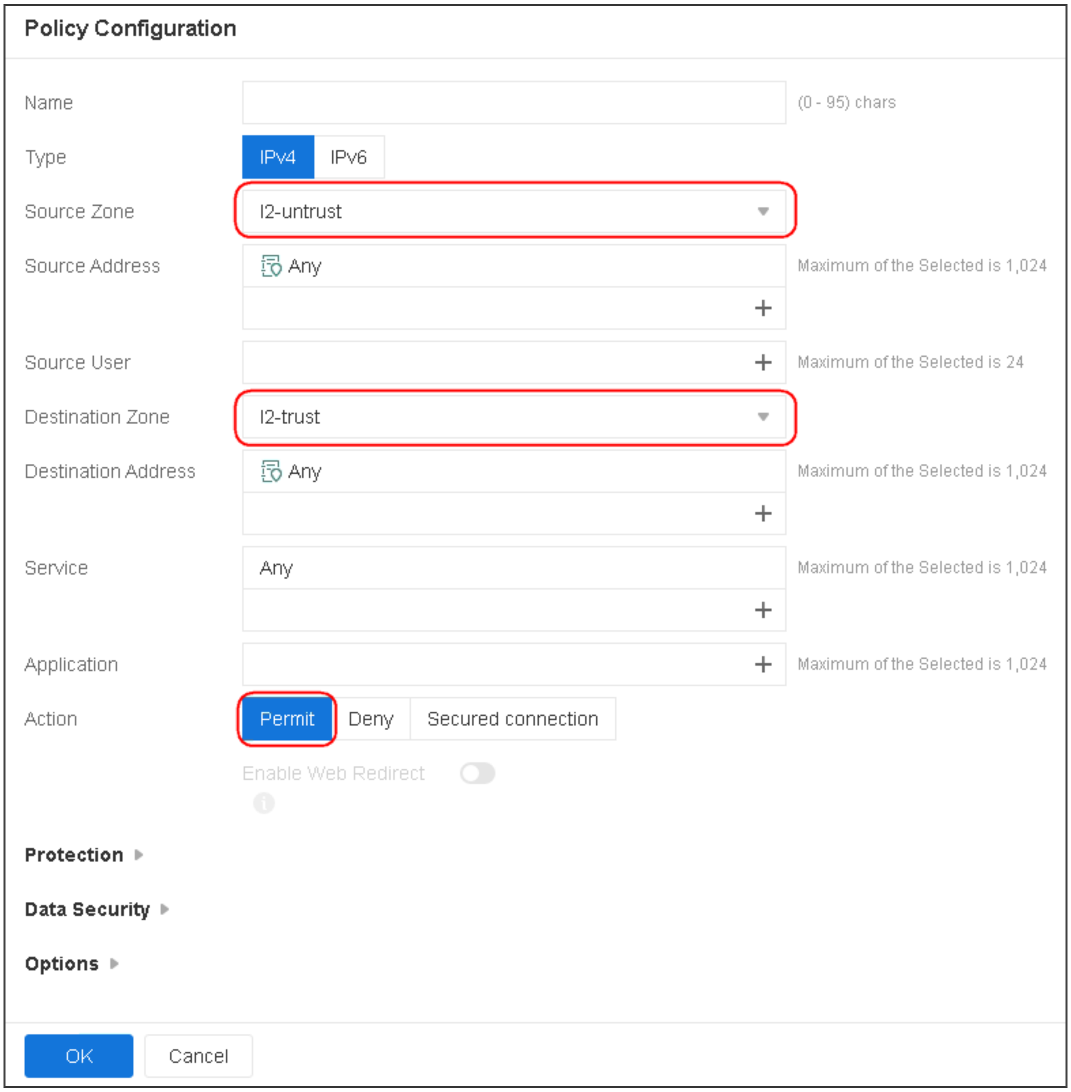
Enable Web Redirect

3. Click **OK**.

- Create a policy to allow the Internet to visit a private network.

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

  2. Click **New**.



Policy Configuration

Name		(0 - 95) chars
Type	[✓ IPv4] IPv6	
Source Zone	l2-untrust	
Source Address	Any	Maximum of the Selected is 1,024
Source User		Maximum of the Selected is 24
Destination Zone	l2-trust	
Destination Address	Any	Maximum of the Selected is 1,024
Service	Any	Maximum of the Selected is 1,024
Application		Maximum of the Selected is 1,024
Action	[✓ Permit] Deny Secured connection	
	Enable Web Redirect ○	

Protection

Data Security

Options

OK Cancel

  3. Click **OK**.

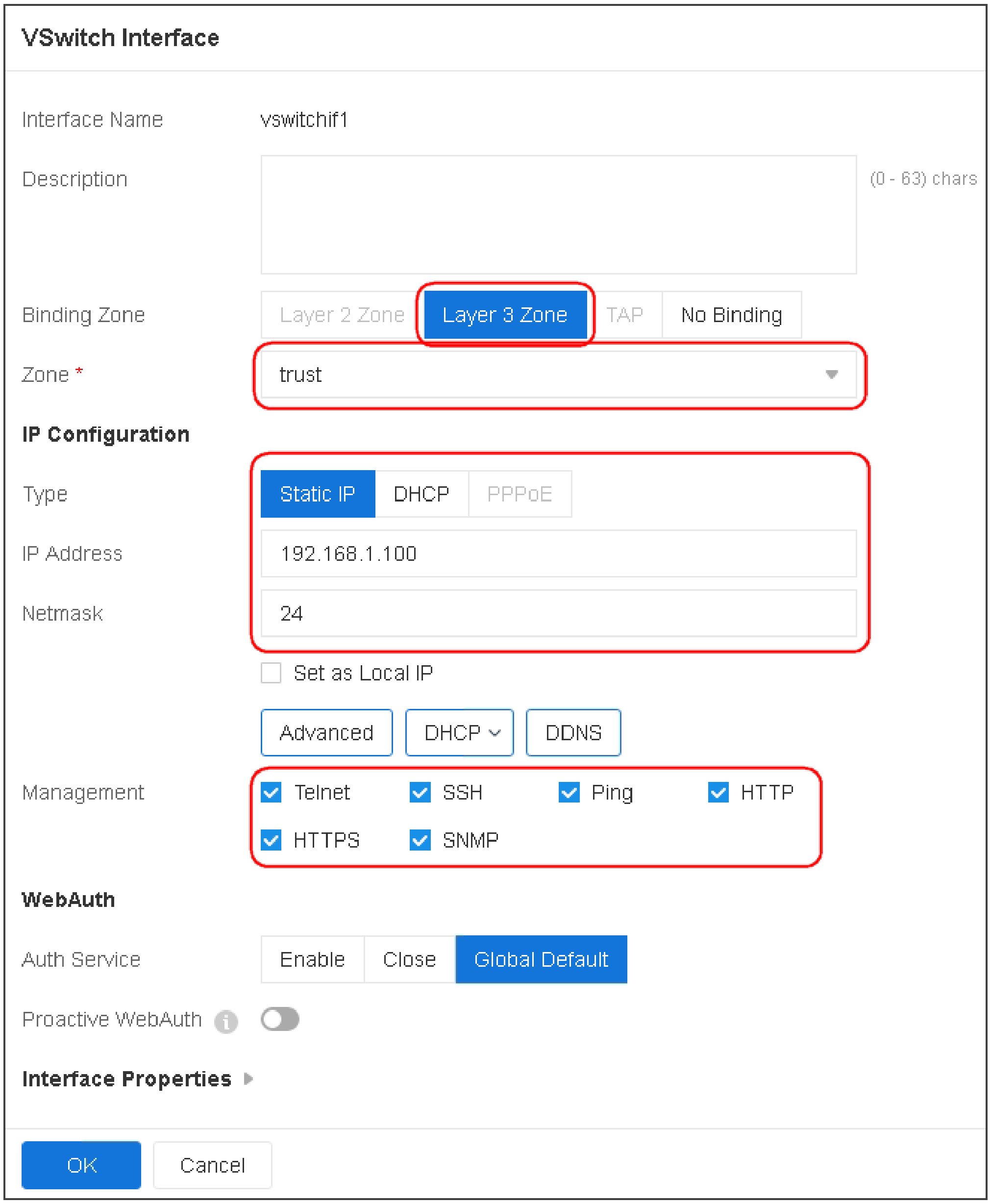
- The two policies above ensure communication between a private network and the Internet. If you want to set up more details, e.g. to limit P2P download, you can add more policies and overlap the new policies with the old ones. The match sequence of policies is determined by their position in the policy list, not their ID numbers.

(Optional) Step 4: Configuring VSwitch Interface for managing the firewall.

If you want any PC in the private network to visit and configure the firewall, you can configure a VSwitch interface as a management interface.

1. Select **Network** > **Interface**.

2. Double click vswtichif1.



VSwitch Interface

Interface Name: vswitchif1

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone [✓ Layer 3 Zone] TAP No Binding

Zone *: trust

IP Configuration

Type: [✓ Static IP] DHCP PPPoE

IP Address: 192.168.1.100

Netmask: 24

□ Set as Local IP

Management: ☑ Telnet ☑ SSH ☑ Ping ☑ HTTP ☑ HTTPS ☑ SNMP

WebAuth

Auth Service: Enable Close [✓ Global Default]

Proactive WebAuth: ○

Interface Properties

Notes: When configuring **IP Configuration**, set an IP address in the same subnet of the private network.

3. Click **OK**.

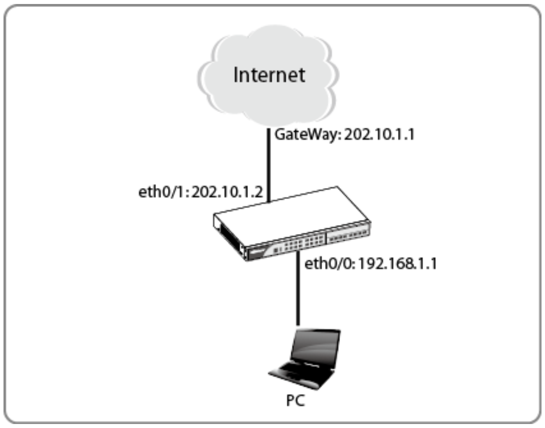
4. With any PC in the private network, enter the IP address of vswitchif1, and you will visit the firewall web user interface.

Deploying Routing Mode

Routing mode deployment often uses the NAT function, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. A firewall in routing mode can work as a router and a security devcie.

Routing mode is mostly used when the firewall is installed between an internal network and the Internet.

The example which is based on the below topology shows you how to connect and configure a new Hillstone device in routing mode. The device connects a private network to the Internet.



Step 1: Connecting to the device

1. Connect one port (e.g. eth0/1) of the Hillstone device to your ISP network. In this way, "eth0/1" is in the untrust zone.

2. Connect your internal network to another Ethernet interface (e.g. eth0/0) of the device. This means "eth0/0" is connected to the trust zone.

3. Power on the Hillstone device and your PCs.

4. If one of the internal interfaces already has been configured with an IP address, use a browser to visit that address from one of your internal PCs.

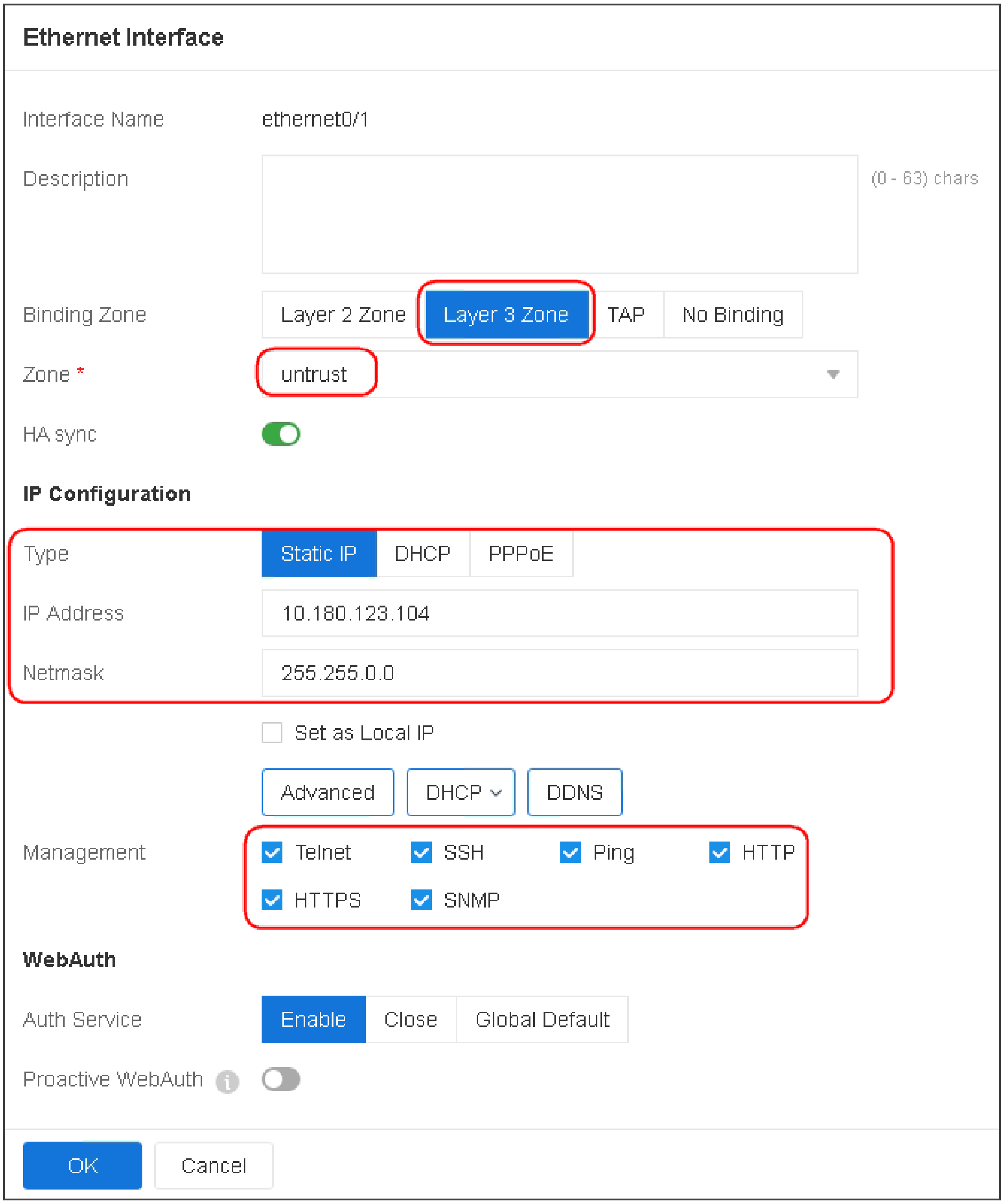
If it is a new device, use the methods in "Initial Visit to Web Interface" on Page 4 to visit.

5. Enter "hillstone" for both the username and the password.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.

2. Double click **ethernet0/1**.



Ethernet Interface

Interface Name	ethernet0/1
Description	(0 - 63) chars
Binding Zone	Layer 2 Zone [✓ Layer 3 Zone] TAP No Binding
Zone *	untrust
HA sync	●

IP Configuration

Type	[✓ Static IP] DHCP PPPoE
IP Address	10.180.123.104
Netmask	255.255.0.0
	□ Set as Local IP
	Advanced DHCP DDNS
Management	☑ Telnet ☑ SSH ☑ Ping ☑ HTTP ☑ HTTPS ☑ SNMP

WebAuth

Auth Service	[✓ Enable] Close Global Default
Proactive WebAuth	○

In the Ethernet Interface dialog box, enter values

Option	Value
Binding	L3-zone

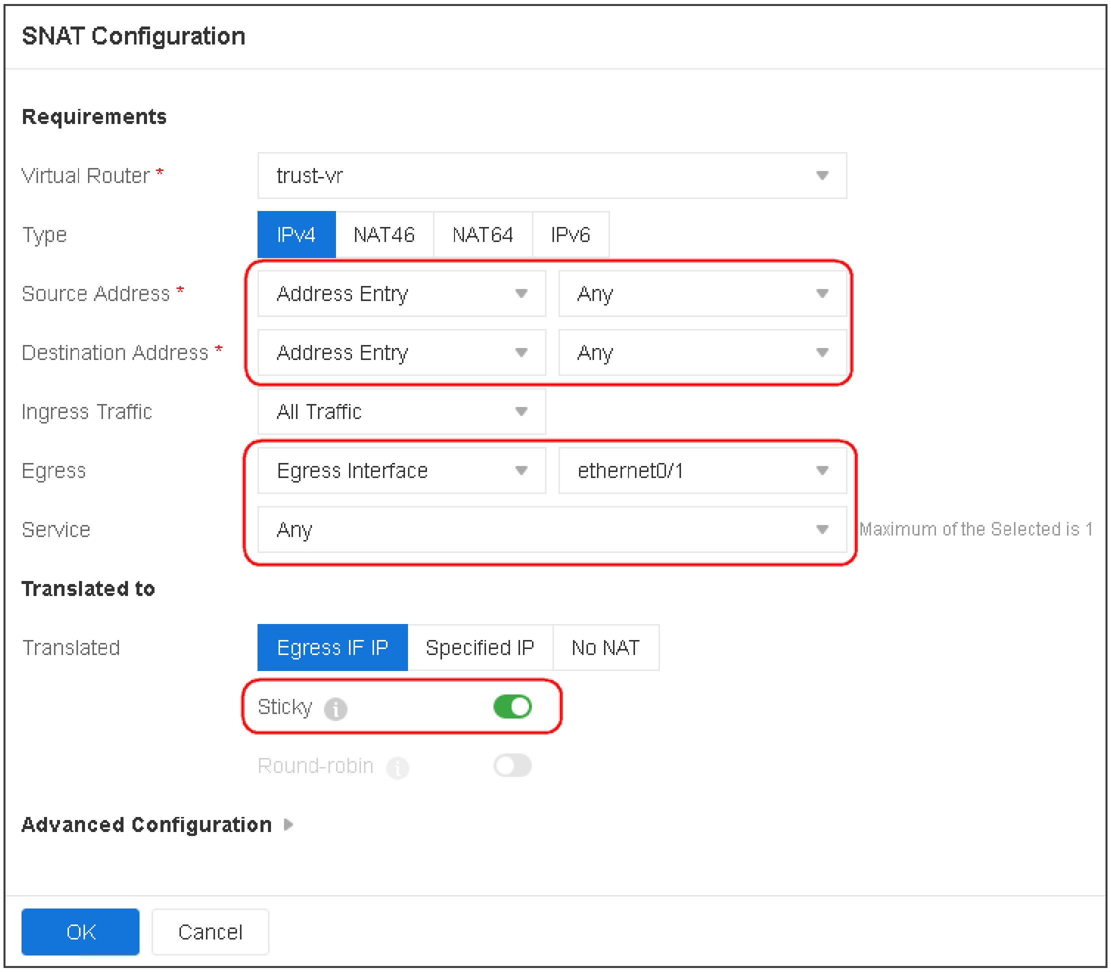
Option	Value
Zone	
Zone	untrust
Type	Static IP
IP Address	202.10.1.1 (public IP address provided by your ISP)
Netmask	255.255.255.0
Management	Select the protocols that you want to use to access the device.

3. Click **OK**.

Step 3: Creating a NAT rule to translate internal IP to public IP

1. Go to **Policy** > **NAT** > **SNAT**.

2. Select **New**



SNAT Configuration

Requirements

Virtual Router *: trust-vr

Type: IPv4 | NAT46 | NAT64 | IPv6

Source Address *: Address Entry, Any

Destination Address *: Address Entry, Any

Ingress Traffic: All Traffic

Egress: Egress Interface, ethernet0/1

Service: Any — Maximum of the Selected is 1

Translated to

Translated: Egress IF IP | Specified IP | No NAT

Sticky: on

Round-robin: off

Advanced Configuration

OK | Cancel

In the SNAT Configuration dialog box, enter values

Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any

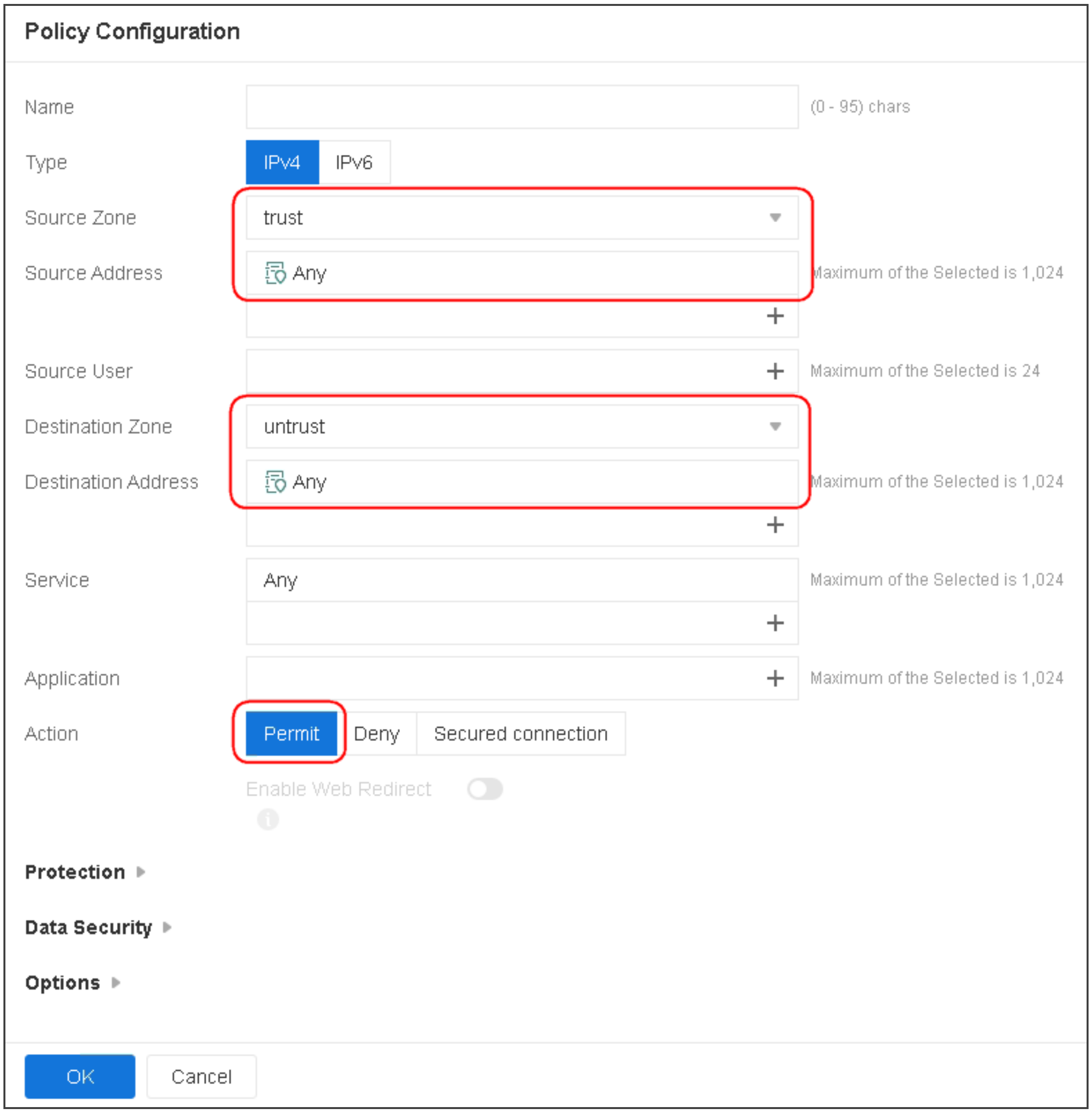
Option	Value
Egress	Egress interface, ethernet 0/1
Translated	Egress IP
Sticky	Enable

3. Click **OK**.

Step 4: Creating a security policy to allow internal users to access the Internet.

1. Go to **Policy > Security Policy>Policy**.

2. Click **New**,select **Policy** from the drop-down list.



Policy Configuration

Name (0 - 95) chars

Type: IPv4 | IPv6

Source Zone: trust

Source Address: Any — Maximum of the Selected is 1,024

Source User — Maximum of the Selected is 24

Destination Zone: untrust

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application — Maximum of the Selected is 1,024

Action: Permit | Deny | Secured connection

Enable Web Redirect

Protection

Data Security

Options

In the Policy Configuration dialog box, enter values.

Source Information	
Zone	trust
Address	Any
Destination Information	

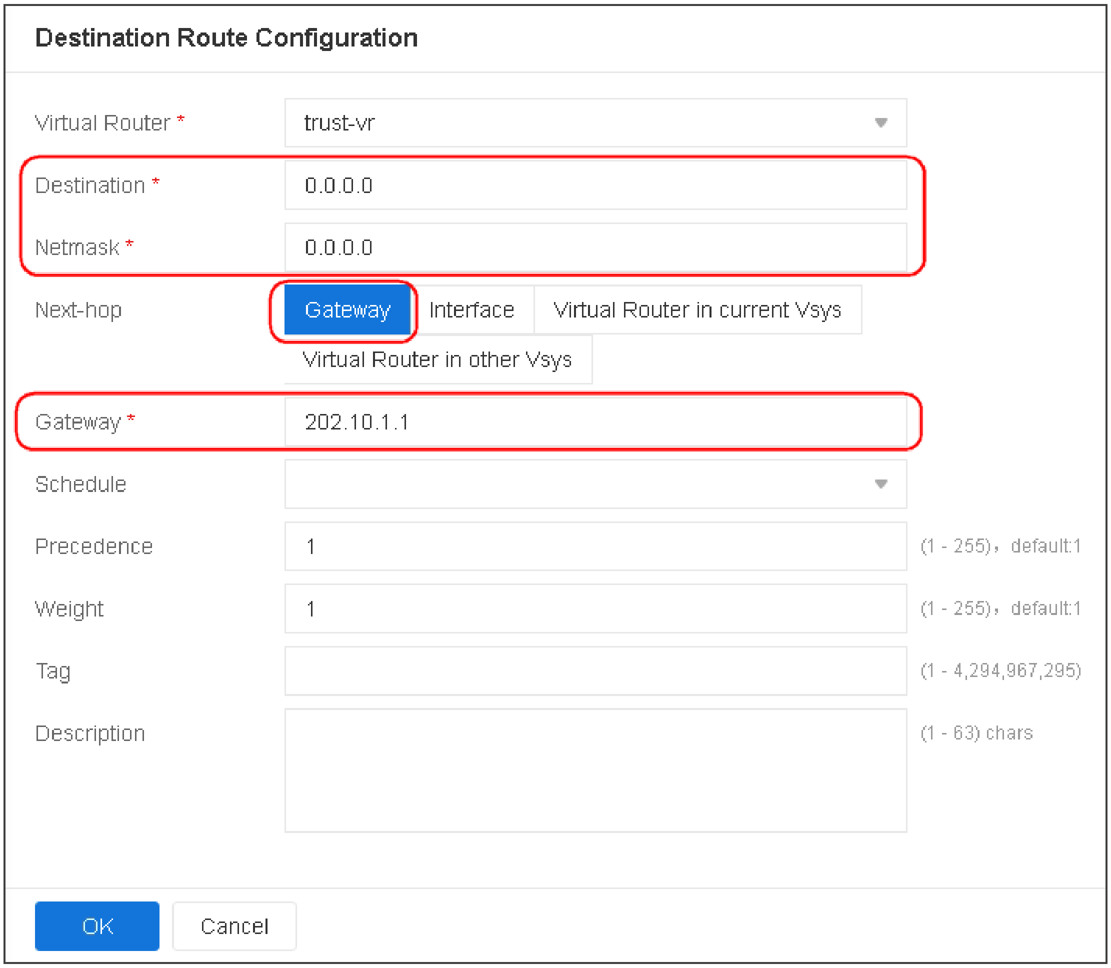
Zone	untrust
Address	Any
Other Information	
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click OK.

Step 5: Configuring a default route

1. Go to **Network** >**Routing** > **Destination Route**.

2. Click **New**.



Destination Route Configuration

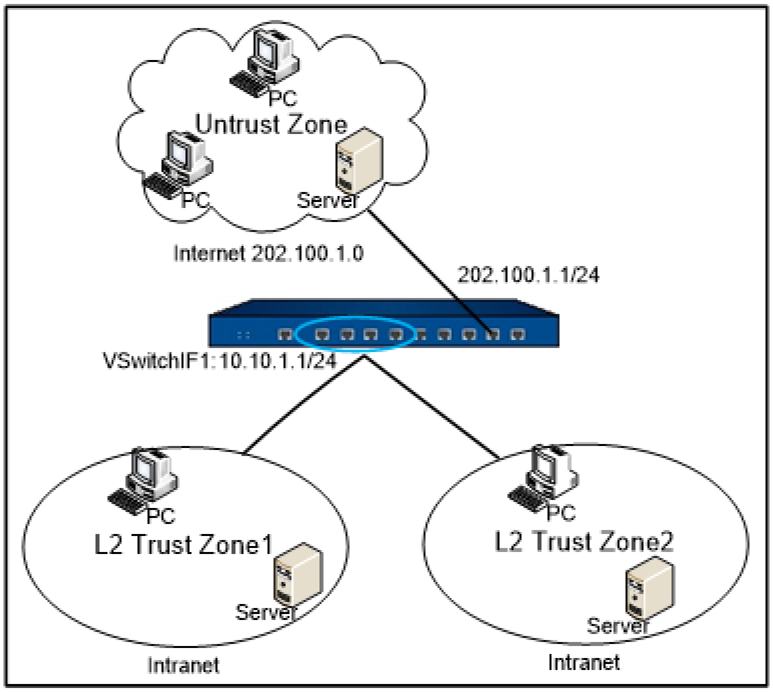
Virtual Router *	trust-vr	
Destination *	0.0.0.0	
Netmask *	0.0.0.0	
Next-hop	[✓ Gateway] Interface Virtual Router in current Vsys Virtual Router in other Vsys	
Gateway *	202.10.1.1	
Schedule		
Precedence	1	(1 - 255)，default:1
Weight	1	(1 - 255)，default:1
Tag		(1 - 4,294,967,295)
Description		(1 - 63) chars

In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0 (means all network)
Subnet Mask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

Deploying Mix Mode

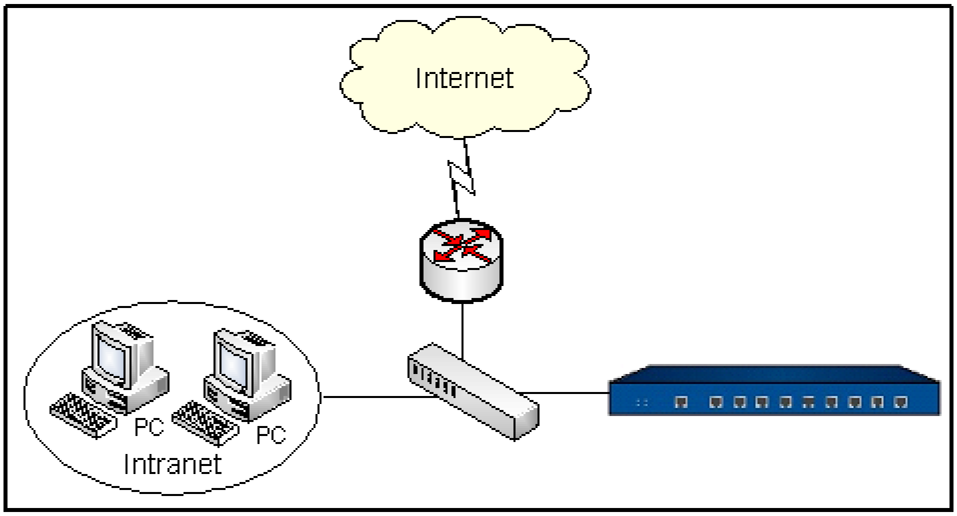
If the firewall has both L2 interfaces (transparent mode) and L3 interfaces (routing mode), the firewall is in mix mode.



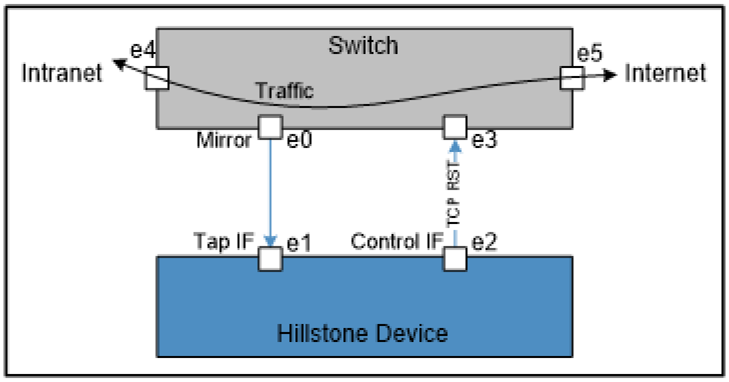
To configure a mix mode, you need to combine the routing mode of the deployment methods with the transparent mode. Please refer to these two modes.

Deploying Tap Mode

In most cases, the security device is deployed within the network as a serial node. However, in some other scenarios, an IT administrator would just want the auditing and statistical functions like IPS, antivirus, and Internet behavior control. For these features, you just need to connect the device to a mirrored interface of a core network. The traffic is mirrored to the security device for auditing and monitoring.



The bypass mode is created by binding a physical interface to a tap zone. Then, the interface becomes a bypass interface.



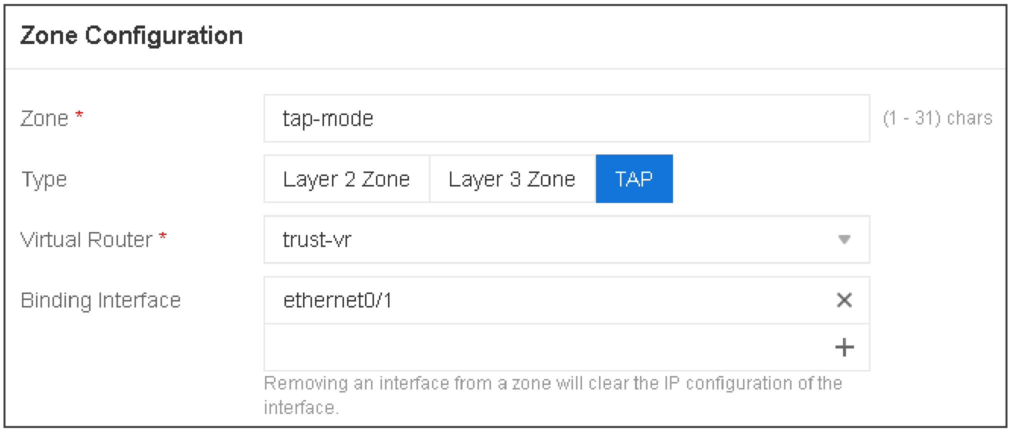
Use an Ethernet cable to connect e0 of the Switch with e1 of the Hillstone device. The interface e1 is the bypass interface and e2 is the bypass control interface. The interface e0 is the mirror interface of the switch.The switch mirrors the traffic to e1 and the Hillstone device will monitor, scan, and log the traffic received from e1. After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.

Notes: Before configuring tap mode in the device, you need to set up an interface mirroring your primary switch. Mirror the traffic of the switch from e0 to e1, and the device can scan, monitor and count the mirrored traffic.

Here provides an example of monitoring IPS in tap mode.

Step 1: Creating tap mode by binding an interface

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



Zone Configuration

Zone *	tap-mode	(1 - 31) chars
Type	Layer 2 Zone / Layer 3 Zone / TAP (selected)	
Virtual Router *	trust-vr	
Binding Interface	ethernet0/1	

Removing an interface from a zone will clear the IP configuration of the interface.

Option	Value
Zone	enter a name, e.g. "tap-zone" .
Type	TAP
Binding Interface	Select the bypass interface (only a physical interface, aggregate interface or redundant interface can apply, subinterface is not allowed).

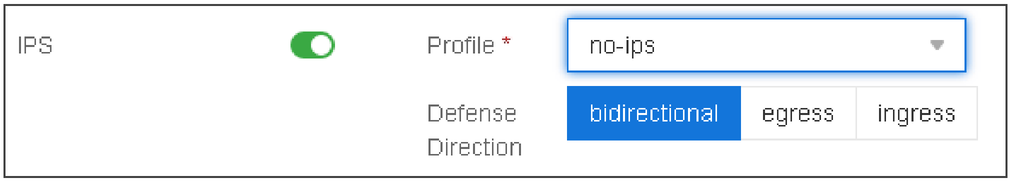
2. Click **OK**.

Step 2: Creating an IPS rule

1. Select **Object > Intrusion Prevention System**.
2. Click **New**.
3. Enter the rule name.
4. Configure the signatures settings.
5. Configure the protocol settings.
6. Click **OK** to complete IPS rule configuration.

Step 3: Add IPS rule into Tap zone

1. Select **Network > Zone**, and double-click the tap zone created in step 1.
2. In the Treat Prevention tab, enable IPS and select the IPS rule created.



IPS

Profile * no-ips

Defense Direction: bidirectional | egress | ingress

3. Click **OK**.

(Optional) Block traffic in switch

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, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.

By default, the bypass interface itself is the control interface. However, you may also change the control interface.

To change a bypass control interface, you can only use the command line interface:

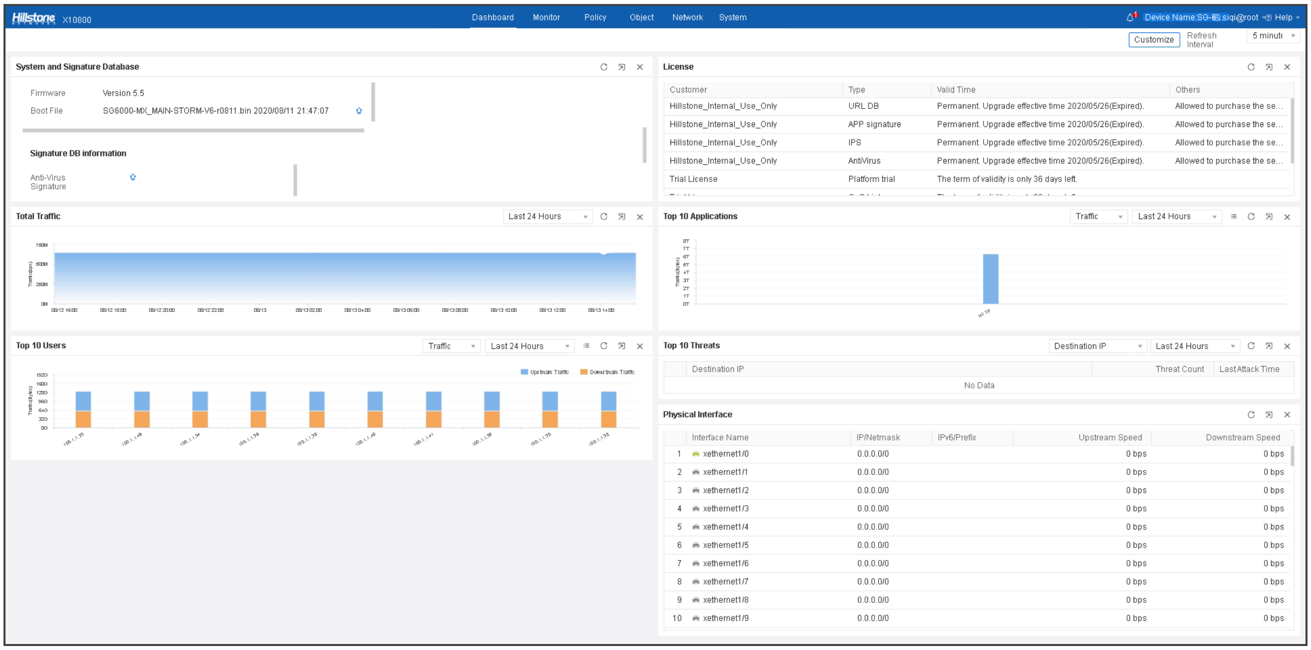
tap control-interface *interface-name*

- *interface-name* - Specifies which interface is used as the bypass control interface.

Chapter 3 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:



System and Signature Database

Firmware Version 5.5

Boot File SG6000-MX_MAIN-STORM-V6-r0811.bin 2020/08/11 21:47:07

Signature DB information

Anti-Virus Signature

License

Customer	Type	Valid Time	Others
Hillstone_Internal_Use_Only	URL DB	Permanent. Upgrade effective time 2020/05/26(Expired).	Allowed to purchase the se...
Hillstone_Internal_Use_Only	APP signature	Permanent. Upgrade effective time 2020/05/26(Expired).	Allowed to purchase the se...
Hillstone_Internal_Use_Only	IPS	Permanent. Upgrade effective time 2020/05/26(Expired).	Allowed to purchase the se...
Hillstone_Internal_Use_Only	AntiVirus	Permanent. Upgrade effective time 2020/05/26(Expired).	Allowed to purchase the se...
Trial License	Platform trial	The term of validity is only 36 days left.	

Total Traffic

Top 10 Applications

Top 10 Users

Top 10 Threats

Destination IP	Threat Count	Last Attack Time
No Data		

Physical Interface

	Interface Name	IP/Netmask	IPv6/Prefix	Upstream Speed	Downstream Speed
1	xethernet1/0	0.0.0.0/0		0 bps	0 bps
2	xethernet1/1	0.0.0.0/0		0 bps	0 bps
3	xethernet1/2	0.0.0.0/0		0 bps	0 bps
4	xethernet1/3	0.0.0.0/0		0 bps	0 bps
5	xethernet1/4	0.0.0.0/0		0 bps	0 bps
6	xethernet1/5	0.0.0.0/0		0 bps	0 bps
7	xethernet1/6	0.0.0.0/0		0 bps	0 bps
8	xethernet1/7	0.0.0.0/0		0 bps	0 bps
9	xethernet1/8	0.0.0.0/0		0 bps	0 bps
10	xethernet1/9	0.0.0.0/0		0 bps	0 bps

Customization

You can customize the dashboard display function or modify the function area location as needed.

- To customize the dashboard display function:

  1. Click **Customize** at the top-right corner.

  2. Select the function check box from the expanded list.

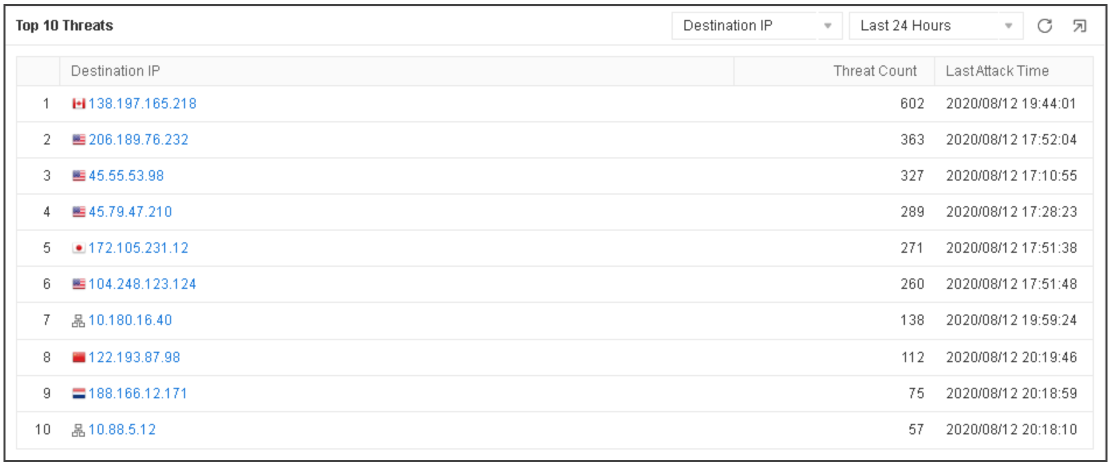
- To modify the function area location:

1. Hover your mouse over the title part in the ribbon.

2. When ✥ appears, press and hold the mouse functional area , the regional location to be displayed .

Threats

Display the top 10 threats information within the specified period.



Top 10 Threats

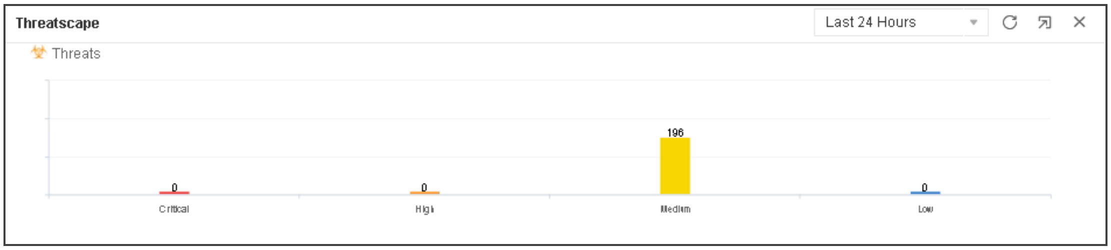
Destination IP ▾ Last 24 Hours ▾

	Destination IP	Threat Count	Last Attack Time
1	138.197.165.218	602	2020/08/12 19:44:01
2	206.189.76.232	363	2020/08/12 17:52:04
3	45.55.53.98	327	2020/08/12 17:10:55
4	45.79.47.210	289	2020/08/12 17:28:23
5	172.105.231.12	271	2020/08/12 17:51:38
6	104.248.123.124	260	2020/08/12 17:51:48
7	10.180.16.40	138	2020/08/12 19:59:24
8	122.193.87.98	112	2020/08/12 20:19:46
9	188.166.12.171	75	2020/08/12 20:18:59
10	10.88.5.12	57	2020/08/12 20:18:10

- Click Destination IP ▾ to specify the type of display: Destination IP, Source IP or Threat Name.

Threatscape

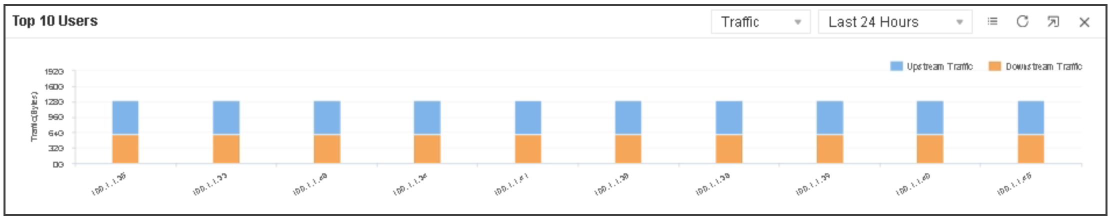
The threat information statistic chart is displayed within the specified period.



- Click the column to jump to the iCenter page, and the list will display the corresponding threat level.

User

Display the top 10 user traffic information within the specified period.

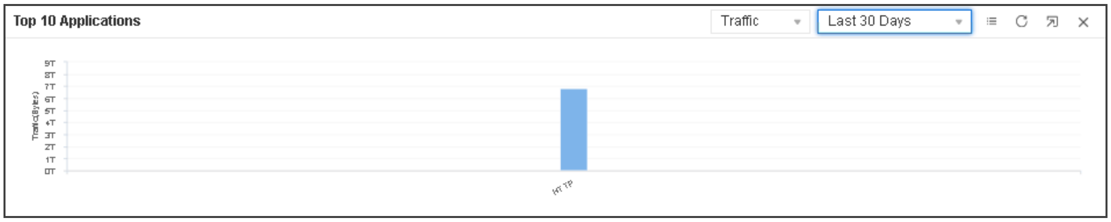


Top 10 Users

- Specify the type of display: by Traffic or by Concurrent Sessions from the drop-down menu.
- Click☰and 📊, switch between the table and the bar chart.
- Hover your mouse over a bar, to view users' upstream traffic, downstream traffic, total traffic or concurrent sessions.

Application

Display the top 10 application traffic information within the specified period.

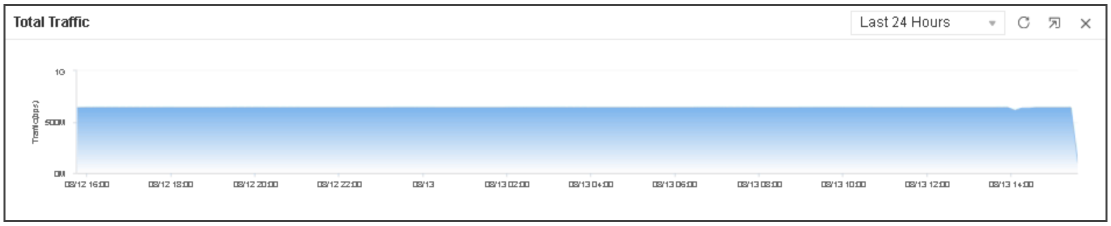


Top 10 Applications

- Specify the type of display: by Traffic or by concurrent sessions from the drop-down menu.
- Click☰and 📊, switch between the table and the bar chart.
- Hover your mouse over a bar, to view users' total traffic or concurrent sessions.

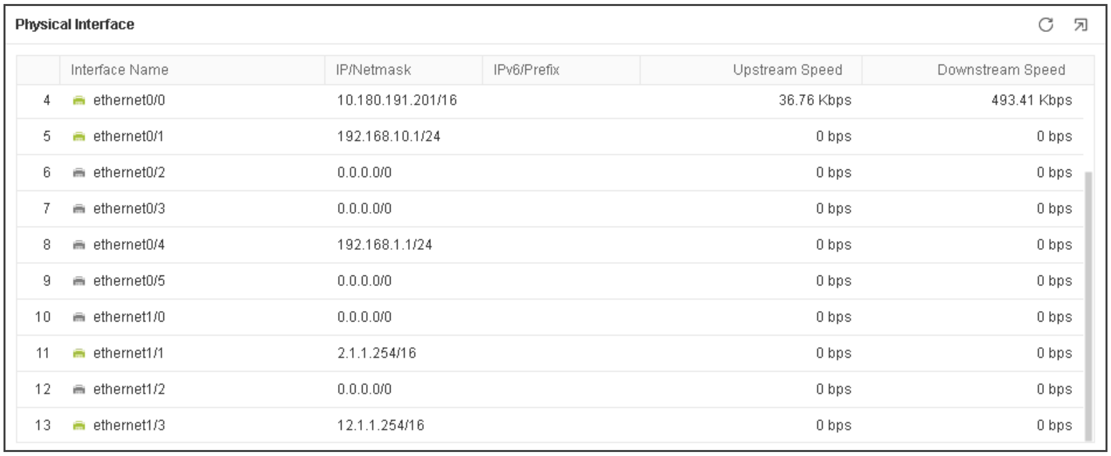
Total Traffic

Show the Total Traffic within the specified period .



Physical Interface

Display the statistical information of interfaces, including the interface name, IP address, upstream speed, downstream speed, and total speed.



	Interface Name	IP/Netmask	IPv6/Prefix	Upstream Speed	Downstream Speed
4	ethernet0/0	10.180.191.201/16		36.76 Kbps	493.41 Kbps
5	ethernet0/1	192.168.10.1/24		0 bps	0 bps
6	ethernet0/2	0.0.0.0/0		0 bps	0 bps
7	ethernet0/3	0.0.0.0/0		0 bps	0 bps
8	ethernet0/4	192.168.1.1/24		0 bps	0 bps
9	ethernet0/5	0.0.0.0/0		0 bps	0 bps
10	ethernet1/0	0.0.0.0/0		0 bps	0 bps
11	ethernet1/1	2.1.1.254/16		0 bps	0 bps
12	ethernet1/2	0.0.0.0/0		0 bps	0 bps
13	ethernet1/3	12.1.1.254/16		0 bps	0 bps

System and Signature Database

System Information

System information include.

- Serial number: The serial number of the device.
- Host name: The host name of the device.
- Platform: The platform type of the device.
- System Time: The time of system.
- System Uptime: The running time of system.

- HA State: The HA State of device:
    - Standalone: Non-HA mode which represents HA is disabled.
    - Init: Initial state.
    - Hello: Negotiation state which represents the device is negotiating the relationship between master and backup.
    - Master: Master state which represents current device is master.
    - Backup: Backup state which represents current device is backup.
    - Failed: Fault state which represents the device is failed.
- Firmware: The version number and version time of the firmware running on the device.
- Boot File: The boot file name.

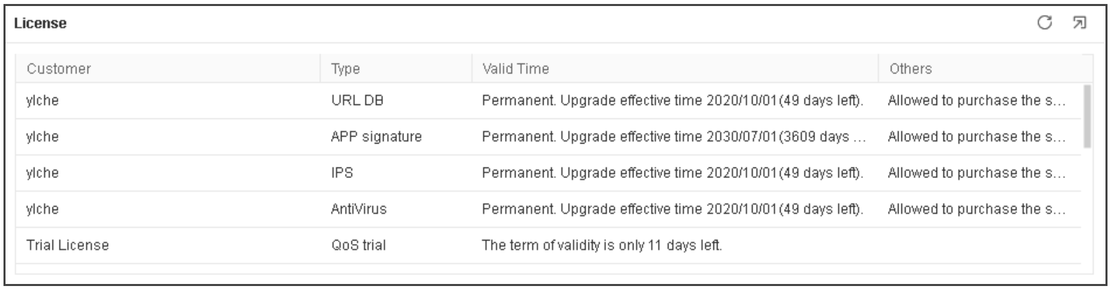
Signature DB Information

Signature database information include.

- Anti Virus Signature: The version number and time of the anti virus signature database.
- IPS Signature: The version number and time of the IPS signature database.
- URL Category Database: The version number and time of the URL category database.
- Application Signature: The version number and time of the application signature database.
- IP Reputation Database: The version number and time of the IP reputation database.

License

Display the detailed information of installed licenses.



License

Customer	Type	Valid Time	Others
ylche	URL DB	Permanent. Upgrade effective time 2020/10/01(49 days left).	Allowed to purchase the s...
ylche	APP signature	Permanent. Upgrade effective time 2030/07/01(3609 days ...	Allowed to purchase the s...
ylche	IPS	Permanent. Upgrade effective time 2020/10/01(49 days left).	Allowed to purchase the s...
ylche	AntiVirus	Permanent. Upgrade effective time 2020/10/01(49 days left).	Allowed to purchase the s...
Trial License	QoS trial	The term of validity is only 11 days left.	

- Customer: Displays the name of the customer who applied for the license.
- Type: Displays the type of license.
- Valid Time: Displays the valid time of license.
- Others: Displays additional notes for the license.

Specified Period

System supports the predefined time cycle and the custom time cycle. Click on the top right corner of each tab to set the time cycle.

- Realtime: Display the statistical information within 5 minutes of the current time.
- Last Hour: Display the statistical information within the latest 1 hour.
- Last Day: Display the statistical information within the latest 1 day.
- Last Month: Display the statistical information within the latest 1 month.
- Custom: Customize the time cycle. Select **Custom** and the **Custom Date and Time** dialog. Select the start time and the end time as needed.

In the top-right corner, you can set the refresh interface of the displayed data.

Notes: The specified period may vary slightly on different platforms and different statistical objects. Please see the actual page for the feature that your device delivers.

Chapter 4 iCenter

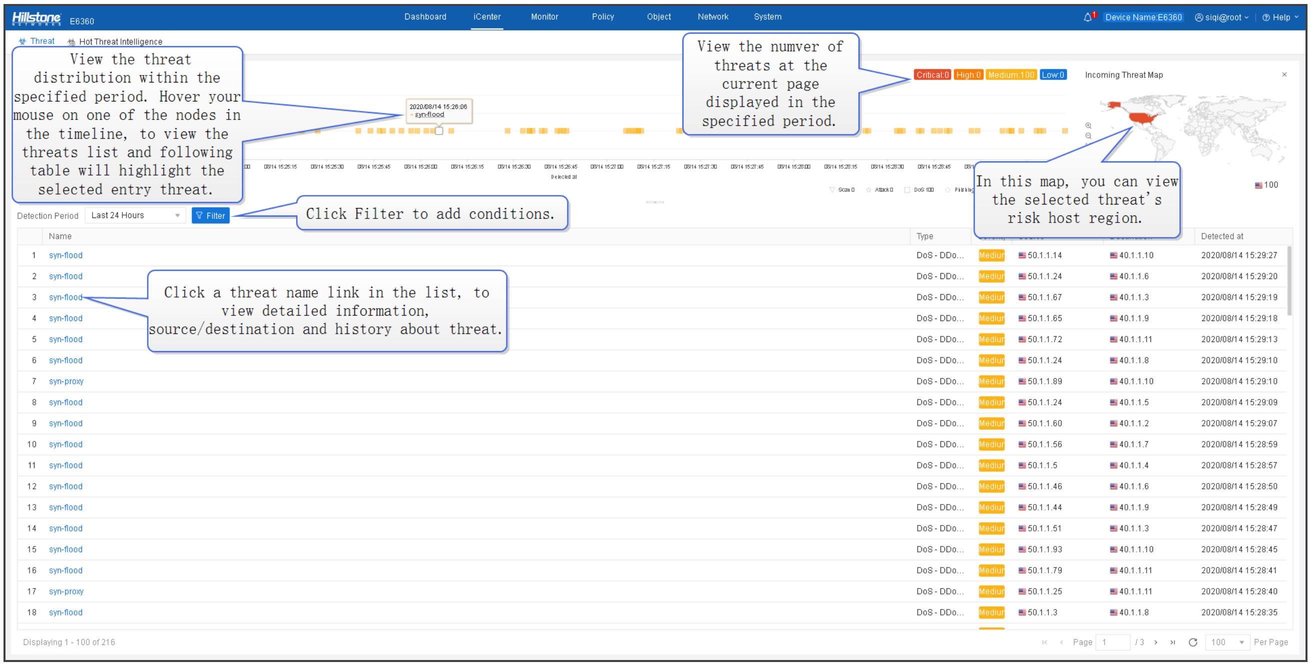
This feature may not be available on all platforms. Please check actual page in system to see whether your device delivers this feature.

The multi-dimensional features show threats to the whole network in depth. threats of the whole network.

If IPv6 function is enabled, you can view the threat information of IPv6 address through iCenter page.

Threat

Threats tab statistics and displays the all threats information of the whole network within the "Specified Period" on Page 61. Click **iCenter**.



View the threat distribution within the specified period. Hover your mouse on one of the nodes in the timeline, to view the threats list and following table will highlight the selected entry threat.

View the numver of threats at the current page displayed in the specified period.

In this map, you can view the selected threat's risk host region.

Click Filter to add conditions.

Click a threat name link in the list, to view detailed information, source/destination and history about threat.

	Name	Type				Detected at
1	syn-flood	DoS - DDo...	Mediur	50.1.1.14	40.1.1.10	2020/08/14 15:29:27
2	syn-flood	DoS - DDo...	Mediur	50.1.1.24	40.1.1.6	2020/08/14 15:29:20
3	syn-flood	DoS - DDo...	Mediur	50.1.1.67	40.1.1.3	2020/08/14 15:29:19
4	syn-flood	DoS - DDo...	Mediur	50.1.1.65	40.1.1.9	2020/08/14 15:29:18
5	syn-flood	DoS - DDo...	Mediur	50.1.1.72	40.1.1.11	2020/08/14 15:29:13
6	syn-flood	DoS - DDo...	Mediur	50.1.1.24	40.1.1.8	2020/08/14 15:29:10
7	syn-proxy	DoS - DDo...	Mediur	50.1.1.89	40.1.1.10	2020/08/14 15:29:10
8	syn-flood	DoS - DDo...	Mediur	50.1.1.24	40.1.1.5	2020/08/14 15:29:09
9	syn-flood	DoS - DDo...	Mediur	50.1.1.60	40.1.1.2	2020/08/14 15:29:07
10	syn-flood	DoS - DDo...	Mediur	50.1.1.56	40.1.1.7	2020/08/14 15:28:59
11	syn-flood	DoS - DDo...	Mediur	50.1.1.5	40.1.1.4	2020/08/14 15:28:57
12	syn-flood	DoS - DDo...	Mediur	50.1.1.46	40.1.1.6	2020/08/14 15:28:50
13	syn-flood	DoS - DDo...	Mediur	50.1.1.44	40.1.1.9	2020/08/14 15:28:49
14	syn-flood	DoS - DDo...	Mediur	50.1.1.51	40.1.1.3	2020/08/14 15:28:47
15	syn-flood	DoS - DDo...	Mediur	50.1.1.93	40.1.1.10	2020/08/14 15:28:45
16	syn-flood	DoS - DDo...	Mediur	50.1.1.79	40.1.1.11	2020/08/14 15:28:41
17	syn-proxy	DoS - DDo...	Mediur	50.1.1.25	40.1.1.11	2020/08/14 15:28:40
18	syn-flood	DoS - DDo...	Mediur	50.1.1.3	40.1.1.8	2020/08/14 15:28:35

Displaying 1 - 100 of 216

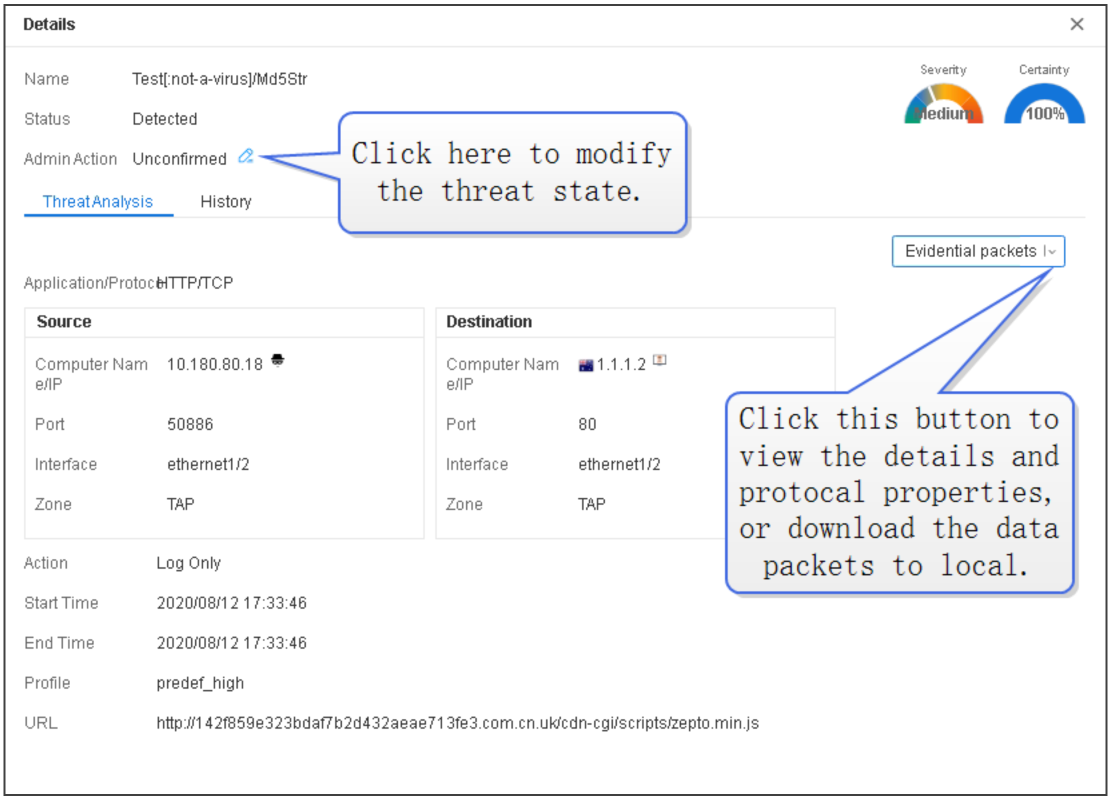
Page 1 / 3 100 Per Page

Click a threat name link in the list to view the detailed information , source/destination, knowledge base and history about the threat.

- Threat Analysis: Depending on the threats of the different detection engine , the content of

Threat Analysis tab is also different.

- **Anti Virus/IPS**: Display the detailed threat information .



Details

Name Test[:not-a-virus]/Md5Str

Status Detected

Admin Action Unconfirmed

Threat Analysis History

Application/ProtocolHTTP/TCP

Source		Destination	
Computer Name/IP	10.180.80.18	Computer Name/IP	1.1.1.2
Port	50886	Port	80
Interface	ethernet1/2	Interface	ethernet1/2
Zone	TAP	Zone	TAP

Action Log Only

Start Time 2020/08/12 17:33:46

End Time 2020/08/12 17:33:46

Profile predef_high

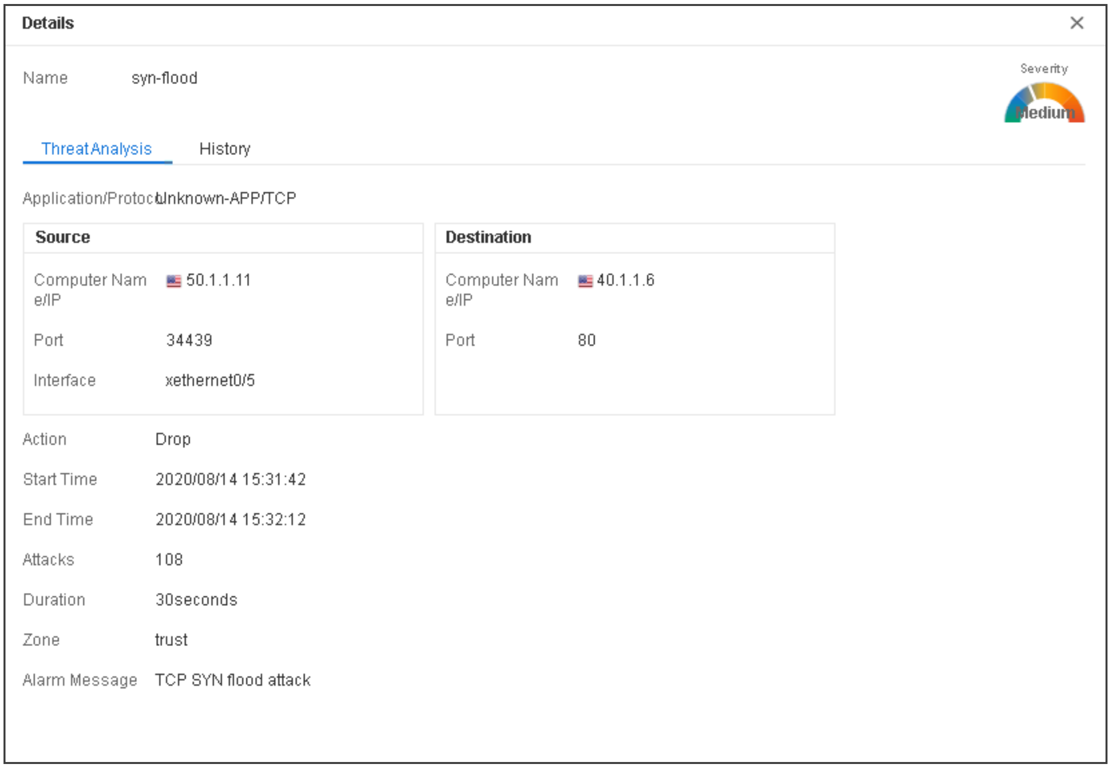
URL http://142f859e323bdaf7b2d432aeae713fe3.com.cn.uk/cdn-cgi/scripts/zepto.min.js

Click here to modify the threat state.

Click this button to view the details and protocal properties, or download the data packets to local.

For the Anti Virus/IPS function introduction, see "Anti-Virus" on Page 915/" Intrusion Prevention System" on Page 927.

- **Attack Defense/Perimeter Traffic Filtering**: Display the threat detailed information.



Name syn-flood

Application/Protocol Unknown-APP/TCP

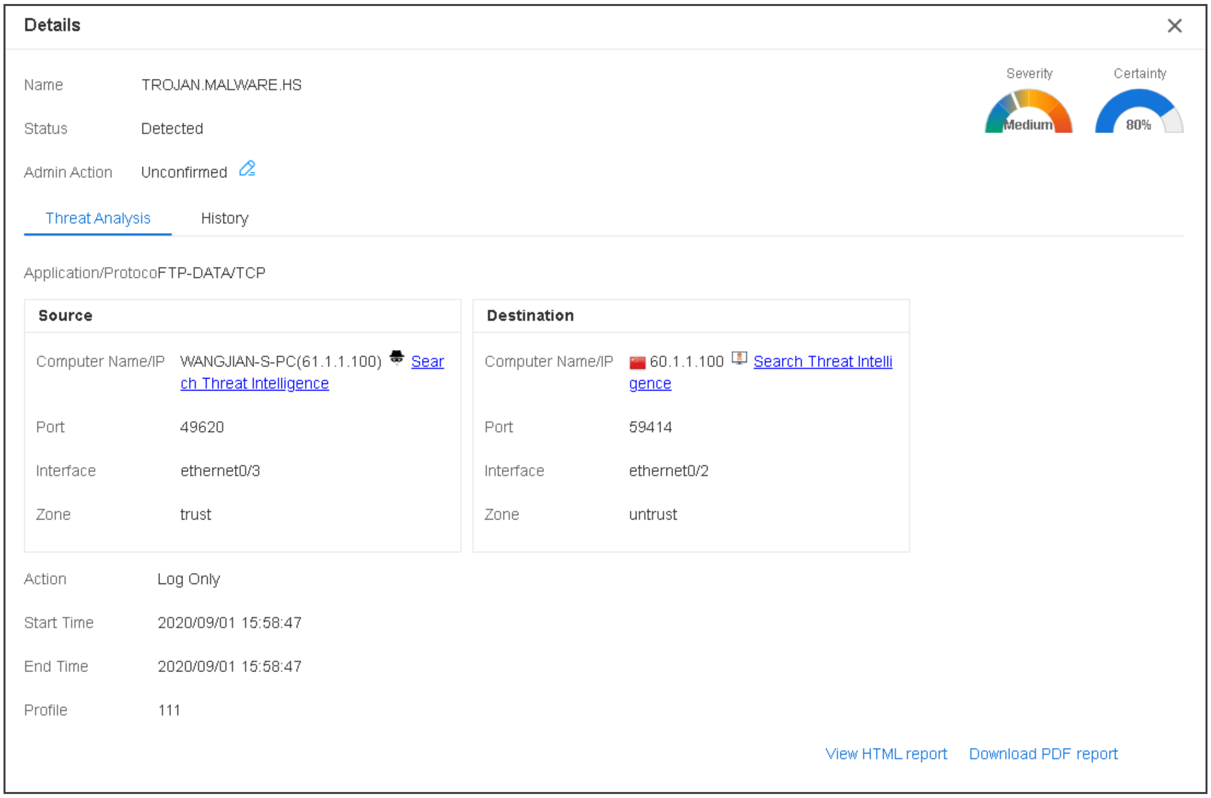
Source	
Computer Name/IP	50.1.1.11
Port	34439
Interface	xethernet0/5

Destination	
Computer Name/IP	40.1.1.6
Port	80

Action	Drop
Start Time	2020/08/14 15:31:42
End Time	2020/08/14 15:32:12
Attacks	108
Duration	30seconds
Zone	trust
Alarm Message	TCP SYN flood attack

For the Attack Defense/Perimeter Traffic Filtering function introduction, see "Attack-Defense" on Page 981/"Perimeter Traffic Filtering" on Page 1001.

- **Sandbox Threat Detection**: Display the detailed threat information of the suspicious file.



Details

Name TROJAN.MALWARE.HS

Status Detected

Admin Action Unconfirmed

Severity: Medium

Certainty: 80%

Application/ProtocoFTP-DATA/TCP

Source		Destination	
Computer Name/IP	WANGJIAN-S-PC(61.1.1.100) Search Threat Intelligence	Computer Name/IP	60.1.1.100 Search Threat Intelligence
Port	49620	Port	59414
Interface	ethernet0/3	Interface	ethernet0/2
Zone	trust	Zone	untrust

Action Log Only

Start Time 2020/09/01 15:58:47

End Time 2020/09/01 15:58:47

Profile 111

For the Sandbox function, see "Sandbox" on Page 971.

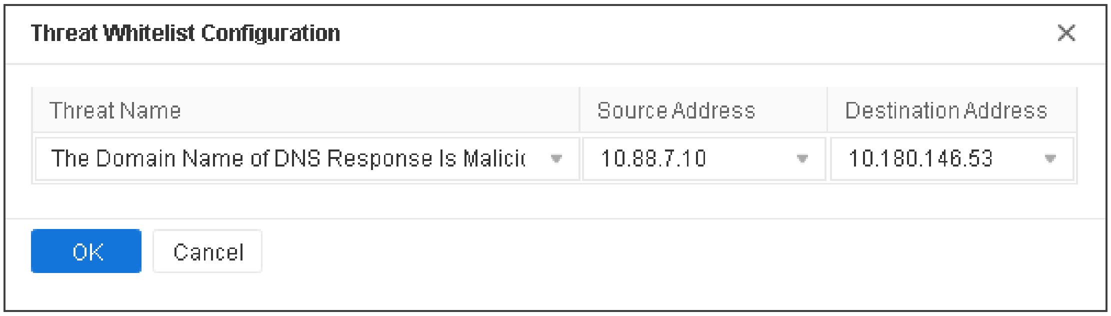
- Knowledge Base: Display the specified threat description, solution, etc. of the threats detected by IPS .
- Threat History: Display the selected threat historical information of the whole network .

Creating a White List

To create a threat white list, take the following steps:

1. Click **iCenter**, and select **Threat** tab.
2. Select the threat entries that need to be added to the white list, and click the threat name link in the list to open the **Threat** page.
3. Click ✎ to open the **Admin Analysis** page.

4. Click **Create White List** button.



Threat Whitelist Configuration

Threat Name	Source Address	Destination Address
The Domain Name of DNS Response Is Malicic	10.88.7.10	10.180.146.53

In the Threat White List Configuration page , enter the configurations

Option	Description
Threat Name	Specify the white list name. Click threat name, select the name in the drop-down list, which can be used as a threat name or **any** to whitelist name.
Source Address	Specify the white list source address to be matched. Click Source Address, select the source address of selected threat event or **any** in the drop-down list.
Destination Address	Specify the white list destination address to be matched. Click Destination Address, select the source address of selected threat event or **any** in the drop-down list.

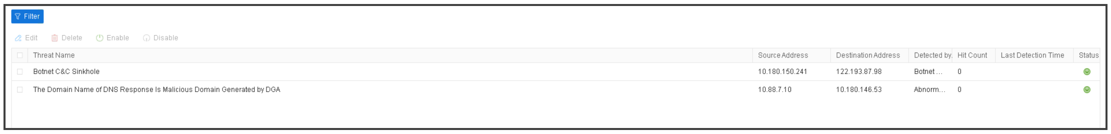
5. Click **OK**.

Viewing the White List

To view the threat white list entries, take the following steps:

1. Click **iCenter**.

2. Click **Whitelist Management** tab.



☐	Threat Name	Source Address	Destination Address	Detected by.	Hit Count	Last Detection Time	Status
☐	Botnet C&C Sinkhole	10.180.150.241	122.193.87.98	Botnet ...	0		●
☐	The Domain Name of DNS Response Is Malicious Domain Generated by DGA	10.88.7.10	10.180.146.53	Abnorm...	0		●

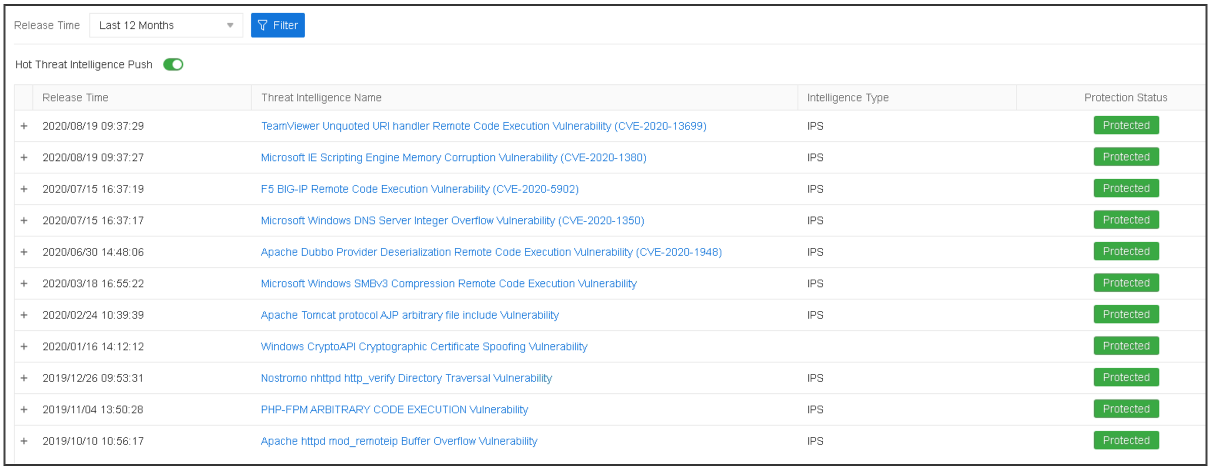
The information of white list

Option	Description
Threat Name	Displays the threat name of white list.
Source Address	Displays the source address of white list.
Destination Address	Displays the destination address of white list.
Detected by	Displays the detection engine.
Hit Count	Displays the hit count of white list entry.
Last Detection Time	Displays the last detection time of hit the threat white list.
Status	Displays the status of white list entry. ● indicates the status is enable , ○ indicates the status is disable.

Hot Threat Intelligence

Hot threat intelligence page displays the intelligence of hot threats on the Internet, including IPS vulnerability, virus and threats detected by the cloud sandbox. You can view the details of the hot threats, or carry out protection operations to prevent them.

Click **iCenter> Hot Threat Intelligence** to enter the Hot Threat Intelligence page. By default, the threats intelligence list shows the information of the latest year, including the release time, name, type, protection status and operation.



	Release Time	Threat Intelligence Name	Intelligence Type	Protection Status
+	2020/08/19 09:37:29	TeamViewer Unquoted URI handler Remote Code Execution Vulnerability (CVE-2020-13699)	IPS	Protected
+	2020/08/19 09:37:27	Microsoft IE Scripting Engine Memory Corruption Vulnerability (CVE-2020-1380)	IPS	Protected
+	2020/07/15 16:37:19	F5 BIG-IP Remote Code Execution Vulnerability (CVE-2020-5902)	IPS	Protected
+	2020/07/15 16:37:17	Microsoft Windows DNS Server Integer Overflow Vulnerability (CVE-2020-1350)	IPS	Protected
+	2020/06/30 14:48:06	Apache Dubbo Provider Deserialization Remote Code Execution Vulnerability (CVE-2020-1948)	IPS	Protected
+	2020/03/18 16:55:22	Microsoft Windows SMBv3 Compression Remote Code Execution Vulnerability	IPS	Protected
+	2020/02/24 10:39:39	Apache Tomcat protocol AJP arbitrary file include Vulnerability	IPS	Protected
+	2020/01/16 14:12:12	Windows CryptoAPI Cryptographic Certificate Spoofing Vulnerability		Protected
+	2019/12/26 09:53:31	Nostromo nhttpd http_verify Directory Traversal Vulnerability	IPS	Protected
+	2019/11/04 13:50:28	PHP-FPM ARBITRARY CODE EXECUTION Vulnerability	IPS	Protected
+	2019/10/10 10:56:17	Apache httpd mod_remoteip Buffer Overflow Vulnerability	IPS	Protected

- Select a time period from the **Release Time** drop-down list to filter the threat information of the specified time period. Click + Filter to add conditions to filter threat information as needed.

- Click the button after "Hot Threat Intelligence Push" . If it' s enabled, Hillstone Cloud server will push the latest hot threat intelligence to system , and once system gets threat intelligence from the Hillstone Cloud server, it will be notified in the form of pop-up window. Otherwise, Hillstone cloud platform will no longer push the latest hot threat intelligence. Meanwhile, the previously received threat intelligence can only be viewed, and relevant protective operations are not allowed.

- Select one threat intelligence item in the list and the corresponding threat details and protection logs will be displayed below the list.

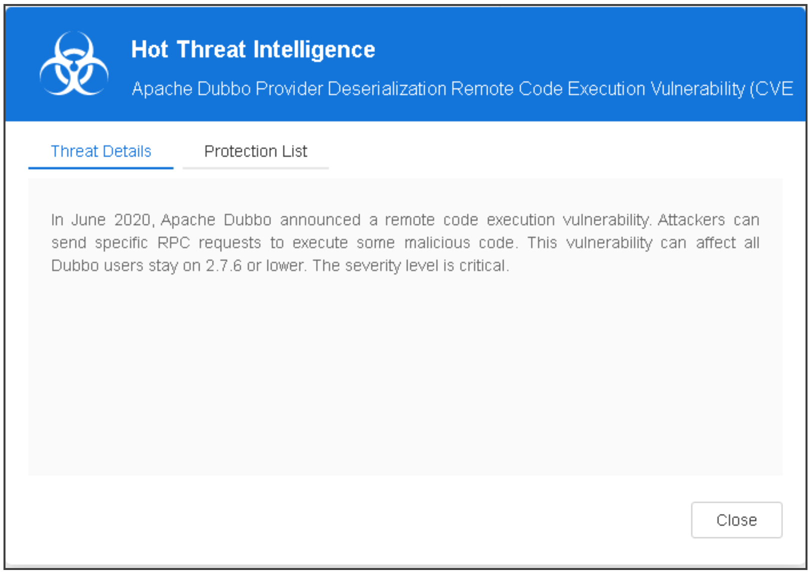
  - **Threat Details**: You can view the detailed threat information, including the release time ,the name, signature ID, severity, details, solutions, affected systems and other information (the items may vary slightly for different types of threat).

Option	Description
Release Time	Displays the release time of threat intelligence.

Option	Description
Threat Intelligence Name	Displays the threat intelligence name.
Signature ID	Displays the corresponded signature ID of the IPS signature database of the threat intelligence.
Severity	Displays the severity of threat intelligence.
Details	Displays the details of threat intelligence.
Solution	Displays the solutions to the threat .
Affected Systems	Displays the name of operating system that the threat will affect.
CVE ID	Displays the CVE ID and link of the threat. Click the link address, and a new page will be opened, where you can view the CVE details.
Reference Information	Displays links of the reference information about the threat. Click the link address and a new page will be opened, where you can view details of the reference information.

- **Protection Log**: If system has been attacked by the threat described in the threat intelligence in the latest month, the protection logs will be displayed. If not, the protection log is empty.

- Click the threat intelligence name in the list or the corresponded operation ("Protect Now" or "View Details") in the "Operation" column, and the < Hot Threat Intelligence > dialog box will pop up. You can view the information about the hot threat intelligence in the dialog.


Hot Threat Intelligence
Apache Dubbo Provider Deserialization Remote Code Execution Vulnerability (CVE
Threat Details
Protection List
Close

In June 2020, Apache Dubbo announced a remote code execution vulnerability. Attackers can send specific RPC requests to execute some malicious code. This vulnerability can affect all Dubbo users stay on 2.7.6 or lower. The severity level is critical.

- Click <Threat Summary> to view the information about the threat.

- For some threats in the "unprotected" status, you can see the corresponding protection solutions in the <Solution >tab. Click the links in sequence according to the steps in the solution, and configure the related functions. Only when you finish all the steps in one solutions (multiple solutions, at least one solution), the threat intelligence status will become "Protected".

  o For some threats in the "unprotected" status, the < Solutions> tab will not be displayed and you need to take the protective measures on other websites or servers, but system provides some solutions in the <Threats Details> tab. After the threat is protected, click **Confirm As Protected** button and the status of threat intelligence will be changed to "Protected".

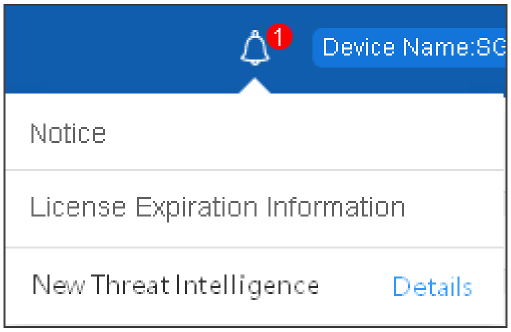
- For the threat in the "Protected" status, if it’ s protected by system, you can click < Protection List >to view the protective measures, and click "View Details" to view details of the protective measures.

Notes: Because the operation steps in the < Solution >tab are correlated, please follow the steps of the solution in turn. For example, if the signature database has not been upgraded, the signature ID will not be shown, and subsequent protections may be unavailable. Or after the signature database is upgraded, the subsequent steps may change or some of the subsequent steps may be omitted.

Viewing Hot Threat Intelligence

System will obtain and download the latest threat intelligence information from the Hillstone cloud server at the set time every day or when you log in to system, and the information will be upgraded in the hot threat intelligence list.

When you enable the "Hot Threat Hot Threat Intelligence Push" function, once system gets a new intelligence, the notice of New Threat Intelligence will display in the upper right corner of the page. Hover the mouse over the notification, click "details", and the page will jump to the hot threat intelligence page. On the **iCenter> Hot Threat Intelligence** page, the new threat intelligence will be displayed in the form of pop-up windows for users to view.



Chapter 5 Network

This chapter describes factors and configurations related to network connection, including:

- Security Zone: The security zone divides the network into different section, such as the trust zone and the untrust zone. The device can control the traffic flow from and to security zones once the configured policy rules have been applied.
- Interface: The interface allows inbound and outbound traffic flow to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone.
- MGT Interface: To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, system has an independent management interface(MGT Interface).
- VLAN: Virtual LAN.
- DNS: Domain Name System.
- DHCP: Dynamic Host Configuration Protocol.
- DDNS: Dynamic Domain Name Server.
- PPPoE: Point-to-Point Protocol over Ethernet.
- Virtual-Wire: The virtual wire allows direct Layer 2 communications between sub networks.
- Virtual Router: Virtual Routerouter (Virtual Router for short) acts as a router. Different Virtual Routers have their own independent routing tables.
- Virtual Switch: Running on Layer 2, VSwitch acts as a switch. Once a Layer 2 security zone is bound to a VSwitch, all the interfaces bound to that zone will also be bound to the VSwitch.

- Port Mirroring: Allow users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.

- WLAN: WLAN represents the local area network that uses the wireless channel as the medial. By configuring the WLAN function, you can establish the wireless local area network and allow the users to access LAN through wireless mode.

- 3G: By configuring the 3G function, users can access the Internet through the wireless mode.

- Link Load Balancing: It takes advantage of dynamic link detection technique to assign traffic to different links appropriately, thus making full use of all available link resources.

- Application Layer Gate: ALG can assure the data transmission for the applications that use multiple channels and assure the proper operation of VoIP applications in the strictest NAT mode.

- Global Network Parameters: These parameters mainly include the IP packet's processing options, like IP fragmentation, TCP MSS value, etc.

Security Zone

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

- An interface should be bound to a zone. A Layer 2 zone will be bound to a VSwitch, while a Layer 3 zone will be bound to a VRouter. Therefore, the VSwitch to which a Layer 2 zone is bound decides which VSwitch the interfaces belong to in that Layer 2 zone, and the VRouter to which a Layer 3 zone is bound decides which VRouter the interfaces belong to in that Layer 3 zone.
- Interfaces in Layer 2 and Layer 3 are working in Layer 2 mode and Layer 3 mode respectively.
- System supports internal zone policies, like trust-to-trust policy rule.

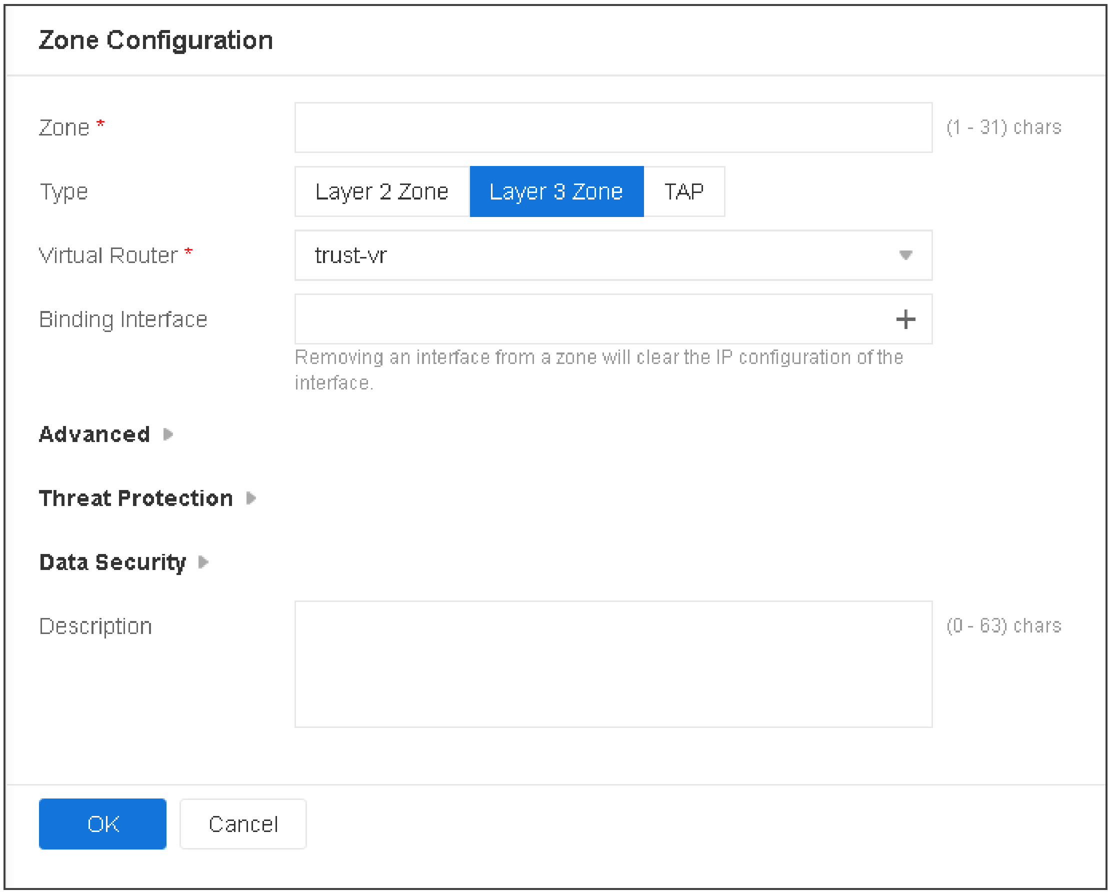
There are 8 pre-defined security zones in StoneOS, which are trust, untrust, dmz, L2-trust, L2-untrust, L2-dmz, vpnhub (VPN functional zone) and ha (HA functional zone). You can also customize security zones. Pre-defined security zones and user-defined security zones have no difference in functions, so you can make your choice freely.

Configuring a Security Zone

To create a security zone, take the following steps：

1. Select **Network** > **Zone**.

2. Click **New**.



Zone Configuration

Zone * (1 - 31) chars

Type: Layer 2 Zone | [✓ Layer 3 Zone] | TAP

Virtual Router * trust-vr

Binding Interface +

Removing an interface from a zone will clear the IP configuration of the interface.

Advanced ▸

Threat Protection ▸

Data Security ▸

Description (0 - 63) chars

3. In the Zone Configuration text box, type the name of the zone into the Zone box.

4. Type the descriptions of the zone in the Description text box.

5. Specify a type for the security zone. For a Layer 2 zone, select a VSwitch for the zone from the VSwitch drop-down list below; for a Layer-3 zone, select a VRouter from the Virtual Router drop-down list. If TAP is selected, the zone created is a tap zone, which is used in Bypass mode.

6. Bind interfaces to the zone. Select an interface from the Binding Interface drop-down list.

7. If needed, select the **Enable** button to enable APP identification for the zone.

8. If needed, select the **Enable** button to set the zone to a WAN zone, assuring the accuracy of the statistic analysis sets that are based on IP data.

9. If needed, select the **Enable** button to enable NetBIOS host query for the zone. For detailed instructions, see "DNS" on Page 164.

10. If needed, select Threat Protection tab and configure the parameters for Threat Protection function. For detailed instructions, see "Chapter 11 Threat Prevention" on Page 913.

11. If needed, select Data Security tab and configure the parameters for Data Security function. For detailed instructions, see "Data Security" on Page 688.

12. If needed, select End Point Prevention tab and configure the parameters for End Point Prevention function. For detailed instructions, see "End Point Protection" on Page 747.

13. If needed, select IoT Monitor tab and configure the parameters for IoT Monitor function. For detailed instructions, see "IoT Policy" on Page 758.

14. Click **OK**.

Notes:

- Pre-defined zones cannot be deleted.
- When changing the VSwitch to which a zone belong, make sure there is no binding interface in the zone.
- The interface bound to the Tap zone only monitor the traffic but does not forward the traffic, but when the device enters the Bypass state (such as system restart, abnormal operation, and device power off), the Bypass interface pair will be physically connected, and then the traffic will be forwarded to each

other. If you want to avoid this situation, try to avoid setting the pair of Bypass interfaces as the tap zone.

Interface

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

The security devices support various types of interfaces which are basically divided into physical and logical interfaces based on the nature.

- Physical Interface: Each Ethernet interface on devices represents a physical interface. The name of a physical interface, consisting of media type, slot number and location parameter, is pre-defined, like ethernet2/1 or ethernet0/2.
- Logical Interface: Include sub-interface, VSwitch interface, VLAN interface, loopback interface, tunnel interface, aggregate interface, redundant interface, PPPoE interface and Virtual Forward interface.

Interfaces can also be divided into Layer 2 interface and Layer 3 interface based on their security zones.

- Layer 2 Interface: Any interface in Layer 2 zone or VLAN.
- Layer 3 Interface: Any interface in Layer 3 zone. Only Layer 3 interfaces can operate in NAT/routing mode.

Different types of interfaces provide different functions, as described in the table below.

Type	Description
Sub-interface	The name of an sub-interface is an extension to the name of its original interface, like ethernet0/2.1. System supports the following types of sub-interfaces: Ethernet sub-interface, aggreg-

Type	Description
	ate sub-interface and redundant sub-interface. An interface and its sub-interfaces can be bound to one single security zone, or to different zones.
VSwitch interface	A Layer 3 interface that represents the collection of all the interfaces of a VSwitch. The VSwtich interface is virtually the upstream interface of a switch that implements packet forwarding between Layer 2 and Layer 3.
VLAN interface	A Layer 3 interface that represents the collection of all the Ethernet interfaces within a VLAN. If only one Ethernet interface is in UP state, the VLAN interface will be UP as well. The VLAN interface is the outbound communication interface for all the devices within a VLAN. Typically its IP address is the gateway's address of the network device within the VLAN.
Loopback interface	A logical interface. If only the security device with loopback interface configured is in the working state, the interface will be in the working state as well. Therefore, the loopback interface is featured with stability.
Tunnel interface	Only a Layer 3 interface, the tunnel interface acts as an ingress for VPN communications. Traffic flows into VPN tunnel through this interface.
Aggregate interface	Collection of physical interfaces that include 1 to 16 physical interfaces. These interfaces averagely share the traffic load to the IP address of the aggregate interface, in an attempt to increase the available bandwidth for a single IP address. If one of the physical interfaces within an aggregate interface fails, other physical interfaces can still process the traffic normally.

Type	Description
	The only effect is the available bandwidth will decrease.
Redundant interface	The redundant interface allows backup between two physical interfaces. One physical interface, acting as the primary interface, processes the inbound traffic, and another interface, acting as the alternative interface, will take over the processing if the primary interface fails.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.
Virtual Forward interface	In HA environment, the Virtual Forward interface is HA group's interface designed for traffic transmission.

The configuration options for different types of interfaces may vary. For more information, see the following instructions.

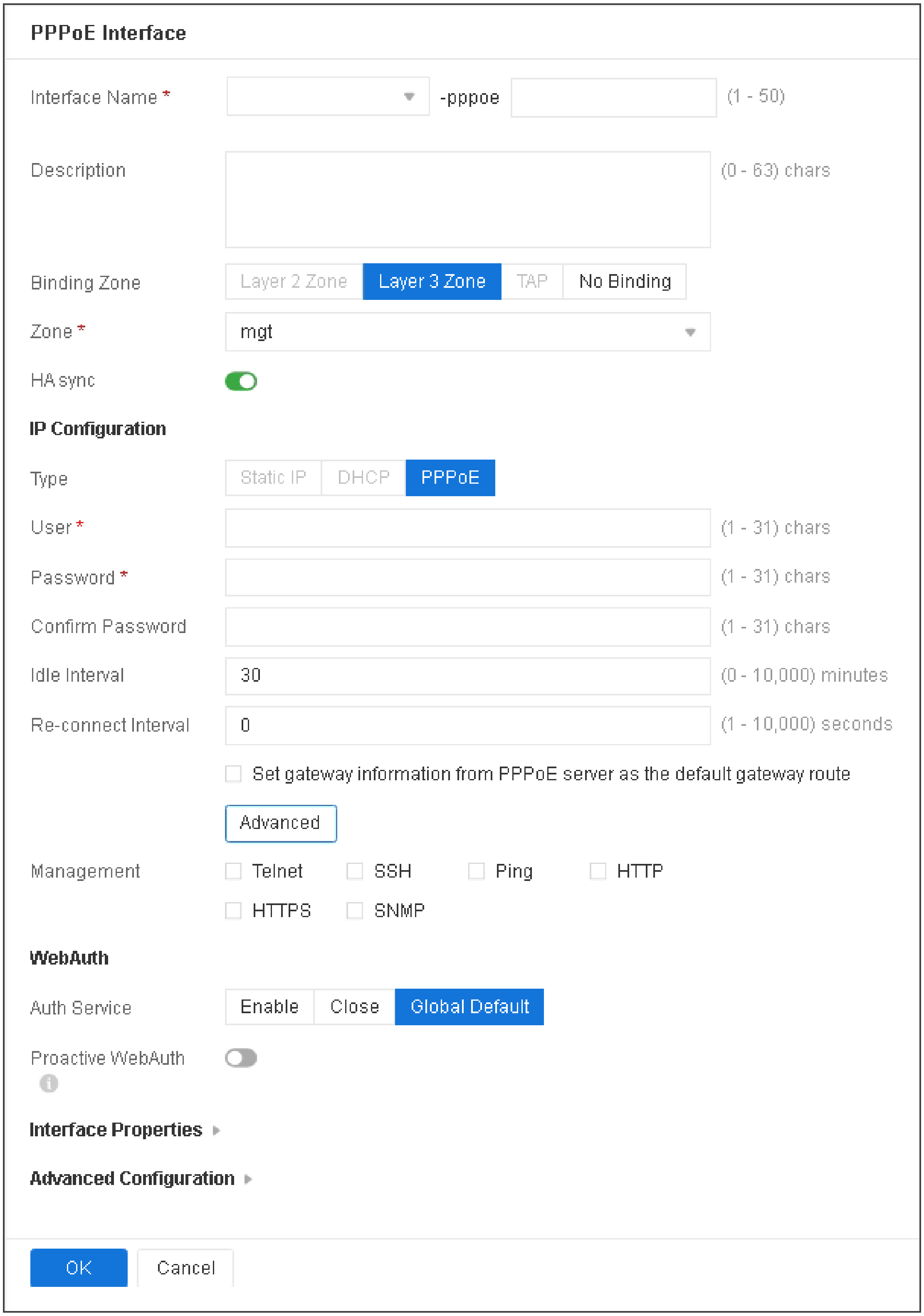
Both IPv4 and IPv6 address can be configured for the interface, but IPv6 address is not supported for the PPPoE interface.

Creating a PPPoE Interface

To create a PPPoE interface, take the following steps:

1. Select **Network > Interface**.

2. Click **New > PPPoE Interface**.



PPPoE Interface

Interface Name * -pppoe (1 - 50)

Description (0 - 63) chars

Binding Zone: Layer 2 Zone | [✓ Layer 3 Zone] | TAP | No Binding

Zone *: mgt

HA sync: on

IP Configuration

Type: Static IP | DHCP | [✓ PPPoE]

User * (1 - 31) chars

Password * (1 - 31) chars

Confirm Password (1 - 31) chars

Idle Interval: 30 (0 - 10,000) minutes

Re-connect Interval: 0 (1 - 10,000) seconds

□ Set gateway information from PPPoE server as the default gateway route

Advanced

Management: □ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

WebAuth

Auth Service: Enable | Close | [✓ Global Default]

Proactive WebAuth: off

Interface Properties ▸

Advanced Configuration ▸

OK Cancel

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 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	
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 cer-

Option	Description
	tain 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 30.
Re-connect interval	Specifies a re-connect interval (i.e., system will try to reconnect 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 selected check box, system will set the gateway information provided by PPPoE server as the default gateway route.
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, any-

Option	Description
	one 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.
DDNS	In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to

Option	Description
	configure the interface management method.
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" on Page 302.
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 con-

Option	Description
	figured 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.

Expand Interface Properties, configure properties for the interface.

Option	Description
Parameters	
ARP Learning	Click the **Enable** button to enable ARP learning.
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.
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 Band-	Specifies the maximum value of the down bandwidth of

Option	Description
width	the interface.

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: • 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

Option	Description
	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.
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. 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 flow-

Option	Description
	ing 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, 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.

Option	Description
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.

Option	Description
	• 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 des-

Option	Description
	ignated 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.

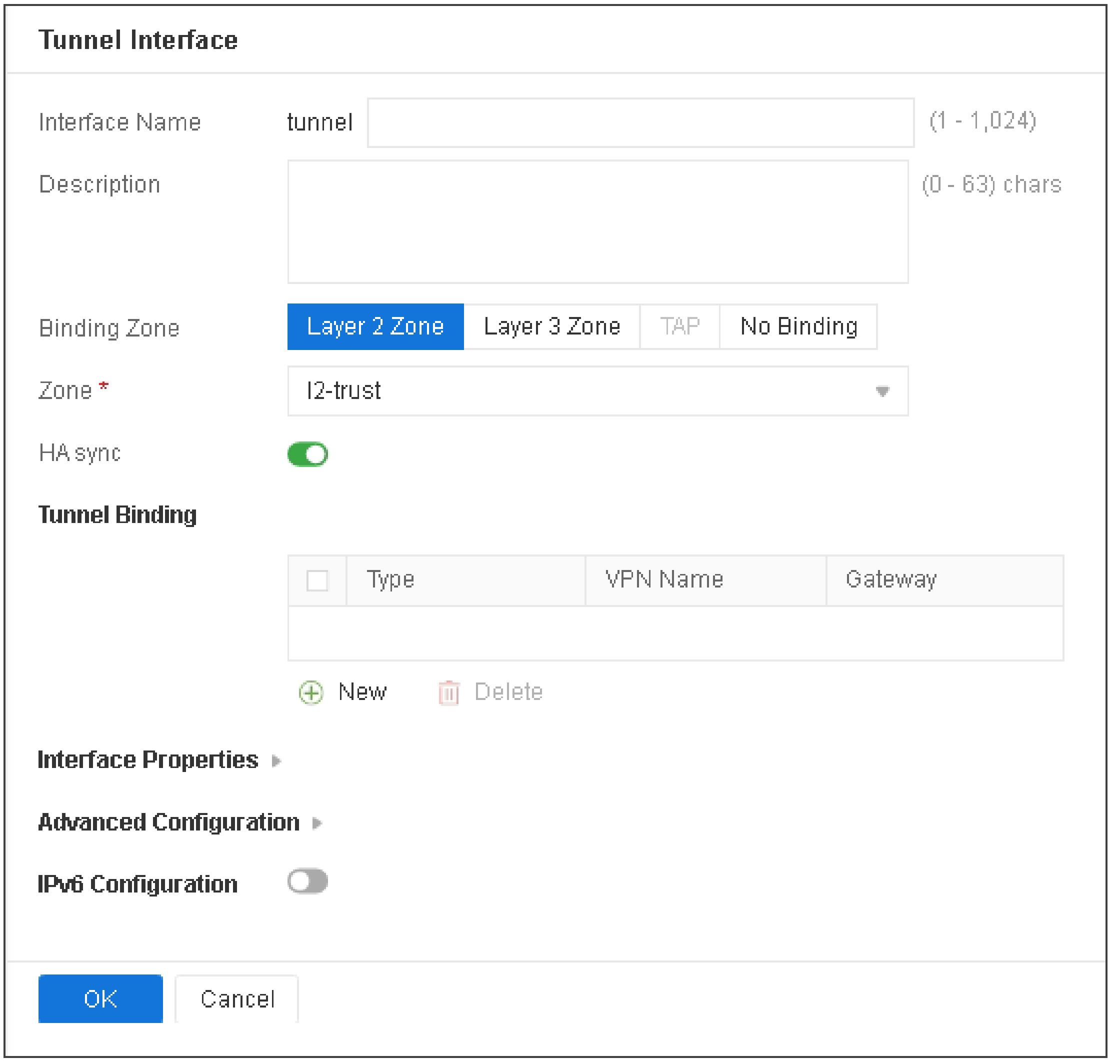
3. Click **OK**.

Creating a Tunnel Interface

To create a tunnel interface:

1. Select **Network > Interface.**

2. Select **New > Tunnel Interface.**



Tunnel Interface

Interface Name tunnel (1 - 1,024)

Description (0 - 63) chars

Binding Zone: Layer 2 Zone

Zone *: l2-trust

HA sync: on

Tunnel Binding

□	Type	VPN Name	Gateway

IPv6 Configuration: off

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the tunnel interface.
Description	Enter descriptions for the tunnel interface.

Option	Description
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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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.
Tunnel Binding	Bind the interface to a IPSec VPN tunnel or a SSL VPN tunnel. One tunnel interface can be bound to multiple IPSec VPN tunnels, while only to one SSL VPN tunnel. • 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.

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 Learning	Click the **Enable** button to enable ARP learning.
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.
Mirror	Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.

Option	Description
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.

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

Option	Description
	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 Enable DNS Proxy: Select this check box to enable DNS proxy for the interface.	
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.

Option	Description
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 unique available address. DAD (Duplicate Address Detection) is designed to verify

Option	Description
	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 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. "Creating a PPPoE Interface" on Page 81
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91
7. "OSPF" on Page 281
8. "Configuring OSPFv3" on Page 288
9. Click **OK**.

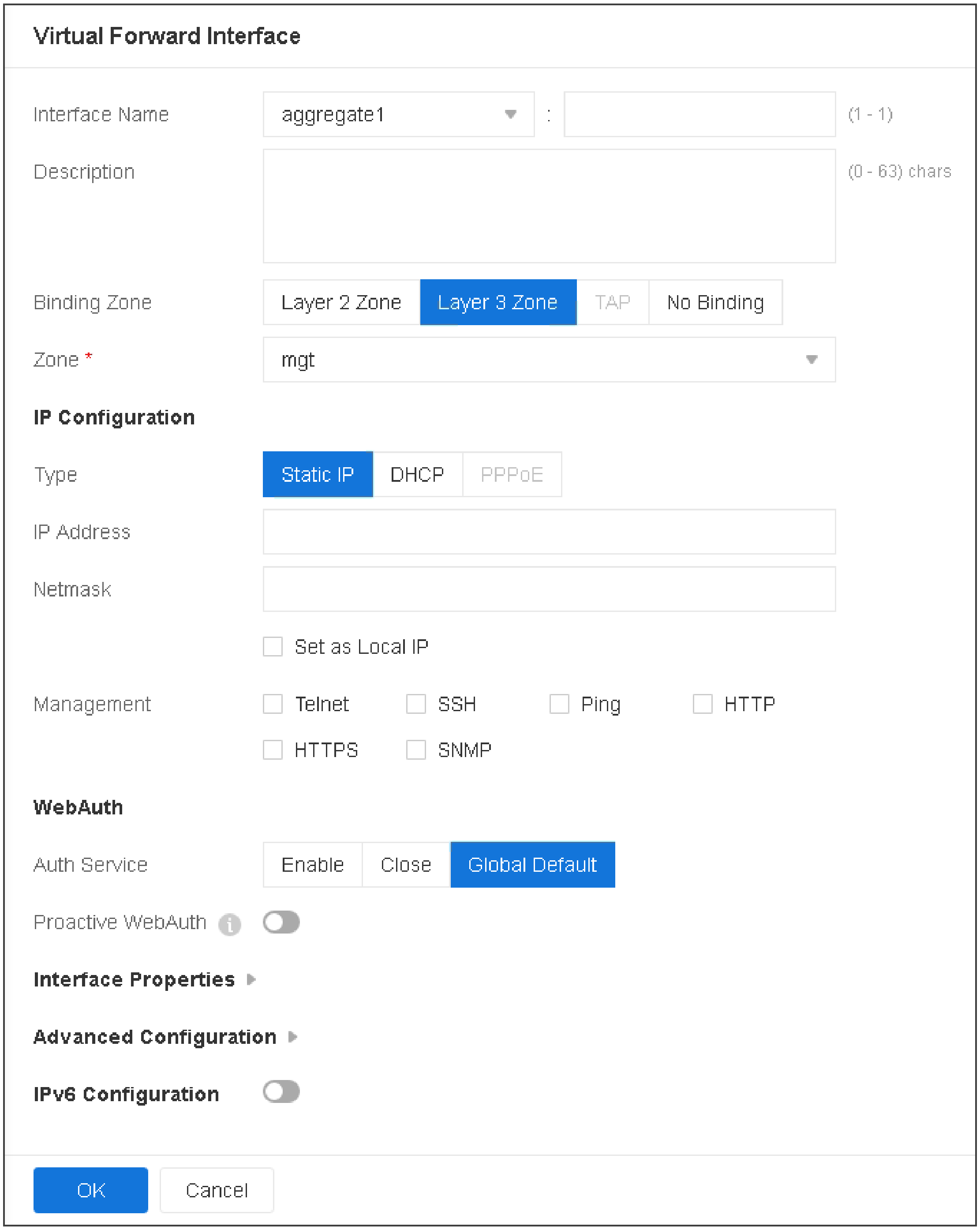
Creating a Virtual Forward Interface

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**.



Virtual Forward Interface

Interface Name: aggregate1 : (1 - 1)

Description: (0 - 63) chars

Binding Zone: Layer 2 Zone [✓ Layer 3 Zone] TAP No Binding

Zone *: mgt

IP Configuration

Type: [✓ Static IP] DHCP PPPoE

IP Address:

Netmask:

□ Set as Local IP

Management: □ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

WebAuth

Auth Service: Enable Close [✓ Global Default]

Proactive WebAuth

Interface Properties ▸

Advanced Configuration ▸

IPv6 Configuration

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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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.
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" on Page 302.
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

Option	Description
	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.

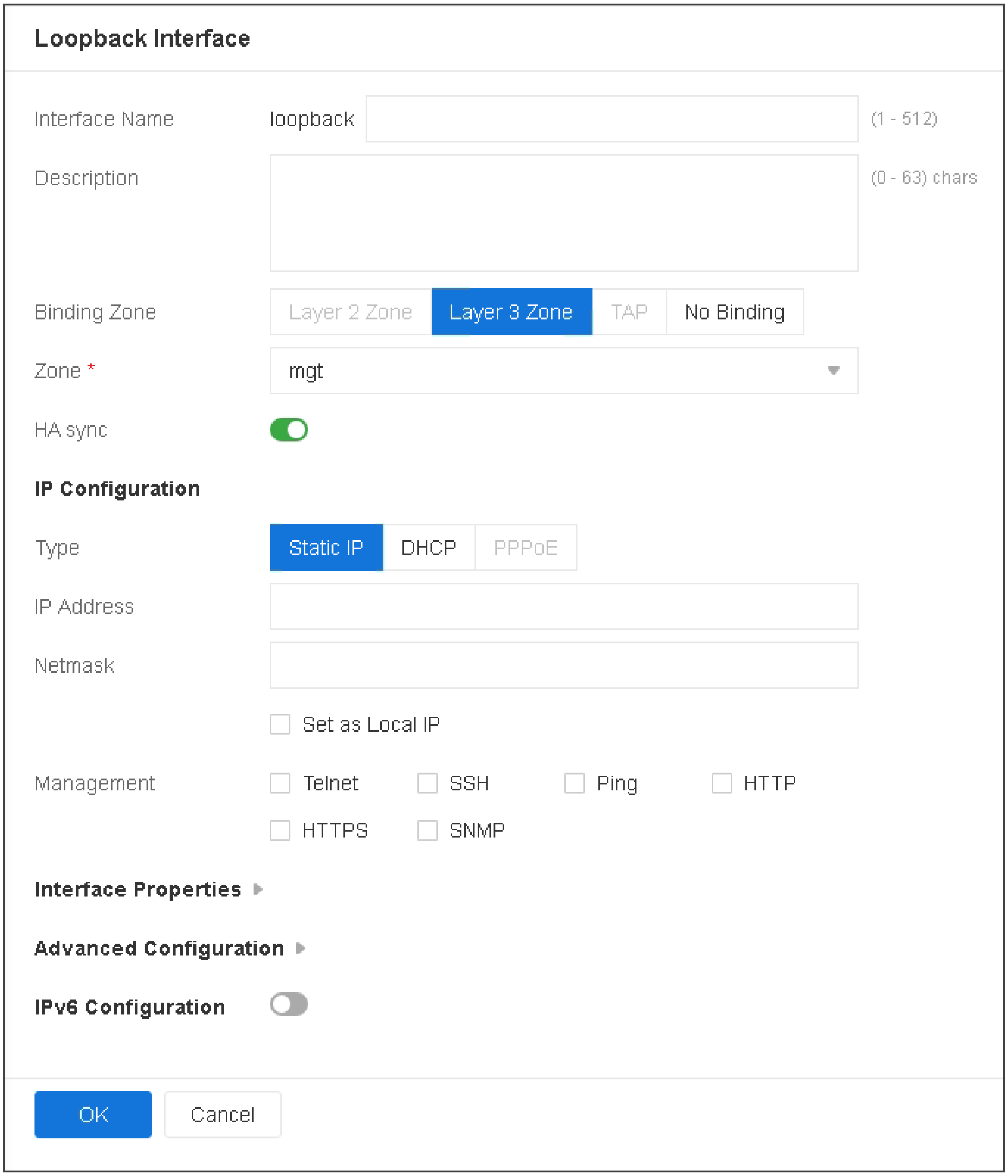
3. "Expand IPv6 Configuration, configure the following." on Page 101
4. "Expand Interface Properties, configure properties for the interface." on Page 99
5. "Creating a PPPoE Interface" on Page 81
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91
7. "OSPF" on Page 281
8. "Configuring OSPFv3" on Page 288
9. Click **OK**.

Creating a Loopback Interface

To create a loopback interface, take the following steps:

1. Select **Network** > **Interface**.

2. Click **New** > **Loopback Interface**.



Loopback Interface

Interface Name loopback (1 - 512)

Description (0 - 63) chars

Binding Zone Layer 2 Zone [✓ Layer 3 Zone] TAP No Binding

Zone * mgt

HA sync

IP Configuration

Type [✓ Static IP] DHCP PPPoE

IP Address

Netmask

□ Set as Local IP

Management □ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

Interface Properties

Advanced Configuration

IPv6 Configuration

OK Cancel

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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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.

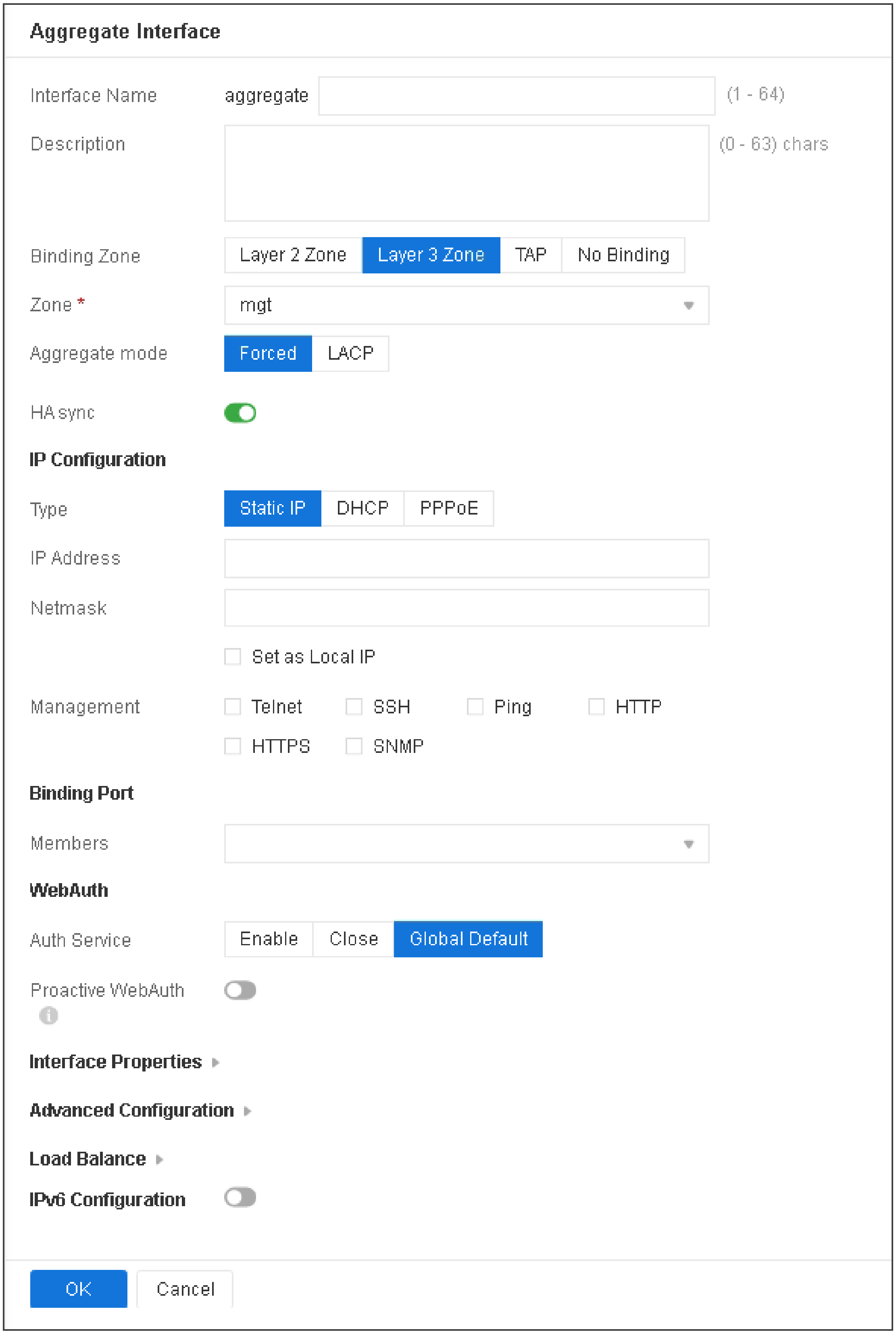
3. "Expand IPv6 Configuration, configure the following." on Page 101
4. "Expand Interface Properties, configure properties for the interface." on Page 99
5. "Creating a PPPoE Interface" on Page 81
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91
7. "OSPF" on Page 281
8. "Configuring OSPFv3" on Page 288
9. Click **OK**.

Creating an Aggregate Interface

To create an aggregate interface, take the following steps：

1. Select **Network > Interface**.

2. Click **New > Aggregate Interface**.



Aggregate Interface

Interface Name: aggregate ______ (1 - 64)

Description: ______ (0 - 63) chars

Binding Zone: Layer 2 Zone | [✓ Layer 3 Zone] | TAP | No Binding

Zone *: mgt

Aggregate mode: [✓ Forced] | LACP

HA sync: on

IP Configuration

Type: [✓ Static IP] | DHCP | PPPoE

IP Address: ______

Netmask: ______

□ Set as Local IP

Management: □ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

Binding Port

Members: ______

WebAuth

Auth Service: Enable | Close | [✓ Global Default]

Proactive WebAuth: off

Interface Properties ▸

Advanced Configuration ▸

Load Balance ▸

IPv6 Configuration: off

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.
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

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>VLAN/aggregate interface/redundant interface:
<table>
<tr><td>Belong to</td><td colspan="2">Description</td></tr>
<tr><td>VLAN</td><td>Acess mode (one VLAN)</td><td>The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</td></tr>
<tr><td></td><td>Trunk mode (multiple VLANs)</td><td>The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</td></tr>
<tr><td>Aggregate Interface</td><td colspan="2">The interface you specified belongs to an aggregate interface. Choose an aggregate interface which the aggregate interface belongs to from the Interface Group drop-down list.</td></tr>
<tr><td>Redundant Interface</td><td colspan="2">This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.</td></tr>
<tr><td>None</td><td colspan="2">This interface does not belong to any object.</td></tr>
</table></td></tr>
</table>

Option	Description
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 number, the status of other legal interfaces will change to

Option	Description
	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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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.

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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. Tip: This function is available only when you edit the interface.
PPPoE	Obtain IP through PPPoE。Configure the following options： • User - Specifies a username 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, the system will disconnect the Internet connection; 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 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.

Option	Description
	• Set gateway information from PPPoE server as the default gateway route - With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
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" on Page 302.
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

Option	Description
	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.

4. "Expand IPv6 Configuration, configure the following." on Page 101

5. "Expand Interface Properties, configure properties for the interface." on Page 99

6. "Creating a PPPoE Interface" on Page 81

7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91

8. "OSPF" on Page 281

9. "Configuring OSPFv3" on Page 288

10. 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.

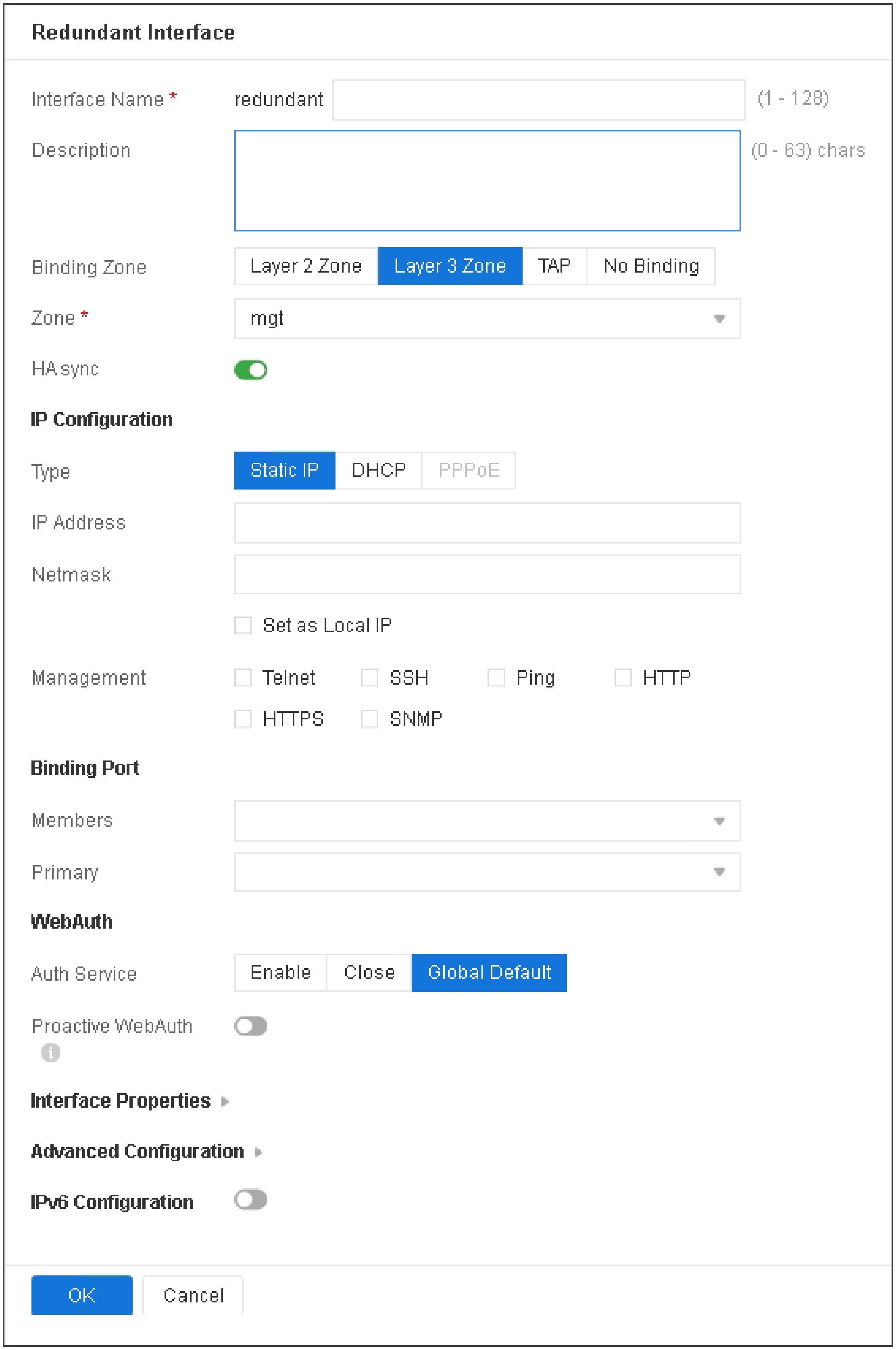
11. Click **OK**.

Creating a Redundant Interface

To create a redundant interface, take the following steps:

1. Select **Network > Interface**.

2. Click **New > Redundant Interface**.



Redundant Interface

Interface Name * redundant (1 - 128)

Description (0 - 63) chars

Binding Zone: Layer 2 Zone [✓ Layer 3 Zone] TAP No Binding

Zone *: mgt

HA sync: ●

IP Configuration

Type: [✓ Static IP] DHCP PPPoE

IP Address

Netmask

□ Set as Local IP

Management: □ Telnet □ SSH □ Ping □ HTTP □ HTTPS □ SNMP

Binding Port

Members

Primary

WebAuth

Auth Service: Enable Close [✓ Global Default]

Proactive WebAuth: ○

Interface Properties

Advanced Configuration

IPv6 Configuration: ○

OK Cancel

3. "In this page, configure the following." on Page 120

4. "Expand IPv6 Configuration, configure the following." on Page 101

5. "Expand Interface Properties, configure properties for the interface." on Page 99

6. "Creating a PPPoE Interface" on Page 81

7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91

8. "OSPF" on Page 281

9. "Configuring OSPFv3" on Page 288

10. 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	If Layer 2 zone or Layer 3 zone is selected, you should

Option	Description
Zone	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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. Tip: This function is available only when you edit the interface.
PPPoE	Obtain IP through PPPoE。Configure the following options：(Effective only when creating a aggregate subinterface) • User - Specifies a username 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, the 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

Option	Description
	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 selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
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" on Page 302.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you

Option	Description
	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.

4. "Expand IPv6 Configuration, configure the following." on Page 101

5. "Expand Interface Properties, configure properties for the interface." on Page 99

6. "Creating a PPPoE Interface" on Page 81

7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91

8. "OSPF" on Page 281

9. "Configuring OSPFv3" on Page 288

10. Click **OK**.

Creating a VSwitch Interface/a VLAN Interface

To create a VSwitch interface/a VLAN interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > VSwitch Interface/VLAN Interface**.
3. "In this page, configure the following." on Page 107
4. "Expand IPv6 Configuration, configure the following." on Page 101
5. "Expand Interface Properties, configure properties for the interface." on Page 99
6. "Creating a PPPoE Interface" on Page 81
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91
8. "OSPF" on Page 281
9. "Configuring OSPFv3" on Page 288
10. 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	Specifies a name for the interface.

Option	Description
Name	
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 IPve4 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;

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>Belong to</td><td colspan="2">Description</td></tr>
<tr><td>VLAN</td><td>Acess mode(one VLAN)</td><td>The interface in Access mode is designed for terminal users and only allows packets from one VLAN to pass through.</td></tr>
<tr><td></td><td>Trunk mode(multiple VLANs)</td><td>The interface in Trunk mode is typically used for inter-connections between devices, and allows packets from multiple VLANs to pass through. When Native VLAN is configured, the interface will delete the tag of the Native VLAN packets being transmitted, and add a Native VLAN tag to the received packets with no tag set.</td></tr>
<tr><td>Aggregate Interface</td><td colspan="2">The interface you specified belongs to a aggregate interface.
• Interface Group: Choose an aggregate interface which the aggregate interface belongs to from Interface Group drop-down list.
• Port LACP priority: Port LACP priority determines the sequence of</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>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 <b>Fast</b> (1 second) and <b>Slow</b> (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.
<table>
<tr><td>Redundant Interface</td><td>This interface belongs to a redundant interface. Select that redundant interface from the Interface Group drop-down list.</td></tr>
<tr><td>None</td><td>This interface does not belong to any object.</td></tr>
</table>
</td></tr>
</table>

Option	Description
Aggregare 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 number, the status of other legal interfaces will change to Standby.

Option	Description
	- 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 6 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 177.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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 learn 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 according to its 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. Tip: This function is available only when you edit the interface.
PPPoE	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. 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

Option	Description
	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 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.

Option	Description
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 192. 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.
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" on Page 302.
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

Option	Description
	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.

4. "Expand IPv6 Configuration, configure the following." on Page 101

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.

Property	Description
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 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.

Property	Description
ARP Learning	Select the Enable checkbox to enable ARP learning.
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.
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. "Creating a PPPoE Interface" on Page 81
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 91
8. "OSPF" on Page 281
9. "Configuring OSPFv3" on Page 288
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.

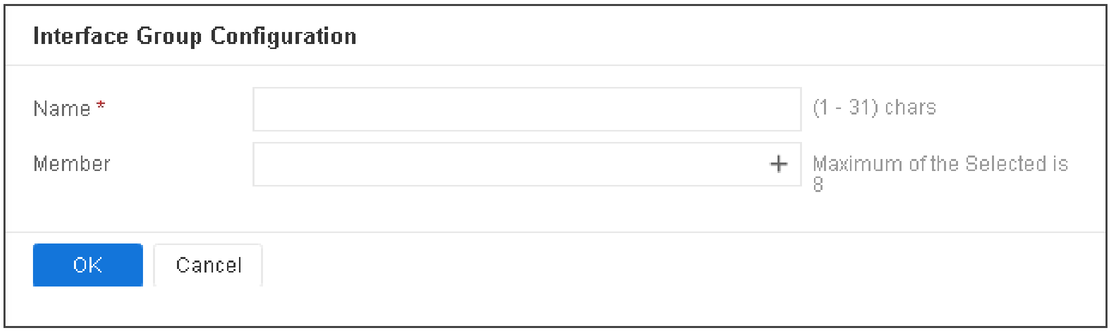
Interface Group

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

Creating an Interface Group

To create an interface group, take the following steps:

1. Select **Network** > **Interface Group**.
2. Click **New**.



Interface Group Configuration

Name *		(1 - 31) chars
Member	+	Maximum of the Selected is 8

3. In the Interface Group Configuration page, type the name for the interface group. Names of the interface group can not be the same.

4. In the **Member** drop-down list, select the interface you want to add to the interface group.

   The maximum number of interfaces is 8.

   Note: Members of an interface group can not conflict with other interface groups.

5. Click **OK**.

   You can click **Edit** or **Delete** button to edit the members of interface group or delete the interface group.

LLDP

Network devices are increasingly diverse, and their configurations are respectively complicate. Therefore, mutual discovery and interactions in information of system and configuration between devices of different manufacturers are necessary to facilitate management. LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol defined in IEEE 802.1ab, which provides a discovery method in link layer network. By means of the LLDP technology, the system can quickly master the information of topology and its changes of the layer-2 network when the scale of network expands rapidly.

By means of LLDP, the LLDP information of the device, including the device information, system name, system description, port description, network management address and so on, can be sent in the form of standard TLV (Type Length Value) multicast message from the physical port to the directly-connected neighbor. If the neighbor enables LLDP too, then neighbor relations will be established between both sides. When the neighbor receives these messages, they are stored in the form of MIB in the SNMP MIB database, in order to be utilized by the network management system to search and analyze the two-layer topology and the problems in it of the current network.

LLDP Work Mode

The 4 work modes of LLDP are listed below:

- Transmit and Receive: the port transmits and receives LLDP messages.
- Receive only: the port only receives LLDP messages.
- Transmit only: the port only transmits LLDP messages.
- Not work: the port neither transmits nor receives LLDP messages.

Related links:

- Configuring LLDP
- Viewing MIB Topology

Configuring LLDP

Configuring LLDP can enable neighbor devices' collection of network topology changes.

- Enabling LLDP
- Modifying LLDP Configuration

Enabling LLDP

LLDP is enabled only when the "Global LLDP" and the "LLDP of Port" are enabled at the same time, so the corresponding port can transmit and receive LLDP messages.

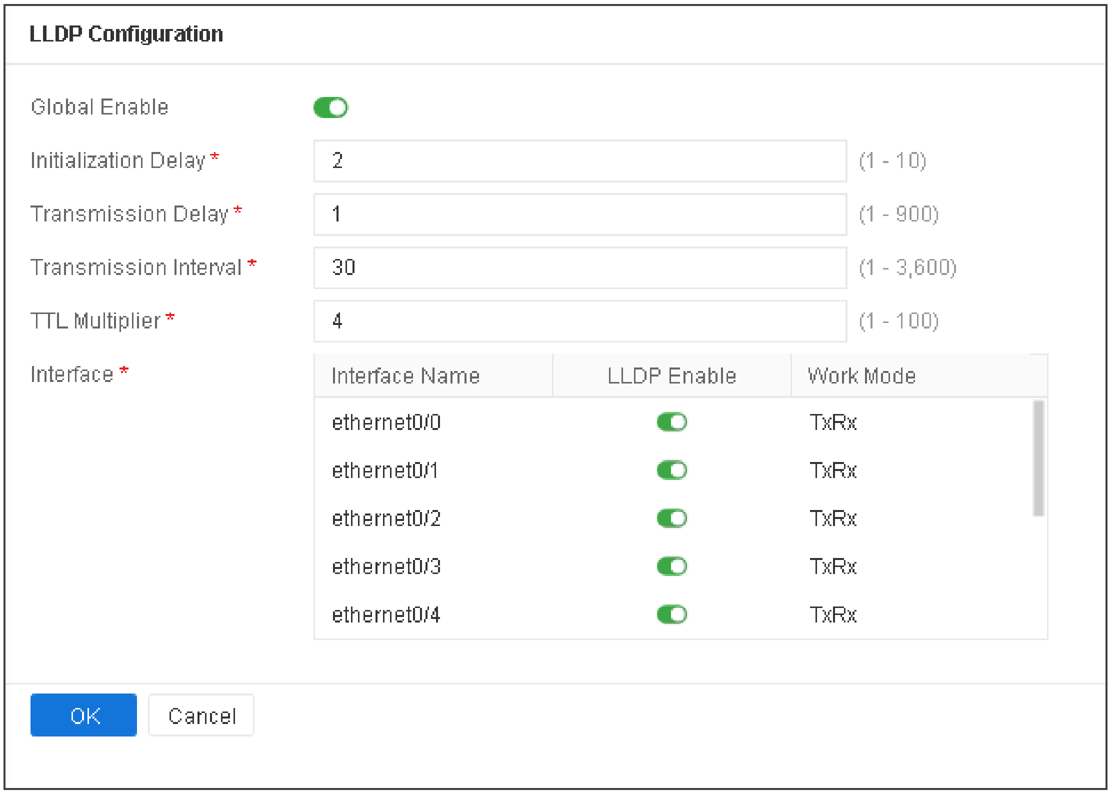
- By default, the global LLDP and the LLDP of port are both disabled.
- When the global LLDP is enabled, the LLDP of port of all the ports of the system will be enabled.
- When the global LLDP is disabled, the LLDP of port of all the ports of the system will be disabled.

- When the global LLDP is enabled, the user does not have to modify LLDP configuration, for LLDP can be enabled by default configuration. If there is a need to optimize LLDP configuration, please see Modifying LLDP Configuration.

Notes: Only the physical port of the device supports enabling LLDP. Logical port does not support this function.

To enable the global LLDP, take the following steps:

1. Select **Network > LLDP > LLDP Configuration**.
2. Click **Global Enable** button.



LLDP Configuration

Global Enable ●

Initialization Delay * 2 (1 - 10)

Transmission Delay * 1 (1 - 900)

Transmission Interval * 30 (1 - 3,600)

TTL Multiplier * 4 (1 - 100)

Interface *

Interface Name	LLDP Enable	Work Mode
ethernet0/0	●	TxRx
ethernet0/1	●	TxRx
ethernet0/2	●	TxRx
ethernet0/3	●	TxRx
ethernet0/4	●	TxRx

3. Click **OK** to enable LLDP by default configuration.

LLDP default configuration is as follows:

Option	Default
Initialization Delay	2 seconds
Transmission Delay	1 seconds
Transmission Interval	30 seconds
TTL Multiplier	4 seconds
port	LLDP is enabled in all the physical ports with the work mode being Transmit and Receive.

Modifying LLDP Configuration

According to the loading condition of network, the user can modify related LLDP configuration to reduce the consumption of system resources and optimize the LLDP performance.

To modify LLDP configuration, take the following steps:

- Select **Network > LLDP > LLDP Configuration**.

In the LLDP Configuration page, configure as follows:

Option	Description
Initialization Delay	When the LLDP work mode of the port changes, the system will operate initialization on the port. Configuring the initialization delay of the port can avoid continuous initialization of the port due to frequent changes of the LLDP work mode.

Option	Description
	Type the delay time of initialization of the port in the **Initialization Delay** text box. The measurement is second-based, and the range is from 1 to 10.
Transmission Delay	Transmission delay refers to the minimal delay time before the LLDP messages are sent to the neighbor device when the state of the local device frequently changes. Type the minimal delay time before the LLDP message is sent in the **Transmission Delay** text box. The measurement is second-based, and the range is from 1 to 900.
Transmission Interval	Transmission interval refers to the time period of transmitting the LLDP message to the neighbor device when the state of the local device state remains stable. Type the transmission period before the LLDP message is sent in the **Transmission Interval** text box. The measurement is second-based, and the range is from 1 to 3600.
TTL Multiplier	TTL (Time to Live) refers to the living time of the local device information in the neighbor device. TTL multiplier is used to adjust the living time of the local device information in the neighbor device. The computational formula is: TTL = Transmission Interval × TTL Multiplier. Type the TTL multiplier value in the **TTL Multiplier** text box. The range is from 1 to 100.
port	Click the Enable button under **LLDP Enable** to enable the

Option	Description
	LLDP function of the port. Select LLDP work mode from the **Work Mode** drop-down menu to modify the LLDP work mode of the port. **Note**: For the introduction of the LLDP work mode, please see LLDP Work Mode.

- Click **OK**.

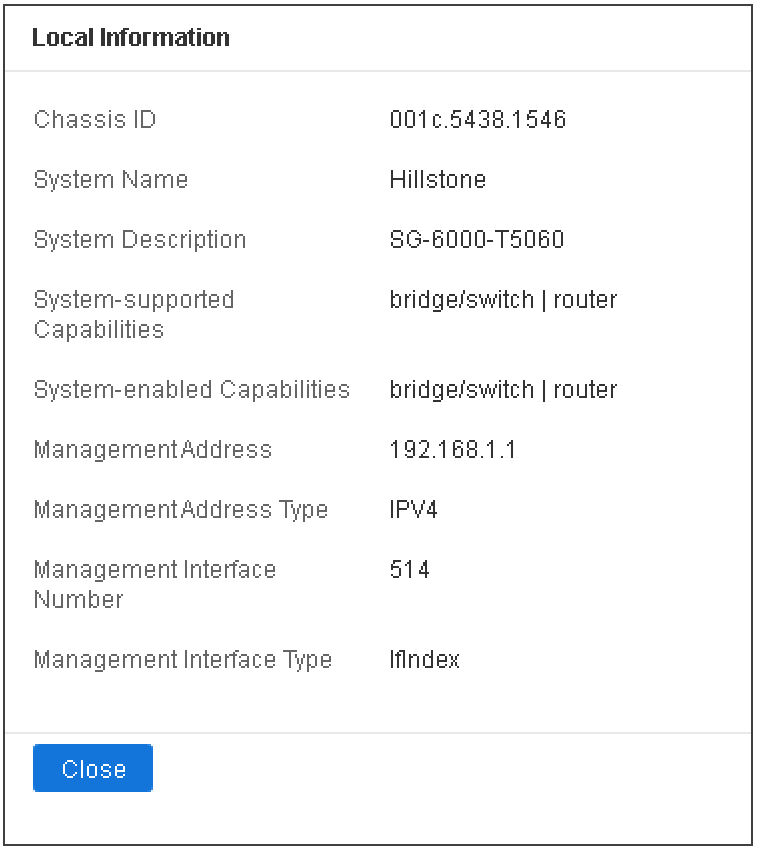
Viewing MIB Topology

The user can view the LLDP local information and the neighbor information (the LLDP information sent from the neighbor device to the local device) of the port in the **MIB Topology** page.

To view the MIB topology, take the following steps.

1. Select **Network > LLDP > MIB Topology**.
2. Click the **Local Information** button to open the **Local Information** page and view the LLDP local information, including chassis ID, system name, system description, system-supported

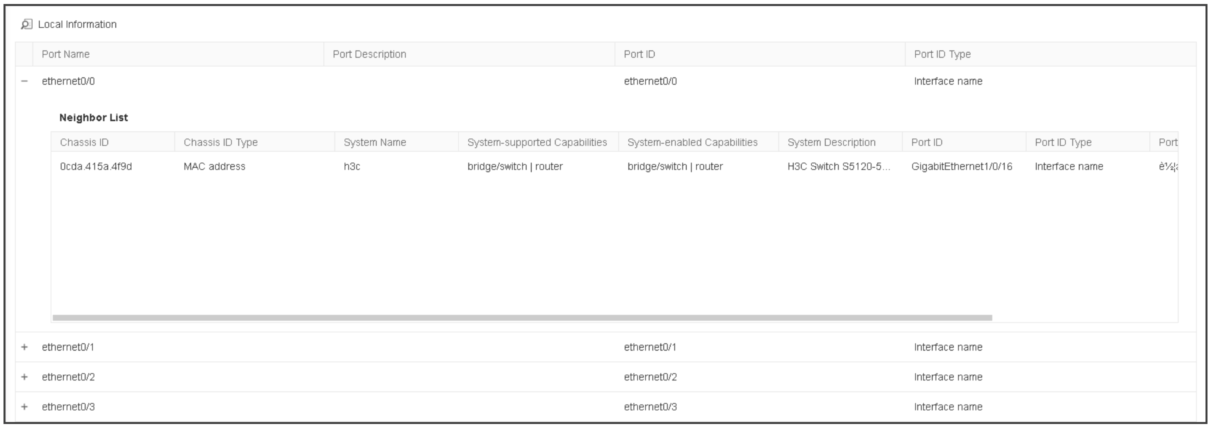
capabilities, management address and so on.



Local Information

Chassis ID	001c.5438.1546
System Name	Hillstone
System Description	SG-6000-T5060
System-supported Capabilities	bridge/switch | router
System-enabled Capabilities	bridge/switch | router
ManagementAddress	192.168.1.1
ManagementAddress Type	IPV4
Management Interface Number	514
Management Interface Type	IfIndex

3. View the MIB topology and neighbor information of all the ports which enable LLDP in the list in the **MIB Topology** page.



Local Information

	Port Name	Port Description	Port ID	Port ID Type
−	ethernet0/0		ethernet0/0	Interface name

Neighbor List

Chassis ID	Chassis ID Type	System Name	System-supported Capabilities	System-enabled Capabilities	System Description	Port ID	Port ID Type	Port
0cda.415a.4f9d	MAC address	h3c	bridge/switch | router	bridge/switch | router	H3C Switch S5120-5...	GigabitEthernet1/0/16	Interface name	è½¦

	Port Name	Port Description	Port ID	Port ID Type
+	ethernet0/1		ethernet0/1	Interface name
+	ethernet0/2		ethernet0/2	Interface name
+	ethernet0/3		ethernet0/3	Interface name

Management Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, the system has an independent management interface (MGT Interface). By default, the management interface belongs to the mgt zone and the mgt-vr virtual router. The mgt zone belongs to the mgt-vr virtual router, the information of routing, ARP table are independent.

Configuring a Management Interface

To configure a MGT interface, take the following steps:

1. Select **Network > Management Interface**.
2. To create the virtual forward interface of MGT0, select **Virtual Forward Interface** from the **New** drop-down list, and the **Virtual Forward Interface** page pops up; To edit interface, select the interface and click **Edit**, and the **MGT Interface** page pops up.
3. Specify the zone for the management interface in the Zone drop-down list. You can only select a Layer 3 zone. By default, the interface is bound in the mgt zone.
4. Click the **Enable** 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.
5. Select a configured NetFlow profile from the **NetFlow Configuration** drop-down list.
6. Specify the method of obtaining IP address in the IP Configuration section. "Static IP" means specifying a static IP address and the netmask. Click **Advanced** to specify the

secondary IP address into the text box. You can specify up to 6 secondary IP addresses. "Auto-obtain" means obtaining the IP address through DHCP.

7. Specify the management methods by selecting the "Telnet/SSH/Ping/HTTP/HTTPS/SNMP" check boxes of the desired management methods.
8. Specify the mode and rate of the management interface. If you select the Auto duplex transmission mode , you can only select the Auto rate.
9. Select the Shut Down check box to shut down the management interface.
10. Click **OK**.

VLAN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

VLAN, the abbreviation for Virtual Local Area Network, is defined in IEEE 802.1Q. VLAN has the following features:

- A physical LAN can be divided into multiple VLANs, and a VLAN might include devices from multiple physical networks.
- A VLAN is virtually a broadcast domain. Layer 2 packets between VLANs are isolated. Communication between VLANs can only be implemented by a Layer 3 route technique (through routers, Layer 3 switches, or other Layer 3 network devices).

VLANs are distinguished by VLAN numbers. The value range is 1 to 4094. System reserves 32 VLAN numbers (224 to 255) for BGroup, but the unused numbers within the range are also available to VLANs.

Configuring a VLAN

To create a VLAN, take the following steps:

1. Select **Network > VLAN**.
2. Click **New**.

   In the VLAN Configuration page, type a number in the VLAN ID text box, the value range is from 1 to 4094.
3. Click **OK**.

DNS

DNS, the abbreviation for Domain Name System, is a computer and network service naming system in form of domain hierarchy. DNS is designed for TCP/IP network to query for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.

The security device's DNS provides the following functions:

- Server: Configures DNS servers and default domain names for the security device.
- Proxy:As a DNS proxy, the device can filter the DNS request according to the DNS proxy rules set by the user, and system will forwarded the qualified DNS request to the designated DNS server.
- Analysis: Sets retry times and timeout for device's DNS service.
- Cache: DNS mappings to cache can speed up query. You can create, edit and delete DNS mappings.
- NBT Cache: Displays NBT cache information.

Configuring a DNS Server

You can configure a DNS server for system to implement DNS resolution. To create a DNS server, take the following steps:

1. Select **Network > DNS > DNS Server**.
2. Click **New** in the DNS Server section.
3. In the <DNS Server Configuration> page, type the IP address for the DNS server into the Server IP box.

4. Select a VRouter from the VR drop-down list. The default VRouter is trust-vr.

5. Click **OK**.

Configuring a DNS Proxy

DNS Proxy function take effect by the DNS proxy rules.Generally a proxy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's ingress interface , source address, destination address, and domain name. The action of the DNS proxy rules includes proxy,bypass and block. When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers, so that the DNS request meeting the filtering condition will be resolved by these DNS proxy servers.

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	Specify the ingress interface of DNS request in the rule to filter the DNS request message.It is permissible to specify numbers of interfaces.
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

Option	Description
	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. - 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

Option	Description
	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 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. - 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.

Option	Description
	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 configuration 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, 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.
DNS Server	Specify the DNS proxy server. When the action of the

Option	Description
	proxy rule is specified as proxy, you need to configure the DNS proxy servers. You can specify up to six DNS server and you can configure the interface and preferred properties for the DNS server as needed. When you configure multiple DNS servers, the DNS server with preferred property will be selected for domain name resolution. If no preferred server is specified, the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin. Except for these two kinds of DNS servers, which means that there are only regular DNS server, then system will select this kind of DNS servers in a round robin. At the bottom of the DNS server list, click the "+" button, and a table entry will be added. Enter the IP address (IPv4 address or IPv6 address) of server and other parameters ,such as the virtual router.
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.

Option	Description
	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 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**.

Enabling/Disabling a DNS Proxy Rule

DNS proxy rule is enabled by default. To disable or enable the function, take the following steps:

1. Select **Network > DNS > DNS Proxy**.

2. Select the rule that you want to enable/disable.

3. Click **Enable** or **Disable** to enable or disable the rule.

Adjusting DNS Proxy Rule Position

To adjust the rule position, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Select the check box of the security policy whose position will be adjusted.
3. Click **Priority**.
4. In the pop-up menu, 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.

DNS Proxy Global Configuration

To set the DNS proxy global configuration, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **DNS Proxy Global Configuration** in the DNS Proxy section.
3. In the <DNS Proxy Global Configuration> page, configure the following settings.

Option	Description
TTL	Enable and specifies the TTL for DNS-proxy’ s response packets. If the DNS-proxy requests are not responded after the TTL, the DNS client will clear all DNS records. The value range is 30 to 600 seconds. The default value is 60.
Server Track	Enable the DNS proxy server track and configure the time interval of tracking for DNS proxy server. System will periodically detect the DNS proxy server at a specific time interval. When the server cannot be tracked, the IP address of server will be removed from the DNS resolution list untill the link is restored. By default, the track-

Option	Description
	ing for DNS proxy server is enabled.
UDP Checksum	Click the checkbox to enable/disable calculating the checksum of UDP packet for DNS proxy. The system will calculate the checksum of UDP packet for DNS proxy when the DNS proxy on interfaces is enabled. If you need to improve the performance of the device, you can disable this function.

4. Click **OK**.

Configuring an Analysis

Analysis configuration includes DNS requests' retry times and timeout.

- Retry: If there is no response from the DNS server after the timeout, system will send the request again; if there is still no response from the DNS server after the specified retry times (i.e. the number of times to repeat the DNS request), system will send the request to the next DNS server.
- Timeout: System will wait for the DNS server's response after sending the DNS request and will send the request again if no response returns after a specified time. The period of waiting for a response is known as timeout.

To configure the retry times and timeout for DNS requests, take the following steps:

1. Select **Network > DNS > Analysis**
2. Select the retry times radio button.

3. Select the timeout values radio button.

4. Click **Apply**.

Configuring a DNS Cache

When using DNS, system might store the DNS mappings to its cache to speed up the query. There are three ways to obtain DNS mappings:

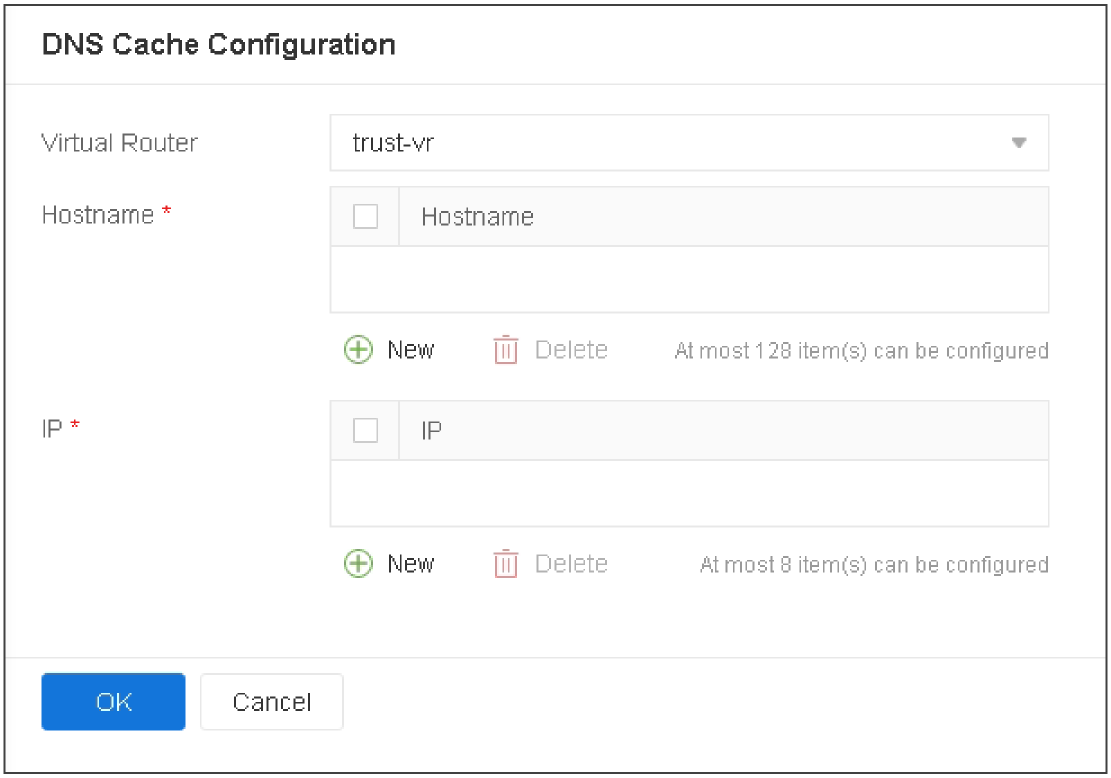
- Dynamic: Obtains from DNS response.
- Static: Adds DNS mappings to cache manually.
- Register: DNS hosts specified by some modules of security devices, such as NTP, AAA, etc.

For convenient management , DNS static cache supports group function, which means users make the multiple domain hosts with the same IP address and virtual router is a DNS static cache group.

To add a static DNS mapping to cache, take the following steps:

1. Select **Network** > **DNS** > **Cache**

2. Click **New**.



DNS Cache Configuration

Virtual Router: trust-vr

Hostname *: □ Hostname

⊕ New 🗑 Delete At most 128 item(s) can be configured

IP *: □ IP

⊕ New 🗑 Delete At most 8 item(s) can be configured

OK Cancel

Option	Description
Hostname	Specify the hostname of a DNS cache group. You can click ⊕ to add or click 🗑 button to delete the specified hostname. The maximum number of domain hosts is 128, and the maximum length of each hostname is 255 characters.
IP	Specify the host IPv4 address of a DNS cache group. You can click ⊕ to add or click 🗑 button to delete the specified IP. The maximum number of host IP address is 8, and the earlier configured IP will be matched first.

Option	Description
Virtual Router	Select a VRouter.

3. Click **OK**.

Notes:

- Only DNS static cache group can support new, edit and delete operation , while dynamic and register cache cannot .
- The DNS dynamic cache can be deleted by command or the lifetime reset. For detailed information , refer to **StoneOS CLI User Guide** and download PDF on website.
- User can clear the register cache only by deleting the defined hosts in function module.
- DNS static cache is superior to dynamic and register cache, which means the static cache will cover the same existed dynamic or register cache.

NBT Cache

System supports NetBIOS name resolution. With this function enabled, system can automatically obtain all the NetBIOS host names registered by the hosts within the managed network, and store them in the cache to provide IP address to NetBIOS host name query service for other modules.

Enabling a NetBIOS name resolver is the pre-requisition for displaying host names in NAT logs. For more information on how to display host names in the NAT logs, see "Log Configuration" on Page 1115.

To enable NetBIOS for a zone, select the NBT cache check box when creating or editing the zone. For more details, see "Security Zone" on Page 74. The security zone with NetBIOS enabled should not be the zone that is connected to WAN. After NetBIOS is enabled, the query process might last for a while, and the query result will be added to the NetBIOS cache table. System will perform the query again periodically and update the result.

Notes: Only when PCs have NetBIOS enabled can their host names be queried. For more information on how to enable NetBIOS, see the detailed instructions of your PC's Operating System.

To clear NBT cache, take the following steps:

1. Select **Network > DNS > NBT Cache**.

2. Select a VRouter from the VR drop-down list to display the NBT cache in that VRouter.

3. Select a NBT cache entry from the list and click **Delete**.

DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for subnetworks automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

DHCP supports to allocate IPv4 and IPv6 addresses.

System supports DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: The interface can be configured as a DHCP client and obtain IP addresses from the DHCP server. For more information on configuring a DHCP client, see "Creating a PPPoE Interface" on Page 81.
- DHCP server: The interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: The interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

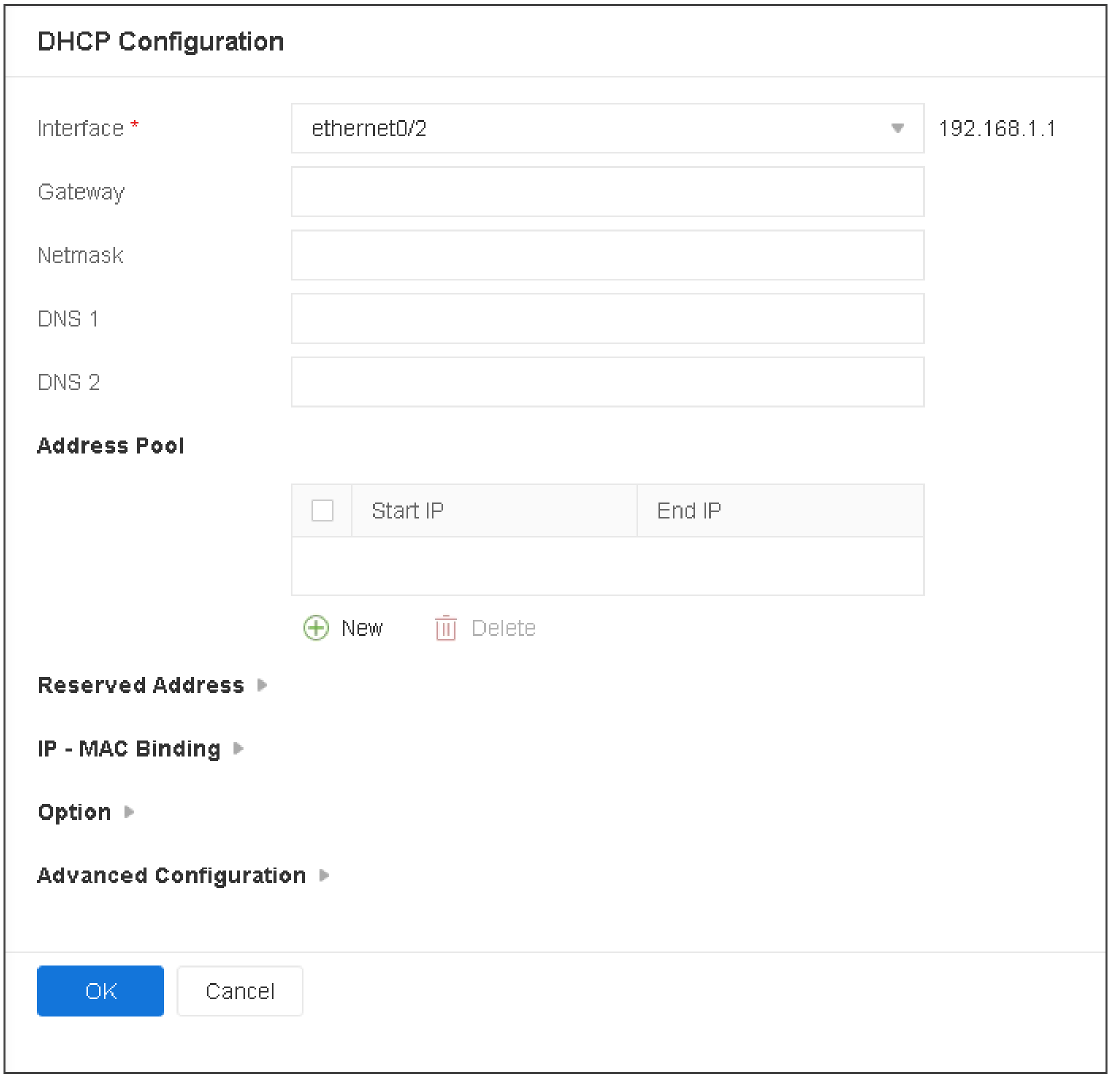
The security devices are designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Server

To create a DHCP server, take the following steps:

1. Select **Network** > **DHCP**.

2. Select **New** > **DHCP Server**.



DHCP Configuration

Interface * ethernet0/2 192.168.1.1

3. In the DHCP Configuration page, configure as following:

Option	Description
Interface	Configures a interface which enables the DHCP server.
Gateway	Configures a gateway IP for the client.

Option	Description
Netmask	Configures a netmask for the client.
DNS1	Configures a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configures an alternative DNS server for the client. Type the server's IP address into the box.
Address pool	Configures an IP range in the address pool. The IPs within this range will be allocated. Take the following steps: 1. Type the start IP and end IP into the Start IP and End IP box respectively. 2. Click **New** to add an IP range which will be displayed in the list below. 3. Repeat the above steps to add more IP ranges. To delete an IP range, select the IP range you want to delete from the list and click **Delete**.

4. Configure Reserved Address (IP addresses in the Reserved Address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated).
   To configure a reserved address, expand **Reserved Address**, type the start and end IP for an IP range into the Start IP and End IP box respectively, and then click **New**. To delete an IP range, select the IP range you want to delete from the list and then click **Delete**.

5. Configure IP-MAC Binding. If the IP is bound to a MAC address manually, the IP will only be allocated to the specified MAC address.
   To configure an IP-MAC Binding, expand **IP-MAC Binding** and type the IP and MAC

address into the IP address and MAC box respectively, type the description in the Description text box if necessary, and then click **New**. Repeat the above steps to add multiple entries. To delete an IP-MAC Binding, select an entry from the list and click **Delete**.

6. **Expand Option, configure the options supported by DHCP server.**

Option	Description
43	Option 43 is used to exchange specific vendor specific information (VSI) between DHCP client and DHCP server. The DHCP server uses option 43 to assign Access Controller (AC) addresses to wireless Access Point (AP), and the wireless AP use DHCP to discover the AC to which it is to connect. 1. Click **New**. 2. Select **43** from the **Option** drop-down list. 3. Select the type of the VSI, ASCII or HEX. When selecting ASCII, the VSI matching string must be enclosed in quotes if it contains spaces. 4. Enter the VSI in the **Sign** text box. **Notes:** If the VCI matching string has been configured, first of all, you need to verify the VCI carried by the option 60 field in client’ s DHCP packets. When the VCI matches the configured one, the IP address, option 43 and corresponding information will be offered. If not, DHCP server will drop client’ s DHCP

Option	Description
	💡 packets and will not reply to the client.
49	After you configure the option 49 settings, the DHCP client can obtain the list of the IP addresses of systems that are running the X window System Display Manager. To configure the option 49 settings: 1. Click **New**. 2. Select **49** from the **Option** drop-down list. 3. Enter the IP address of the system that is running the X window System Display Manager into the **IP address** box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
60	After configuring the VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI. 1. Click **New**. 2. Select **60** from the **Option** drop-down list. 3. Select the type of the VCI, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces.

Option	Description
	4. Enter the VCI in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
66	The option 66 is used to configure the TFTP server name option. By configuring Option 66, the DHCP client get the domain name or the IP address of the TFTP server. You can download the startup file specified in the Option 67 from the TFTP server. 1. Click **New**. 2. Select **66** from the **Option** drop-down list. 3. Select the type of the TFTP server name, ASCII or HEX. When selecting ASCII, the length of TFTP server is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters. 4. Enter the domain name or the IP address of the TFTP server in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
67	The option 67 is used to configure the startup file name

Option	Description
	option for the TFTP server. By configuring option 67, the DHCP client can get the name of the startup file. 1. Click **New**. 2. Select **67** from the **Option** drop-down list. 3. Select the type of the startup file name, ASCII or HEX. When selecting ASCII, the length of startup file name is 1 to 255 characters. 4. Enter the startup file name in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
138	The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list. 1. Click **New**. 2. Select **138** from the **Option** drop-down list. 3. Enter the AC IP address in the **IP address** text box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and

Option	Description
	click **Delete**. You can add up to four AC IP addresses. If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will not offer the option 138 settings.
150	The option 150 is used to configure the address options for the TFTP server. By configuring option 150, the DHCP client can get the address of the TFTP server. 1. Click **New**. 2. Select **150** from the **Option** drop-down list. 3. Enter the TFTP server IP address in the **IP address** text box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
242	The option 242 is a private DHCP private option for IP phones. By configuring option 242, the specific parameters information of IP phone can be exchanged between DHCP server and DHCP client, such as call server address (MCIPADD), call the server port (MCPORT), the address of the TLS server (TLSSRVR), HTTP (HTTPSRVR) HTTP server address and server port (HTTPPORT) etc.

Option	Description
	1. Click **New**. 2. Select **242** from the **Option** drop-down list. 3. Select the type of the specific parameters of the IP phone, ASCII or HEX. When selecting ASCII, the length of startup file name is 1 to 255 characters. 4. Enter the specific parameters of the IP phone in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.

7. Expand Advanced Configuration to configure the DHCP server's advanced options.

Option	Description
Domain	The domain name configured by the DHCP client.
Lease	Specifies a lease time. The value range is 300 to 1048575 seconds. The default value is 3600. Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is assigned. After the lease expires, the client will have to request an IP address again from the DHCP server.
Auto Configure	Enables automatic configuration. Select an interface with DHCP client enabled on the same gateway from the drop-

Option	Description
	down list. "----"indicates auto configure is not enabled. Auto configure will activate function in the following condition: Another interface with DHCP configured on the device enables DHCP client. When auto configure is enabled, if the DHCP server (Hillstone device) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will dispatch the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server (Hillstone device). However, the DNS, WINS and domain name that are configured manually still have the priority.
WINS1	Configures a primary WINS server for the client. Type the server's IP address into the box.
WINS2	Configures an alternative WINS server for the client. Type the server's IP address into the box.
Server	
SMTP server	Configures a SMTP server for the client. Type the server's IP address into the box.
POP3 server	Configures a POP3 server for the client. Type the server's IP address into the box.
News server	Configures a news server for the client. Type the server's IP address into the box.

Option	Description
Relay agent	When the device1 with DHCP server enabled is connected to another device2 with DHCP relay enabled, and the PC obtains device1's DHCP information from device2, then only when the relay agent's IP address and netmask are configured on device1 can the DHCP information be transmitted to the PC successfully. Relay agent: Type relay agent's IP address and netmask, i.e., the IP address and netmask for the interface with relay agent enabled on device2.
VCI-match-string	The DHCP server can verify the VCI carried by option 60 in the client’ s DHCP packets.When the VCI in the client's DHCP packet matches the VCI matching string you configured in the DHCP server, the DHCP server will offer the IP address and other corresponding information. If not, the DHCP server will drop the client's DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60. 1. Select the type of the VCI matching string, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 2. Enter the VCI matching string in the text box.

8. Click **OK**.

Configuring a DHCP Relay Proxy

The device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client.

To create a DHCP relay proxy, take the following steps:

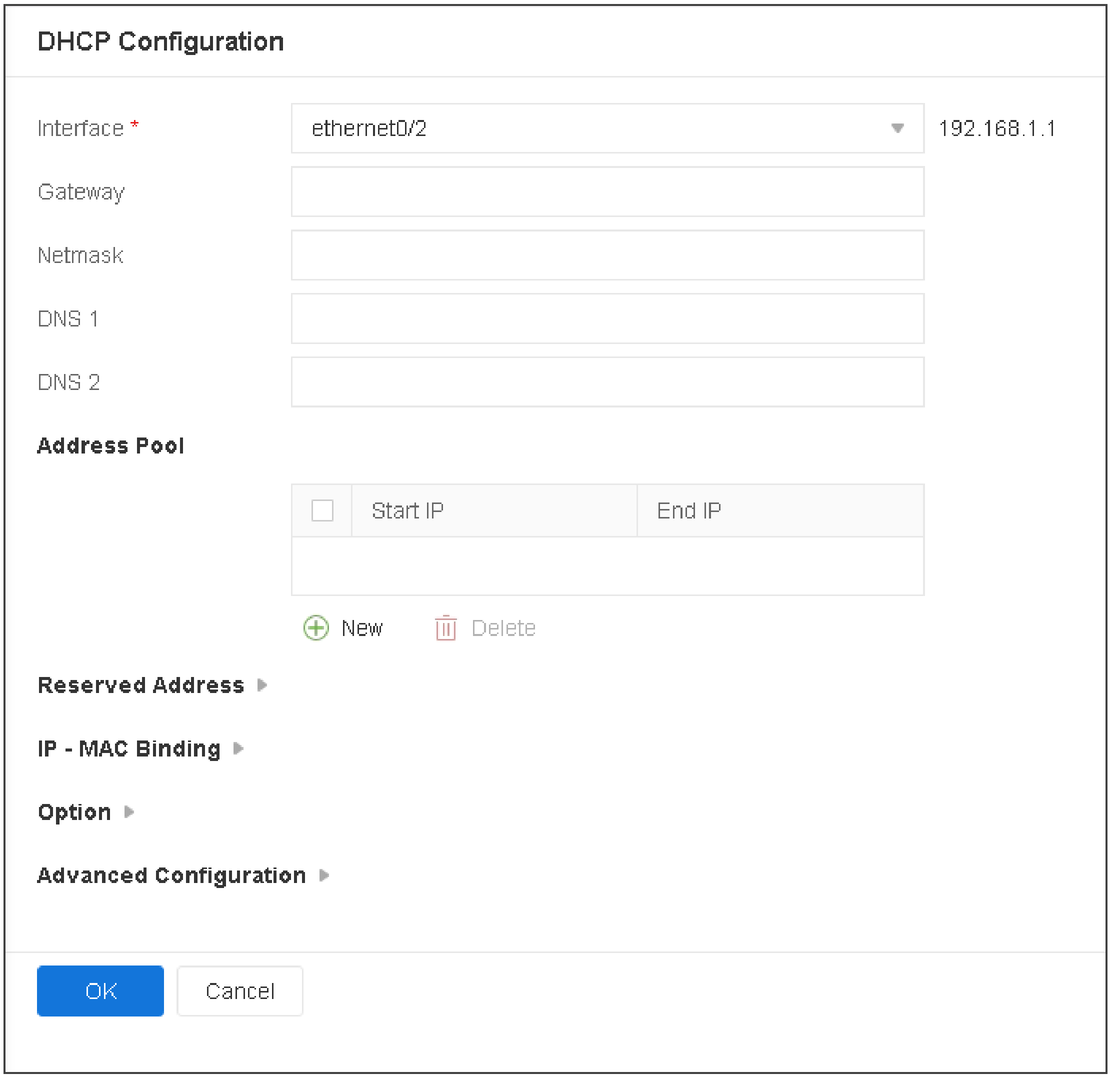
1. Select **Network > DHCP**.
2. Click **New > DHCP Relay Proxy**.
3. In the DHCP Relay Proxy page, select an interface to which the DHCP Relay Proxy will be applied from the Interface drop-down list.
4. Type the IP addresses of DHCP servers into the Server 1/Server 2/Server 3 boxes.
5. Click **OK**.

Configuring a DHCPv6 Server

To create a DHCPv6 server to appropriate IPv6 addresses, take the following steps:

1. Select **Network** > **DHCP**.

2. Select **New** > **DHCPv6 Server**.



Interface * ethernet0/2 192.168.1.1

3. In the DHCPv6 Configuration page, configure as following:

Option	Description
Interface	Configures a interface which enables the DHCPv6 server to appropriate IPv6 addresses.
rapid-commit	Clicking this button can help fast get IPv6 address from

Option	Description
	the server. You need to enable both of the DHCP client and server's Rapid-commit function.
Preference	Specifies the priority of the DHCPv6 server. The range should be from 0 to 255. The bigger the value is, the higher the priority is.
DNS1	Configures a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configures an alternative DNS server for the client. Type the server's IP address into the box.
Domain	Configures the domain name for the DHCP client.
Address Pool: System can act as a DHCPv6 server to allocate IPv6 addresses for the DHCP clients in the subnets.	
IP	Specifies the IPv6 address prefix and prefix length.
Valid Lifetime	Specifies the lifetime of the address.
Preferred Lifetime	Specifies the preferred lifetime for the IPv6 address. The preferred lifetime should not be larger than the valid lifetime.

4. Click **OK**.

Configuring a DHCPv6 Relay Proxy

The device can act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server, and then obtain DHCP information from the server and return it to the client.

To create a DHCPv6 relay proxy, take the following steps:

1. Select **Network > DHCP**.
2. Click **New > DHCPv6 Relay Proxy**.
3. In the DHCP Relay Proxy page, select an interface to which the DHCPv6 Relay Proxy will be applied from the Interface drop-down list.
4. Type the IPv6 addresses of DHCPv6 servers into the Server 1/Server 2/Server 3 boxes.
5. If the DHCPv6 server is specified as link-local address, you need to select the egress interface name from Egress Interface 1/Egress Interface 2/Egress Interface 3 dropdown list.
6. Click **OK**.

DDNS

DDNS (Dynamic Domain Name Server) is designed to resolve fixed domain names to dynamic IP addresses. Generally you will be allocated with a dynamic IP address from ISP each time you connect to the Internet, i.e., the allocated IP addresses for different Internet connections will vary. DDNS can bind the domain name to your dynamic IP address, and the binding between them will be updated automatically each time you connect to the Internet.

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. Hillstone devices support the following 5 DDNS providers, and you can visit one of the following websites to complete the registration:

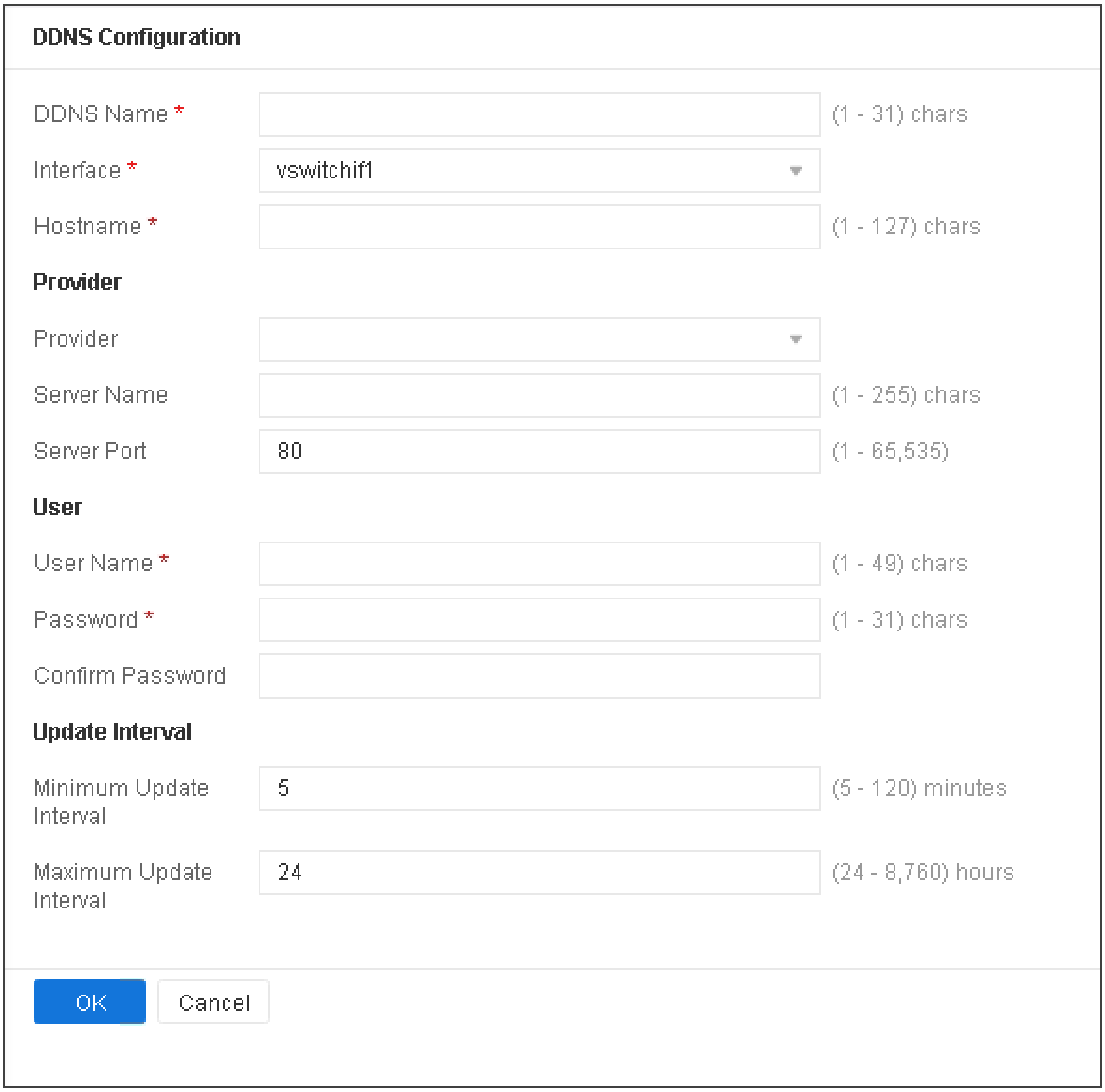
- dyndns.org: http://dyndns.com/dns
- 3322.org: http://www.pubyun.com
- no-ip.com: http://www.noip.com
- Huagai.net: http://www.ddns.com.cn
- ZoneEdit.com: http://www.zoneedit.com

Configuring a DDNS

To create a DDNS, take the following steps:

1. Select **Network > DDNS**.

2. Click **New**.



DDNS Configuration

DDNS Name *		(1 - 31) chars
Interface *	vswitchif1	
Hostname *		(1 - 127) chars
Provider		
Provider		
Server Name		(1 - 255) chars
Server Port	80	(1 - 65,535)
User		
User Name *		(1 - 49) chars
Password *		(1 - 31) chars
Confirm Password		
Update Interval		
Minimum Update Interval	5	(5 - 120) minutes
Maximum Update Interval	24	(24 - 8,760) hours

3. In the DDNS Configuration page, configure as follows:

Option	Description
DDNS Name	Specifies the name of DDNS.
Interface	Specifies the interface to which DDNS is applied.

Option	Description
Hostname	Specifies the domain name obtained from the DDNS provider.
Provider	
Provider	Specifies a DDNS provider. Choose one from the drop-down list.
Server Name	Specifies a server name for the configured DDNS.
Server Port	Specifies a server port number for the configured DDNS. The value range is 1 to 65535.
User	
User Name	Specifies the user name registered in the DDNS provider.
Password	Specifies the corresponding password.
Confirm Password	Enter the password again to confirm.
Update Interval	
Minimum Update Interval	When the IP address of the interface with DDNS enabled changes, system will send an update request to the DDNS server. If the server does not respond to the request, system will send the request again according to the configured min update interval. For example, if the minimum update interval is set to 5 minutes, then system will send the second request 5 minutes after the first request failure; if it fails again, system will send the third

Option	Description
	request 10 (5x2) minutes later; if it fails again, and system will send the forth request 20 (10*2) minutes later, and so forth. The value will not increase anymore when reaching 120 minutes. That is, system will send the request at a fixed interval of 120 minutes. The default value is 5.
Maximum Update Interval	In case the IP address has not changed, system will send an update request to the DDNS server at the maximum update interval. Type the maximum update interval into the box. The value range is 24 to 8760 hours. The default value is 24.

4. Click **OK**.

Notes: The Server name and Server port in the configuration options must be the corresponding name and port of the DDNS server. Do not configure these options if the exact information is unknown. The server will return the name and port information automatically after connection to the DDNS server has been established successfully.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, combines PPP protocol and Ethernet to implement access control, authentication, and accounting on clients during an IP address allocation.

The implementation of PPPoE protocol consists of two stages: discovery stage and PPP session stage.

- Discovery stage: The client discovers the access concentrator by identifying the Ethernet MAC address of the access concentrator and establishing a PPPoE session ID.
- PPP session stage: The client and the access concentrator negotiate over PPP. The negotiation procedure is the same with that of a standard PPP negotiation.

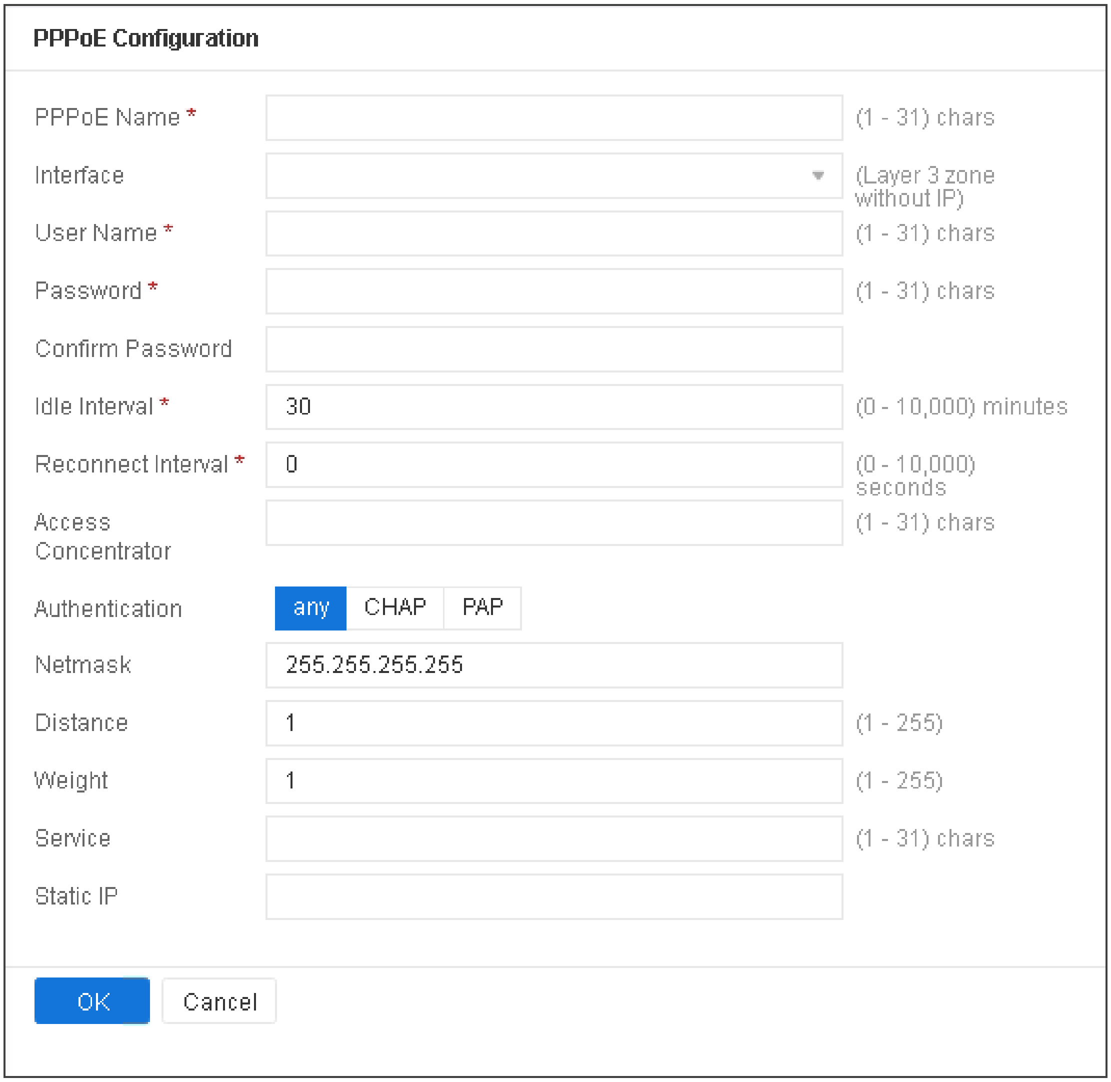
Interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

To create a PPPoE instance, take the following steps:

1. Select **Network > PPPoE**.

2. Click **New**.



PPPoE Configuration

PPPoE Name *		(1 - 31) chars
Interface	▾	(Layer 3 zone without IP)
User Name *		(1 - 31) chars
Password *		(1 - 31) chars
Confirm Password		
Idle Interval *	30	(0 - 10,000) minutes
Reconnect Interval *	0	(0 - 10,000) seconds
Access Concentrator		(1 - 31) chars
Authentication	[✓ any] CHAP PAP	
Netmask	255.255.255.255	
Distance	1	(1 - 255)
Weight	1	(1 - 255)
Service		(1 - 31) chars
Static IP		

3. **In the PPPoE Configuration page, configure as follows.**

Option	Description
PPPoE Name	Specifies a name for the PPPoE instance.
Interface	Select an interface from the drop-down list.

Option	Description
User Name	Specifies a username.
Password	Specifies the corresponding password.
Conform Password	Enter the password again to confirm.
Idle Interval	Automatic connection. 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.
Reconnect Interval	If the PPPoE connection disconnects for any reason for a certain period, i.e. the specified re-connect interval, system will try to re-connect automatically. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
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). To configure a PPPoE authentication method, click the authentication you want to select. The configured

Option	Description
	authentication must be the same with that configured in the PPPoE server.
Netmask	Specifies a netmask for the IP address obtained via PPPoE.
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.
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 Static IP box.

4. Click **OK**.

Virtual Wire

The system supports the VSwitch-based Virtual Wire. With this function enabled and the Virtual Wire interface pair configured, the two Virtual Wire interfaces form a virtual wire that connects the two subnetworks attached to the Virtual Wire interface pair together. The two connected subnetworks can communicate directly on Layer 2, without any requirement on MAC address learning or other sub network's forwarding. Furthermore, controls of policy rules or other functions are still available when Virtual Wire is used.

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

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

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

Packet	Strict	Non-strict
Egress and ingress are interfaces of one Virtual Wire interface pair	Allow	Allow
Ingress is not Virtual Wire's interface	Deny	Deny
Egress and ingress are interfaces of different Virtual Wire interface pairs	Deny	Deny

Packet	Strict	Non-strict
Ingress of to-self packet is a Virtual Wire’ s interface	Deny	Allow
Ingress is Virtual Wire's interface, and egress is a Layer 3 interface	Deny	Allow

Configuring a Virtual-Wire

To create a Virtual-Wire, take the following steps:

1. Select **Network > Virtual-Wire**.
2. Click **New**.
3. In the Virtual-Wire Configuration page, select a virtual switch from the VSwitch drop-down list.
4. In the Interface 1 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
5. In the Interface 2 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
6. Click **OK**.

Configuring the Virtual Wire Mode

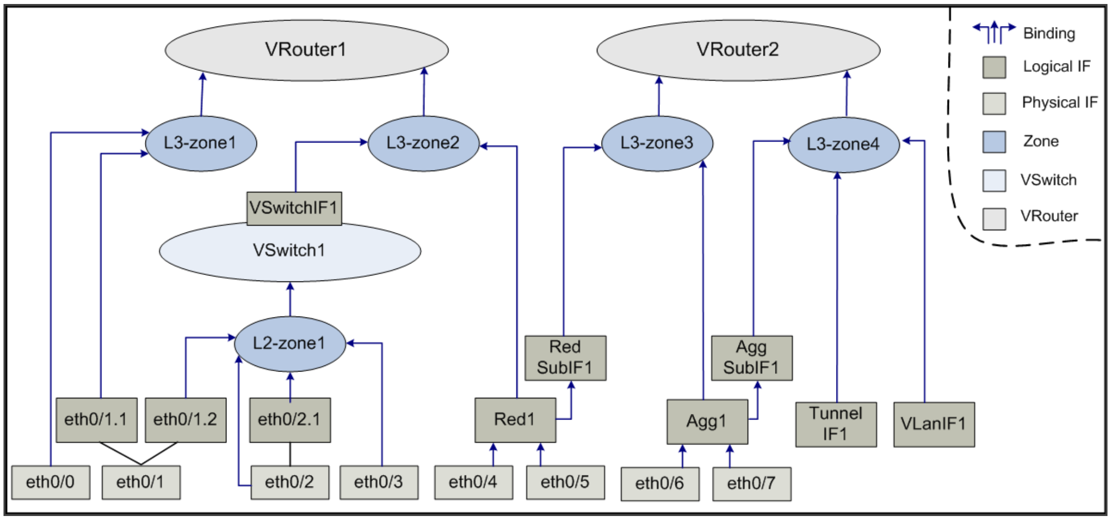
To configure a virtual wire mode, take the following steps:

1. Select **Network > Virtual-Wire**.
2. Click **Virtual-Wire Mode**.

3. In the Virtual-Wire Mode Configuration page, select a virtual switch from the VSwitch drop-down list.
4. Specify a virtual wire mode from one of the following options:
   - Strict - Packets can only be transmitted between virtual wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to the virtual wire can neither manage devices nor access Internet over this interface.
   - Non-strict - Packets can be transmitted between virtual wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between virtual wire interfaces, and does not affect Layer 3 packets' forwarding.
   - Disabled - Disables the virtual wire.
5. Click **OK**.

Virtual Router

Virtual Router (VRouter) is known as VR in system. VR acts as a router, and different VRs have their own independent routing tables. A VR named "trust-vr" is implemented with the system, and by default, all of the Layer 3 security zones are bounded to the trust-vr automatically. Hillstone devices support multiple VRs, and the max amount of supported VRs may vary with different hardware platforms. Multiple VRs divide a device into multiple virtual routers, and each router utilizes and maintains their independent routing table. In such a case one device is acting as multiple routers. Multiple VRs allow a device to achieve the effects of the address isolation between different route zones and address overlapping between different VRs, as well as to avoid route leaking to some extent, enhancing route security of network. For more information about the relationship between interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationship between them are:

- Interfaces are bound to security zones. Those that are bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; the primary interface and sub interface can belong to different security zones.

- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the pre-defined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the pre-defined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwtich or VR.

Creating a Virtual Router

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. Click **OK**.

Global Configuration

Virtual Router's global configuration is the configuration for multiple Virtual Routers. To configure Multi-Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Global Configuration**.
2. Click the **Enable** button for Multi-Virtual Router.
3. Click **Apply**.

Notes:

- After Multi-Virtual Router is enabled or disabled, system must reboot to make it take effect. After rebooting, system's max concurrent sessions will decrease by 15% if the function is enabled, or restore to normal if the function is disabled. When AV and Multi-Virtual Router are enabled simultaneously, the max concurrent session will further decrease by 50% (with AV enabled, the max concurrent session will decrease by half). The formula is: Actual max concurrent sessions = original max concurrent sessions*(1-0.15)*(1-0.5).
- 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.

Virtual Switch

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

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

Creating a VSwitch

To create a VSwitch, take the following steps:

1. Select **Network > VSwitch**.
2. Click **New**.

Options are described as follows.

Option	Description
VSwitch Name	Specifies a name for the VSwitch.
Vsys Shared	Click the **Enable** button and then system will share the VSwitch with different VSYS.
Virtual-Wire	Specifies a Virtual-Wire mode for the VSwitch, including

Option	Description
Mode	(for specific information on Virtual Wire, see "Virtual Wire" on Page 200) - Strict - Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to Virtual Wire can neither manage devices nor access Internet over this interface. - Non-strict - Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding. - Disabled - Disables Virtual Wire.
IGMP Snooping	Enables IGMP snooping on the VSwitch.
Forward Tagged Packets	Enables VLAN transparent so that the device can transmit VLAN tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.
Forward Double Tagged Pack-	Enables VLAN transparent so that the device can transmit VLAN double tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID

Option	Description
ets	after passing through the device.
Drop Unknown Multicast Packets	Drops the packets sent to unknown multicast to save bandwidth.

3. Click **OK**.

Port Mirroring

Some low-end platforms do not support port mirroring.

The device is designed with port mirroring on Ethernet interfaces. This function allows users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.

To configure port mirroring, take the following steps:

1. Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
2. Configure a destination interface.

To configure the destination interface of port mirroring:

1. Select **Network > Port Mirroring**.
2. Select an interfaces from the Destination Interface drop-down list, and click **OK**. All the source and destination interface will be listed in the table below.

WLAN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

WLAN (Wireless Local Area Network) represents the local area network that uses the wireless channel as the medial. WLAN is important supplements and extensions of the wired LAN. By configuring the WLAN function, you can establish the wireless local area network and allow the users to access LAN through wireless mode.

Creating a WLAN

To create a WLAN, take the following steps:

1. Select **Network > WLAN**.

2. Click **New**.

   In the WLAN Configuration page, configure the following information.

Option	Description
SSID	Specifies the name of the WLAN.
WLAN Interface	Specifies the WLAN interface bound to this newly-created WLAN.
SSID Broadcast	Click the **Enable** button to enable the SSID broadcast. After enabling SSID broadcast, any user can search it.
Security Mode	Configures the security mode: • No encryption - Do not perform the encryption. • MAC-PSK - Integrates MAC authentication

Option	Description
	with WPA-WPA2-PSK authentication. • WEP - Specifies the security mode as wired equivalent privacy. • WPA、WPA2 - Specifies the security mode as Wi-FI and uses 802.1X authentication. WPA and WPA2 have stronger performance than WEP. The safety of WPA2 is more reliable than WPA. • WPA-WPA2 - Compatible with WPA and WPA-2. • WPA-PSK、WPA2-PSK - Specifies the security mode as Wi-FI and uses the pre-shared key authentication. • WPA-WPA2-PSK - Compatible with WPA-PSK and WPA2-PSK.
Link-lay-erAuthentication Mode	When using the WEP security mode, specify the authentication mode for the WLAN. • open-system - The default authentication mode. This is the easiest authentication, ie. do not need to certify. • shared-key - Certify with the same shared key authentication.

Option	Description
Data Encryption	When using a security mode besides WEP, specifies the data encryption mode, including TKIP, CCMP, and TKIP-CCMP.
Key	When using the WEP security mode, specify the form and the value of the key. The form of the key can be a character string or a hexadecimal number. When using character strings, you can specify 5 characters or 13 characters. When using hexadecimal numbers, you can specify 10 hexadecimal numbers or 26 hexadecimal numbers.
Pre-shared Key	When using the MAC-PSK, WPA-PSK, WPA2-PSK, WPA-WPA2-PSK security modes, specify the form and the value of the pre-defined key. The form of the key can be a character string or a hexadecimal number. When using character strings, you can specify 8-63 characters. When using hexadecimal numbers, you can specify 64 hexadecimal numbers.
Maximum Users	Specifies the allowed maximum number of users that can access this WLAN. The value ranges from 1 to 128. The default value is 64.
User Isolation	Select **Enable** to enable the user isolation function. After enabling the user isolation, users within one WLAN cannot access each other. User isolation enhances the security for different users.

Option	Description
AAA Server	When specifying the security mode as WPA, WPA2, WPA-WPA2, or MAC-PSK, you must select a configured AAA server as the authentication server for user identification.

3. Click **OK**.

Advanced Settings

To configure the advanced settings for WLAN, take the following steps:

1. Select **Network > WLAN**.
2. Click **Advanced**.

3. In the Advanced page, configure the following information.

Option	Description
Countries & Regions	Different countries or regions have different management and limitations on RF use. The country/region code determines the available frequency range, channel, and legal level of transmit power. The default value is United States.
Working Mode	Configure the working mode. • 802.11a represents that the interface works in the 802.11a mode. • 802.11b represents that the interface works in the 802.11b mode. • 802.11g represents that the interface works in the 802.11g mode. • 802.11an represents that the interface works in the 802.11n mode of 5GHz. • 802.11bgn represents that the interface works in the 802.11n mode of 2.4GHz.
Channel	The available channels you can select vary with the country/region code and RF type. The default value is auto, which represents to ask the system to select the channel automatically. After the country/region code or the operation mode is changed, system will

Option	Description
	select the channel automatically.
Maximum Transmit Power	The maximum transmit power varies with the country/region code and RF type. By default, there are four levels: 12.5% of the maximum transmit power, 25% of the maximum transmit power, 50% of the maximum transmit power, and 100% of the maximum transmit power.

4. Click **OK**.

3G/4G

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

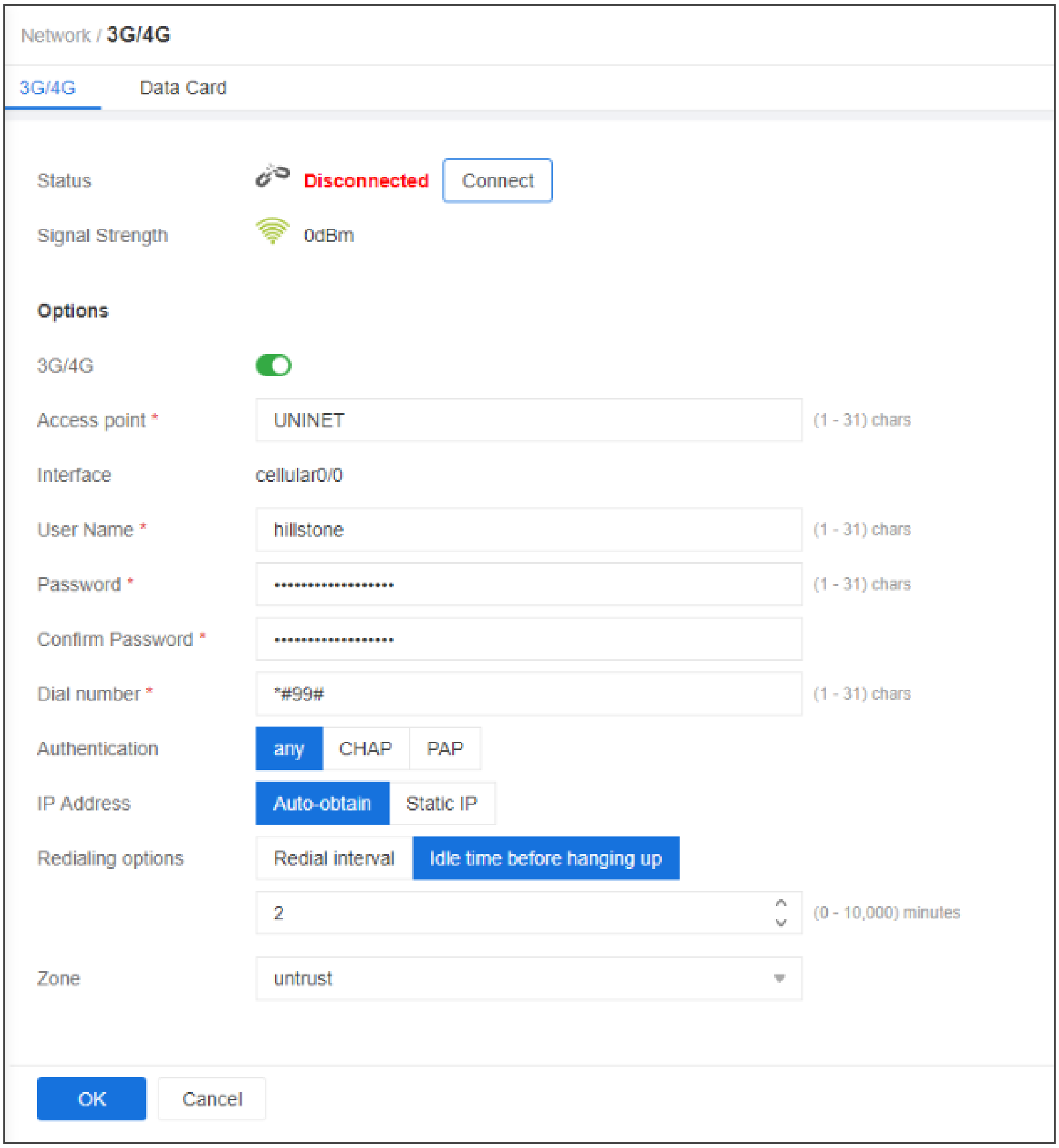
The third generation of mobile telecommunications technology supports the high speed data transmission. There are three standards of 3G/4G: CDMA2000, WCDMA, and TD-SCDMA. By configuring the 3G/4G function, users can access the Internet through wireless mode.

The 3G/4G function needs the support of ISP. Before configuring the 3G/4G function, you need to purchase the SIM card from the ISP, enable the data connection service, and obtain the following 3G/4G parameters: access point, username, password, dial-up string, and correctly installed SIM card.

Configuring 3G/4G Settings

To configure 3G/4G settings, take the following steps:

1. Select **Network > 3G/4G**.



Network / **3G/4G**

3G/4G | Data Card

Status	Disconnected Connect	
Signal Strength	0dBm	

Options

3G/4G	●	
Access point *	UNINET	(1 - 31) chars
Interface	cellular0/0	
User Name *	hillstone	(1 - 31) chars
Password *	••••••••••••••••••	(1 - 31) chars
Confirm Password *	••••••••••••••••••	
Dial number *	*#99#	(1 - 31) chars
Authentication	[✓ any] CHAP PAP	
IP Address	[✓ Auto-obtain] Static IP	
Redialing options	Redial interval [✓ Idle time before hanging up]	
	2	(0 - 10,000) minutes
Zone	untrust	

OK Cancel

2. In the 3G/4G tab, you can view the 3G/4G connection status in the Status section. Click **Connect** to connect to the 3G network.

3. Select **Enable** to enable the 3G/4G function. By default, the 3G function is enabled.

4. Enter the name of the access point in the Access point text box. You can enter up to 31 characters.

5. Specify the 3G/4G user information. In the User Name text box, enter the username of the 3G/4G user. You can enter up to 31 characters. In the Password text box, enter the corresponding password.

6. Configure the dial-up string. Ask your ISP to provide the dial-up string and enter the dial-up string in the Dial number text box.

7. Specify the authentication mode. When 3G/4G dial-up establishes the connection, it needs to pass the PPP protocol verification. The device supports the following verification methods: CHAP, PAP, and Any. Select the desired method by selecting the Authentication radio button.

8. Configure the IP address information for the 3G/4G interface. Select **Auto-obtain** to make the 3G/4G interface obtain the IP address automatically. Select **Static IP** to enter the static IP address and the netmask.

9. Specify the online mode in Redialing options. 3G/4G dial-up has two online modes as follows:

   - Redial interval: When the 3G/4G connection disconnects due to certain reasons and the disconnection time exceeds the specified time interval, system will redial automatically. Specify the time interval in the Redial interval text box. The value ranges from 0 to 10000 seconds. The default value is 0, which represents that the system does not use the **redial automatically** mode.

   - Idle time before hanging up: When the idle time of the 3G/4G (cellular) interface reaches the specified value, system will disconnect the 3G/4G connection. Specify the length of time in the Idle time before hanging up text box. The value ranges from

0 to 10000 seconds. The default value is 0, which represents that the system does not use the **hang up after a specified idle time** mode

> **Notes:** The above two modes cannot be used simultaneously. Without configuring the schedule, system will use the "Redial interval" mode by default.

10. Specify the security zone of the 3G/4G interface.

11. Click **OK**.

> **Notes:** After installing the SIM card, system can automatically configure the settings in the 3G/4G tab based on the information of the 3G/4G module. The settings include the name of the access point, 3G/4G user information, and dial-up string. You can modify the settings according to your requirements.

Managing Data Card

PIN (Personal Identification Number) code is used to identify the user of the SIM card and avoid the illegal use of the SIM card.

Automatically Verifying the PIN Code

After enabling the PIN code protection, you can save the PIN code in system. After system reboots, it can automatically verify the PIN code.

To automatically verify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.

2. Click **Data Card** tab.

3. Enter the PIN code in the PIN Code text box. The value ranges from 4 to 8 numbers.

4. Click **Apply** to make the system save the PIN code.

Notes: After three consecutive failed attempts at PIN code, the SIM card will be locked.

Enabling/Disabling the PIN Code Protection

To enable/disable the PIN code protection, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click Enable PIN code protection in the PIN code management section to enable the PIN code protection function. To disable the function, click Disable PIN code protection.
4. Enter the PIN code in the PIN code text box. The PIN code consists of 4-8 decimal numbers.
5. Click **Apply**.

Modifying the PIN Code

To modify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click Change PIN code in the PIN code management section.
4. Specify the current PIN code in the Current PIN code text box. The PIN code consists of 4-8 decimal numbers.
5. Specify a new PIN code in the New PIN code text box. The PIN code consists of 4-8 decimal numbers.

6. Confirm the new PIN code in the Confirm PIN code text box.

7. Click **Apply**.

Manually Verifying the PIN Code

To manually verify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.

2. Click **Data Card** tab.

3. Click Verify PIN Code in the PIN code management section.

4. Enter the PIN code in the PIN code text box. The PIN code consists of 4-8 decimal numbers.

5. Click **Apply**.

Unlocking the PIN Code

If the SIM card is locked, you need to obtain the PUK code from the ISP to unlock the SIM card and set the new PIN code. To use the PUK code to unlock the PIN code, take the following steps:

1. Select **Network > 3G/4G**.

2. Click **Data Card** tab.

3. Click **Unlock PIN Code** in the PIN code management section.

4. Enter the PUK code in the PUK code text box.

5. Specify a new PIN code in the New PIN code text box. The PIN code consists of 4-8 decimal numbers.

6. Confirm the new PIN code in the Confirm PIN code text box.

7. Click **Apply**.

Outbound Link Load Balancing

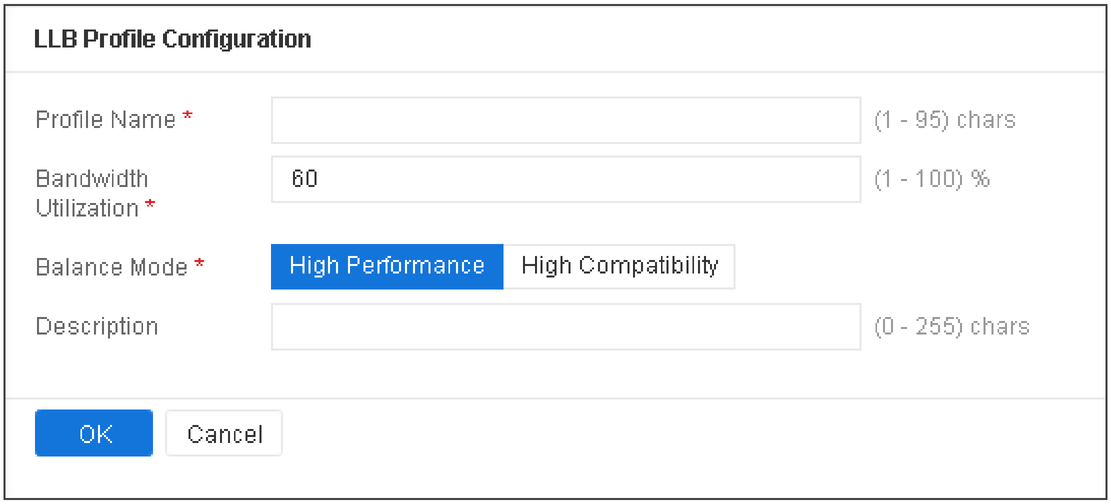
For Outbound LLB, the system can intelligently oute and dynamically adjust the traffic load of each link by monitoring the delay, jitter, packet loss rate and bandwidth utilization of each link in real-time.You can configure a flexible LLB profile to bind to the route (the current system only supports DBR and PBR), forming LLB rules to implement outbound dynamic link load balancing, and thus make efficient use of network bandwidth.

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.

1. Select **Network > Outbound > Profile**.

2. Click **New**.



LLB Profile Configuration

Profile Name * (1 - 95) chars

Bandwidth Utilization * 60 (1 - 100) %

Balance Mode * High Performance High Compatibility

Description (0 - 255) chars

3. **In the LLB Profile Configuration page, configure as follows:**

Option	Description
Profile Name	Specifies the Profile name whose length range is 1-96 characters.
Bandwidth Utilization	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.
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 mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.

Option	Description
Description	Configure Additional details for the LLB profile.

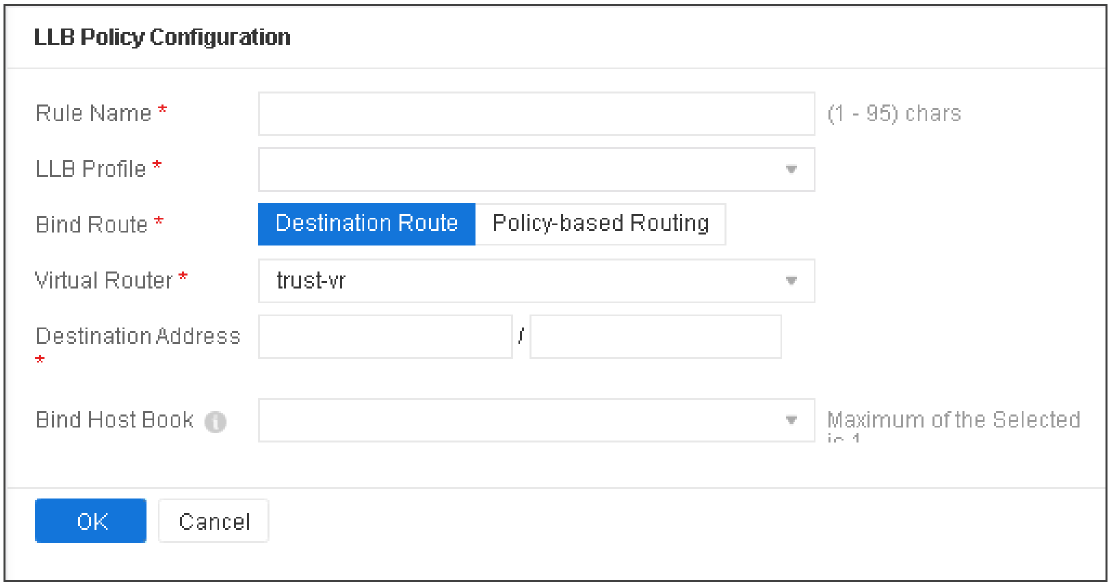
4. Click **OK**.

Configuring LLB Rule

The LLB Profile and the route is bound by the formation of LLB rules that currently support binding destination routing (DBR) and policy-based routing (PBR).

1. Select **Network** > **Outbound** > **Rule**.

2. Click **New**.



LLB Policy Configuration

Rule Name *		(1 - 95) chars
LLB Profile *		
Bind Route *	Destination Route / Policy-based Routing	
Virtual Router *	trust-vr	
Destination Address *	/	
Bind Host Book		Maximum of the Selected is 1

3. **In the LLB Policy Configuration page, configure the following:**

Option	Description
Rule Name	Specifies the Rule name, length of 1-96 characters
LLB Profile	Specifies the bandwidth utilization threshold. It is in the range of 0-100 (0% -100%) and defaults to 60.
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.

4. Click **OK**.

Inbound Link Load Balancing

After enabling the LLB for inbound traffic, the system will resolve domains of different IPs based on the sources of the DNS requests and return IPs for different ISPs to the corresponding users who initiate the requests, which reduces access across ISPs. Such a resolution method is known as SmartDNS.

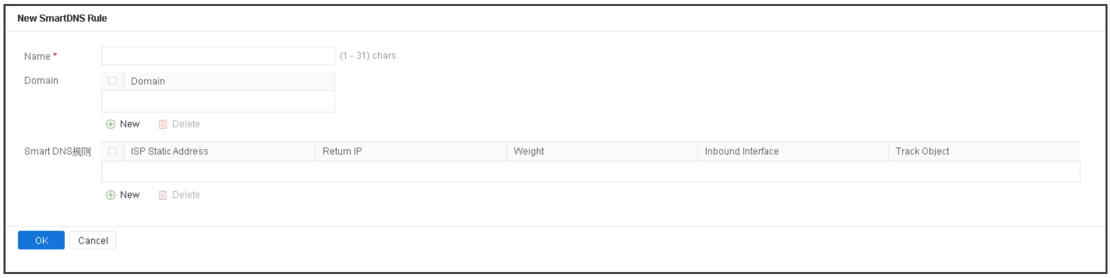
You can enable inbound LLB by the following steps:

1. Enable SmartDNS. This is the prerequisite for the implementation of inbound LLB.
2. Configure a SmartDNS rule table. The smart domain-to-IP resolution is implemented based on the rule table.

Creating a Smart DNS Rule Table

To create a SmartDNS rule table, take the following steps:

1. Select **Network > Inbound**.
2. Click **New > Domain Table**.
3. In the Domain Configuration page, type a domain table name into Domain Table text box.
4. Type a domain name into Domain text box. Separate multiple domain names with comma. Each rule table supports up to 64 domain names (case insensitive).
5. Click **OK**.
6. In the Inbound LLB page, click the domain table name you already created and then click **New**.



New SmartDNS Rule

Name * (1 - 31) chars

Domain

□	Domain

Smart DNS规则

□	ISP Static Address	Return IP	Weight	Inbound Interface	Track Object

In the New SmartDNS Rule page, configure the following:

Option	Description
ISP Static Address	Select a predefined or user-defined ISP from the drop-down list. If the source address matches any address entry of the ISP, system will return the specified IP.
Return IP	Specifies the return IP for different request sources. You can configure up to 64 IPs for a domain name.
Weight	Specifies the weight of the return IP. The value range is 1 to 100. The default value is 1. In the SmartDNS rule table, one domain name might correspond to multiple IPs. System will sort the IPs based on the weight and then return to the users.
Inbound Interface	Specifies the inbound interface for the return IP address. System will judge whether the return IP address is valid according to the track result or the protocol status of the inbound interface. Only the valid IP address will be returned to the request source. Select the proximity address to which the request source address will be matched from the drop-down list.
Track Object	Select a track object of interface type from the drop-

Option	Description
	down list. When the track object fails, the return IP address is invalid. When there' s track object configured on the inbound interface, if the track status is successful, the return IP address is valid. Otherwise the IP address is invalid. When there' s no track object configured on inbound interface, if the protocol state of the interface is UP, the return IP address is valid. Otherwise the IP address is invalid. If you don' t specify the inbound interface for the return IP address, the return IP address is always valid.

7. Click **OK**.

Notes: The ISP route being referenced by the SmartDNS rule table cannot be deleted.

Application Layer Gateway (ALG)

Some applications use multi-channels for data transmission, such as the commonly used FTP. In such a condition the control channel and data channel are separated. Devices under strict security policy control may set strict limits on each data channel, like only allowing FTP data from the internal network to the external network to transfer on the well-known port TCP 21. Once in the FTP active mode, if a FTP server in the public network tries to initiate a connection to a random port of the host in the internal network, devices will reject the connection and the FTP server will not work properly in such a condition. This requires devices to be intelligent enough to properly handle the randomness of legitimate applications under strict security policies. In FTP instances, by analyzing the transmission information of the FTP control channel, devices will be aware that the server and the client reached an agreement, and open up a temporary communication channel when the server takes the initiative to connect to a port of the client, thus assuring the proper operation of FTP.

The system adopts the strictest NAT mode. Some VoIP applications may work improperly after NAT due to the change of IP address and port number. The ALG mechanism can ensure the normal communication of VoIP applications after the NAT. Therefore, the ALG supports the following functions:

- Ensures normal communication of multi-channel applications under strict security policy rules.
- Ensures the proper operation of VoIP applications such as SIP and H.323 in NAT mode, and performs monitoring and filtering according to policies.

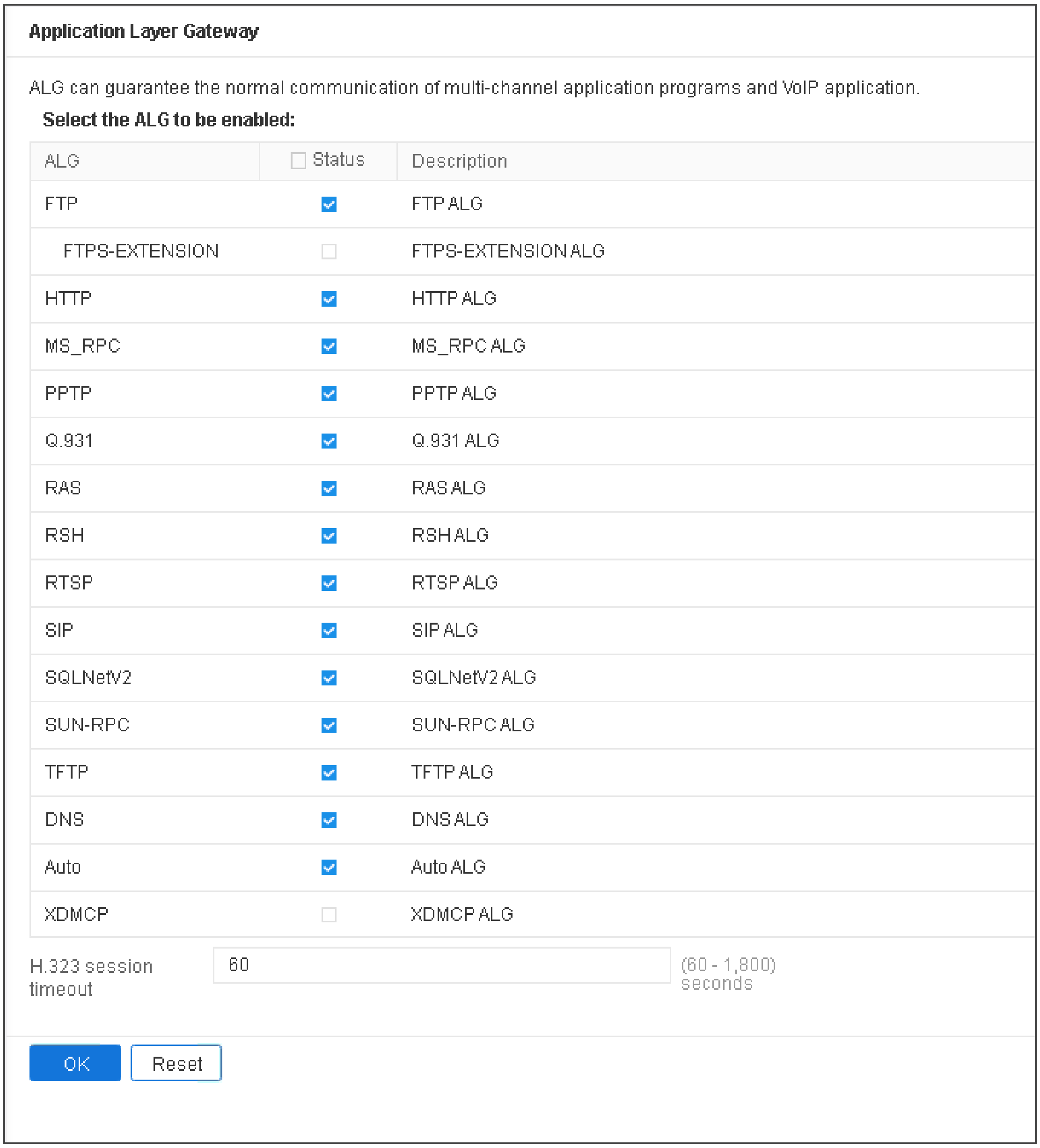
Enabling ALG

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.



Application Layer Gateway

ALG can guarantee the normal communication of multi-channel application programs and VoIP application.

Select the ALG to be enabled:

ALG	□ Status	Description
FTP	☑	FTP ALG
FTPS-EXTENSION	□	FTPS-EXTENSION ALG
HTTP	☑	HTTP ALG
MS_RPC	☑	MS_RPC ALG
PPTP	☑	PPTP ALG
Q.931	☑	Q.931 ALG
RAS	☑	RAS ALG
RSH	☑	RSH ALG
RTSP	☑	RTSP ALG
SIP	☑	SIP ALG
SQLNetV2	☑	SQLNetV2 ALG
SUN-RPC	☑	SUN-RPC ALG
TFTP	☑	TFTP ALG
DNS	☑	DNS ALG
Auto	☑	Auto ALG
XDMCP	□	XDMCP ALG

H.323 session timeout: 60 (60 - 1,800) seconds

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.

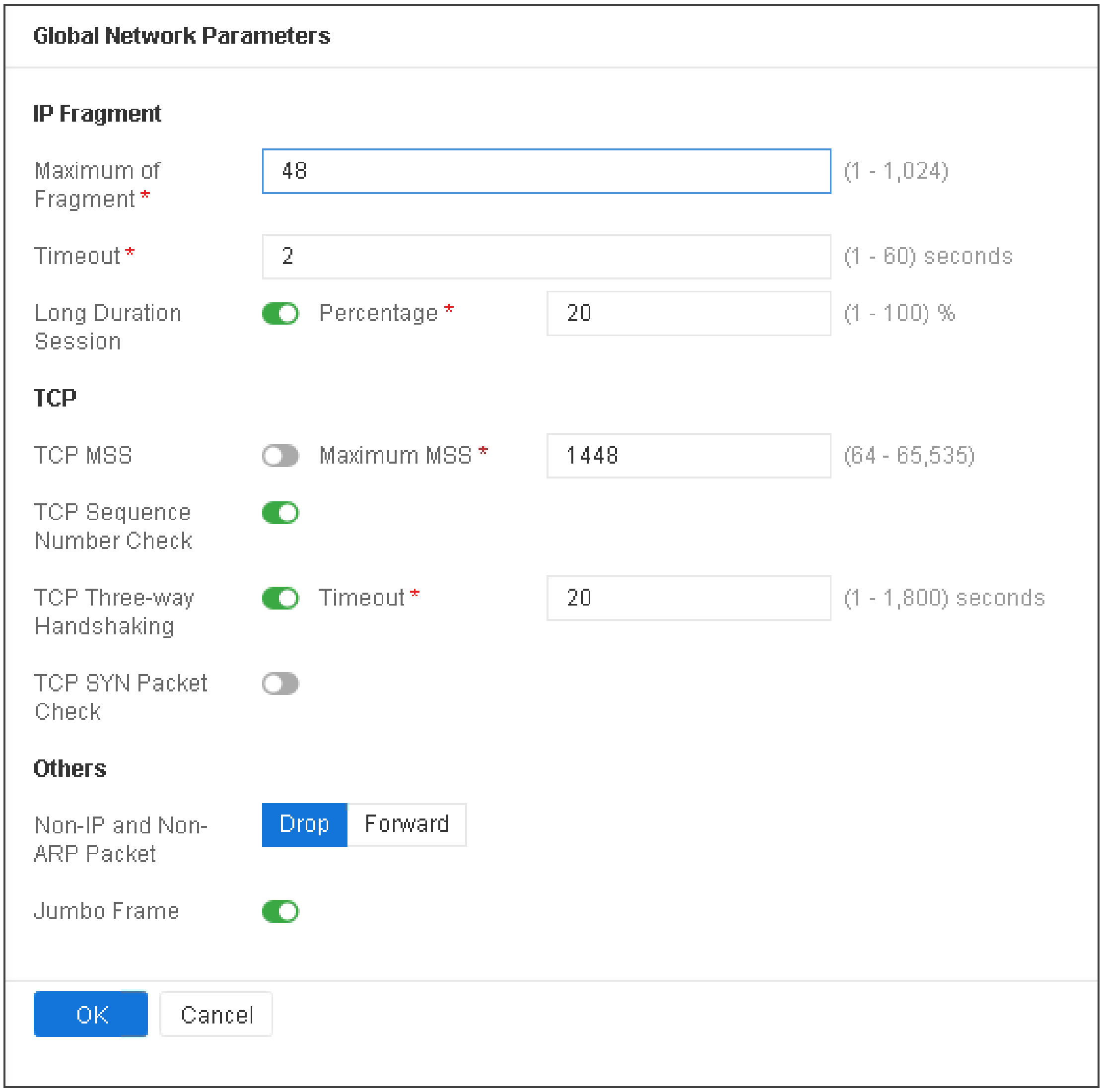
Global Network Parameters

Global network parameter configuration includes IP fragment, TCP packet processing methods and other options.

Configuring Global Network Parameters

To configure global network parameters, take the following steps:

1. Select **Network** > **Global Network Parameters** > **Global Network Parameters**.



Global Network Parameters

IP Fragment

Maximum of Fragment *	48		(1 - 1,024)
Timeout *	2		(1 - 60) seconds
Long Duration Session	☑	Percentage * 20	(1 - 100) %

TCP

TCP MSS	☐	Maximum MSS * 1448	(64 - 65,535)
TCP Sequence Number Check	☑		
TCP Three-way Handshaking	☑	Timeout * 20	(1 - 1,800) seconds
TCP SYN Packet Check	☐		

Others

Non-IP and Non-ARP Packet	[✓ Drop] Forward
Jumbo Frame	☑

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 30. 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.
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 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

Option	Description
	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 Handshaking	Configures if the timeout of TCP three-way handshaking will be checked. 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. • drop: When the received packet is a TCP non-SYN packet, the system will drop the packet.

Option	Description
	• 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.
Others	
Non-IP and Non-ARP Packet	Specifies how to process packets that are neither IP nor ARP.
Jumbo Frame	Click the **Enable**/**Disable** button to enable or disable the Jumbo Frame function. This function is enabled 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

Option	Description
	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.

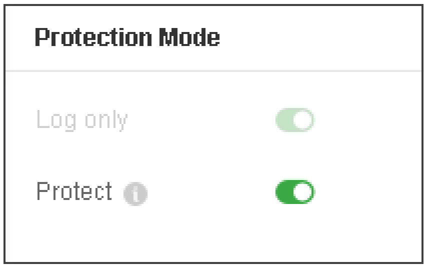
3. Click **OK**.

Configuring Protection Mode

To configure the protection mode, take the following steps:

1. Select **Network** > **Global Network Parameters** > **Protection Mode**.

2. Configure the traffic working mode.



Protection Mode

Log only

Protect

- Log only - System only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections.

- Protect - System not only records attack behavior detected by Intrusion Prevention System, Anti-Virus or AD, Policy, Black list, but also reset the connection or block the access.

Notes: Log & reset mode is recommended. In this mode, the security performance of the device can take effect normally. If log only mode is selected, system can only record logs, and functions which can block traffic in system will be invalid, including policy, IPS, AV, QoS, etc.

Chapter 6 Advanced Routing

Routing is the process of forwarding packets from one network to the destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

Hillstone devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. System implements with a default VRouter trust-vr, and also supports multiple VRouters (multi-VR).

Hillstone devices support destination routing, ISP routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), dynamic routing (including RIP, OSPF and BGP) and Equal Cost MultiPath Routing (ECMP).

- Destination Routing: A manually-configured route which determines the next routing hop according to the destination IP address.
- DIBR: A manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.
- SBR: Source IP based route which selects routers and forwards data according to the source IP address.
- SIBR: Source IP and ingress interface based route.
- ISP Profile: Add a subnet to an ISP.
- ISP Routing: A kind of route which determines the next hop based on different ISPs.
- PBR: A route which forwards data based on the source IP, destination IP address and service type.

- Dynamic Routing: Selects routers and forwards data according to the dynamic routing table generated by dynamic routing protocols ("RIP" on Page 276, "OSPF" on Page 281 or BGP).
- ECMP: Load balancing traffic destined to the same IP address or segment in multiple routes with equal management distance.

When forwarding the inbound packets, the device will select a route in the following sequence: PBR > SIBR > SBR > DIBR > Destination routing/ISP routing/Proximity routing/Dynamic routing.

Routing supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the routing rule.

Related Topics:

- "Destination Route" on Page 241
- "Destination-Interface Route" on Page 244
- "Source Route" on Page 248
- "Source-Interface Route" on Page 252
- "ISP Profile" on Page 256
- "ISP Route" on Page 259
- "Policy-based Route" on Page 263
- "RIP" on Page 276

Destination Route

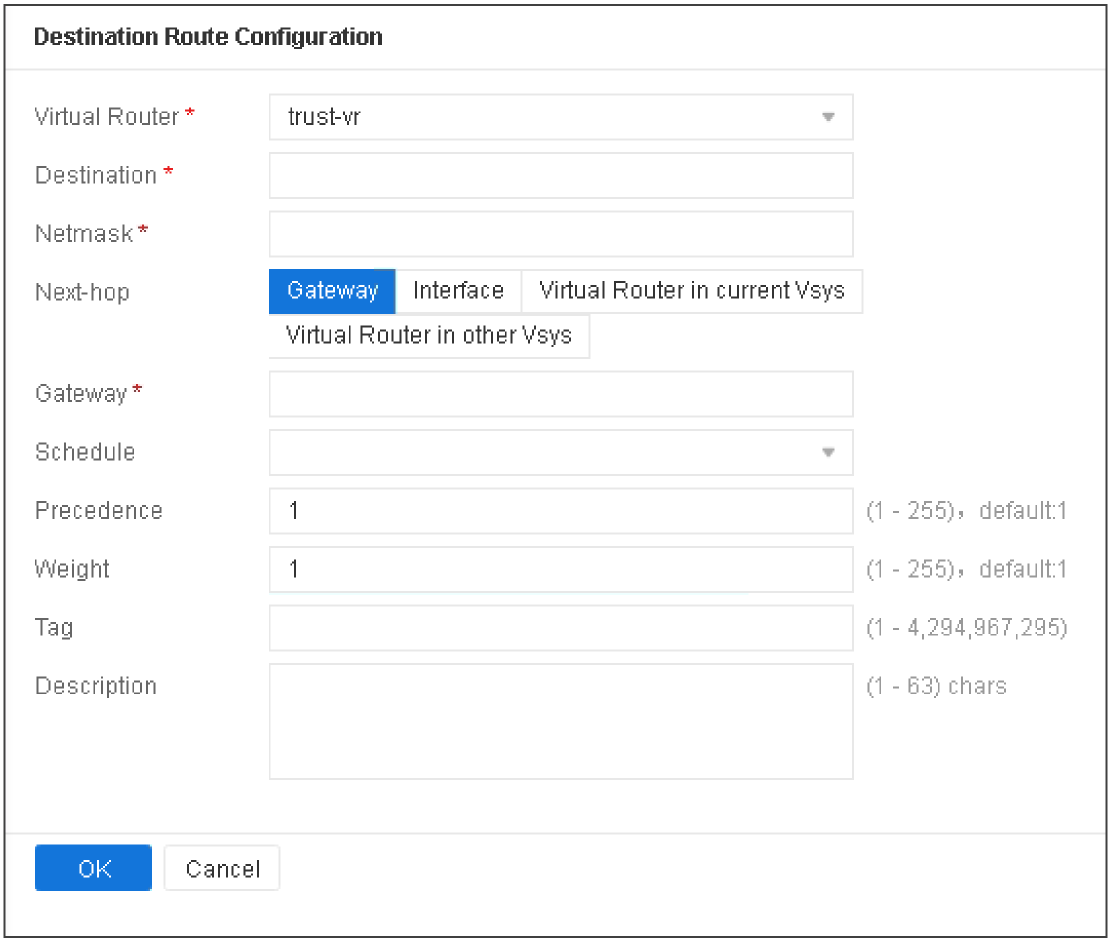
The destination route is a manually-configured route entry that determines the next routing hop based on the destination IP address. Usually a network with comparatively a small number of outbound connections or stable Intranet connections will use a destination route. You can add a default route entry at your own choice as needed.

Creating a Destination Route

To create a destination route, take the follwing steps:

1. Select **Network** > **Routing** > **Destination Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 destination route or IPv6 destination route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

   In the Destination Route Configuration page, enter values.



Destination Route Configuration

Virtual Router * trust-vr

Destination *

Netmask *

Next-hop: Gateway | Interface | Virtual Router in current Vsys | Virtual Router in other Vsys

Gateway *

Schedule

Precedence 1 (1 - 255)，default:1

Weight 1 (1 - 255)，default:1

Tag (1 - 4,294,967,295)

Description (1 - 63) chars

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Destination	Type the IP address for the route into the text box.
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Current VRouter**, **Interface**, or **Other VRouter**. • Gateway: Type the IP address into the **Gateway**

Option	Description
	text box. - Current VRouter: Select a name from the drop-down list. - Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below. - Other VRouter: Select a name from the **Vsys** drop-down list. Select a name from the **Virtual Router** drop-down list.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This para-

Option	Description
	meter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Tag	Specifies the tag value of the destination route. When OSPF redistributes routes, if the configured routing tag values here are matched to the rules in the routing mapping table, the route will be redistributed to filter its information. The value range is 1 to 4294967295.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

Destination-Interface Route

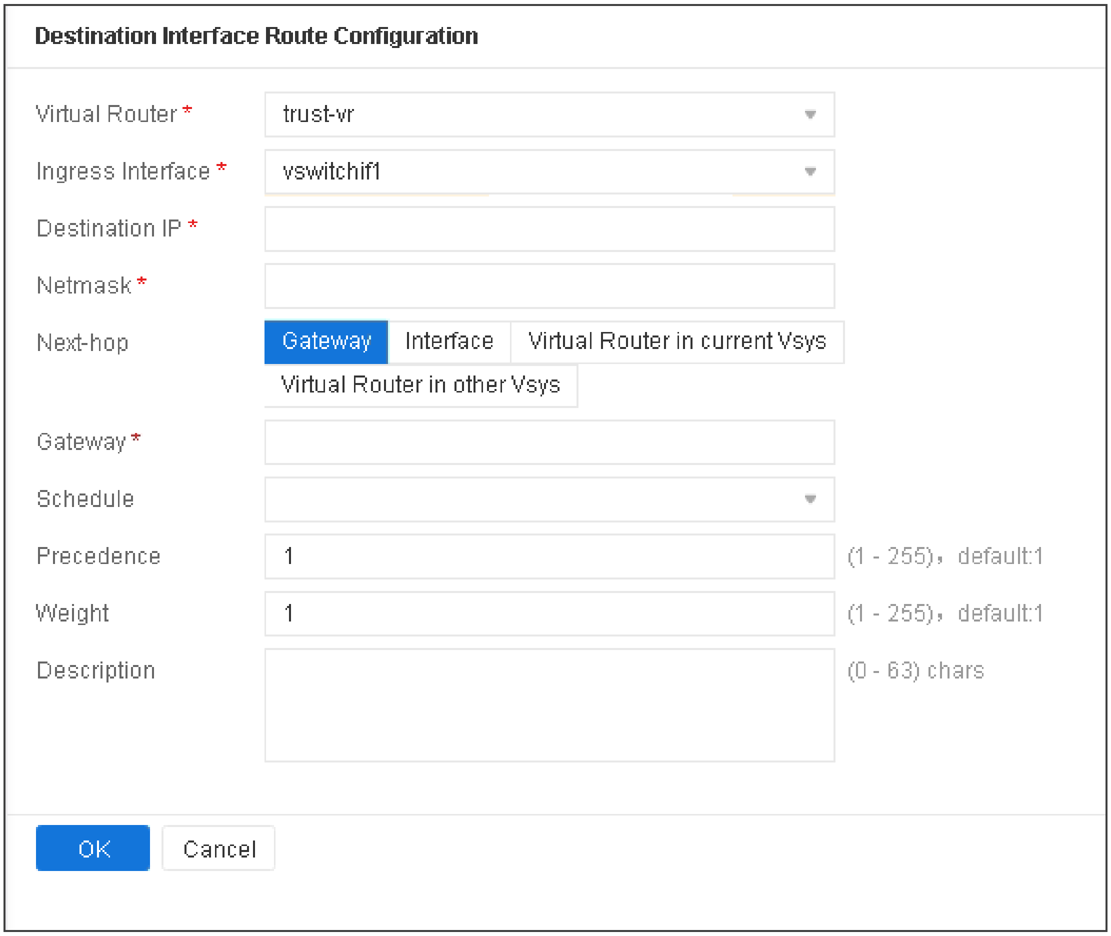
Destination interface route is designed to select a route and forward data based on the Destination IP address and ingress interface of a packet.

Creating a Destination-Interface Route

To create a Destination-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Destination Interface Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 Destination-Interface route or IPv6 Destination-Interface route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

In the Destination Interface Route Configuration page, enter values.



Destination Interface Route Configuration

Virtual Router * trust-vr

Ingress Interface * vswitchif1

Destination IP *

Netmask *

Next-hop: Gateway | Interface | Virtual Router in current Vsys | Virtual Router in other Vsys

Gateway *

Schedule

Precedence 1 (1 - 255)，default:1

Weight 1 (1 - 255)，default:1

Description (0 - 63) chars

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Destination IP	Type the Destination IP for the route into the textbox.
Netmask	Type the corresponding subnet mask into the textbox.

Option	Description
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router in current Vsys: Select a name from the **Virtual Router** drop-down list. • Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below. • Virtual Router in other Vsys: Select a name from the **Vsys** drop-down list. Select a name from the **Virtual Router** drop-down list.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will

Option	Description
	be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the DIBR into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

Source Route

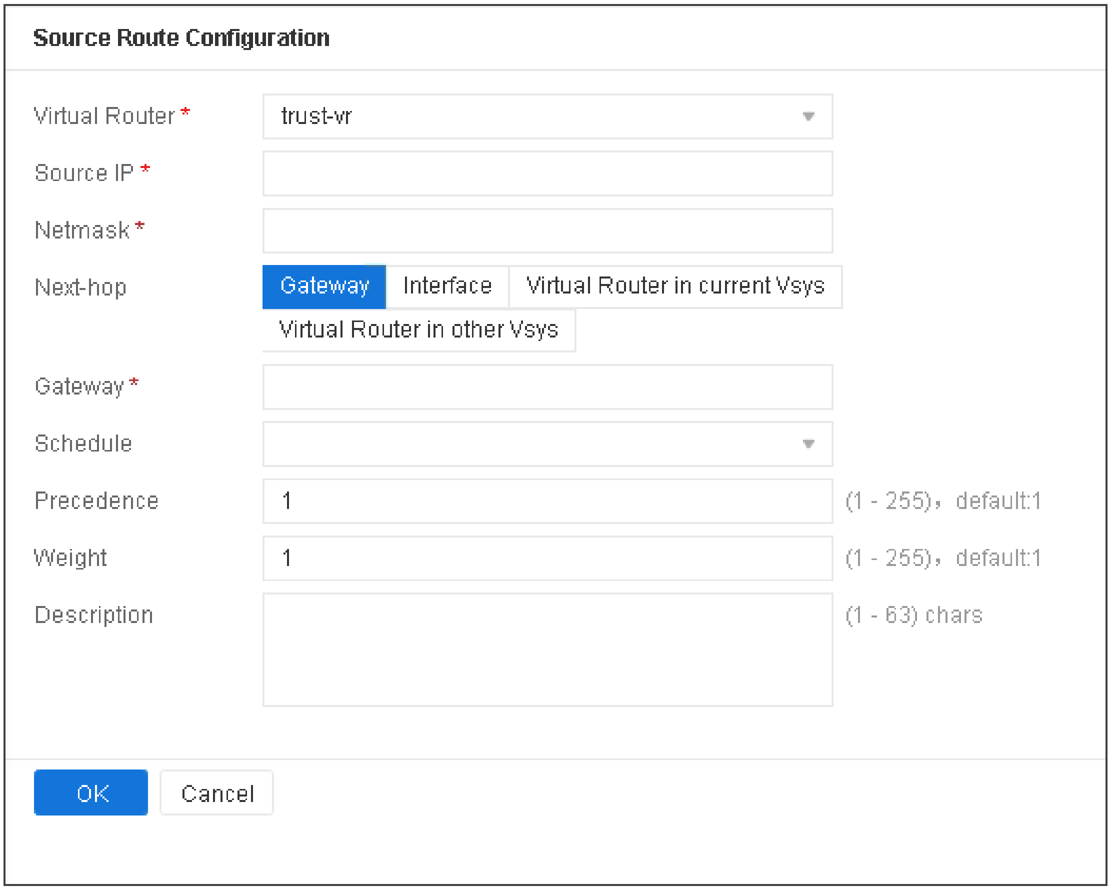
Source route is designed to select a router and forward data based on the source IP address of a packet.

Creating a Source Route

To create a source route, take the following steps:

1. Select **Network** > **Routing** > **Source Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 source route or IPv6 source route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

In the Source Route Configuration page, enter values.



Source Route Configuration

Virtual Router * trust-vr

Source IP *

Netmask *

Next-hop: [✓ Gateway] Interface Virtual Router in current Vsys Virtual Router in other Vsys

Gateway *

Schedule

Precedence 1 (1 - 255)，default:1

Weight 1 (1 - 255)，default:1

Description (1 - 63) chars

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Source IP	Type the source IP for the route into the box.
Netmask	Type the corresponding subnet mask into the box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box.

Option	Description
	• Virtual Router in current Vsys: Select a name from the drop-down list. • Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below. • Virtual Router in other Vsys: Select a name from the **Vsys** drop-down list. Select a name from the **Virtual Router** drop-down list.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.

Option	Description
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

Source-Interface Route

Source interface route is designed to select a router and forward data based on the source IP address and ingress interface of a packet.

Creating a Source-Interface Route

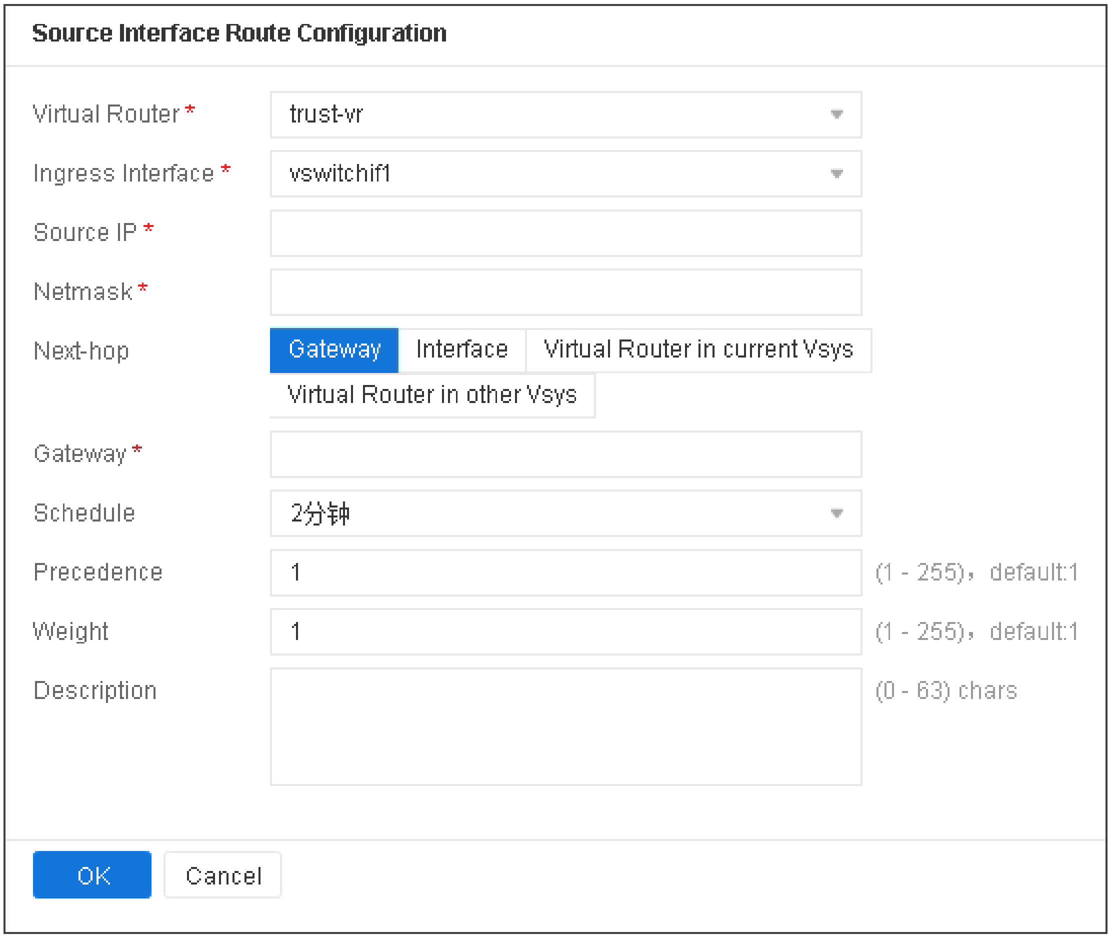
To create a Source-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Source Interface Route**.

2. Select the IPv4 or IPv6 tab page, and create an IPv4 Source-Interface route or IPv6 Source-Interface route on the corresponding page. This step is only applicable for IPv6 version.

3. Click **New**.

   In the Source Interface Route Configuration page, enter values.



Source Interface Route Configuration

Virtual Router * trust-vr

Ingress Interface * vswitchif1

Source IP *

Netmask *

Next-hop: Gateway | Interface | Virtual Router in current Vsys | Virtual Router in other Vsys

Gateway *

Schedule 2分钟

Precedence 1 (1 - 255)，default:1

Weight 1 (1 - 255)，default:1

Description (0 - 63) chars

Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Source IP	Type the source IP for the route into the textbox.
Netmask	Type the corresponding subnet mask into the textbox.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual**

Option	Description
	Router in current Vsys, **Interface**, or **Virtual Router in other Vsys**. - Gateway: Type the IP address into the **Gateway** text box. - Virtual Router in current Vsys: Select a name from the **Virtual Router** drop-down list. - Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below. - Virtual Router in other Vsys: Select a name from the **Vsys** drop-down list. Select a name from the **Virtual Router** drop-down list.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default

Option	Description
	value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

ISP Profile

To configure an ISP route, you need to first add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information.

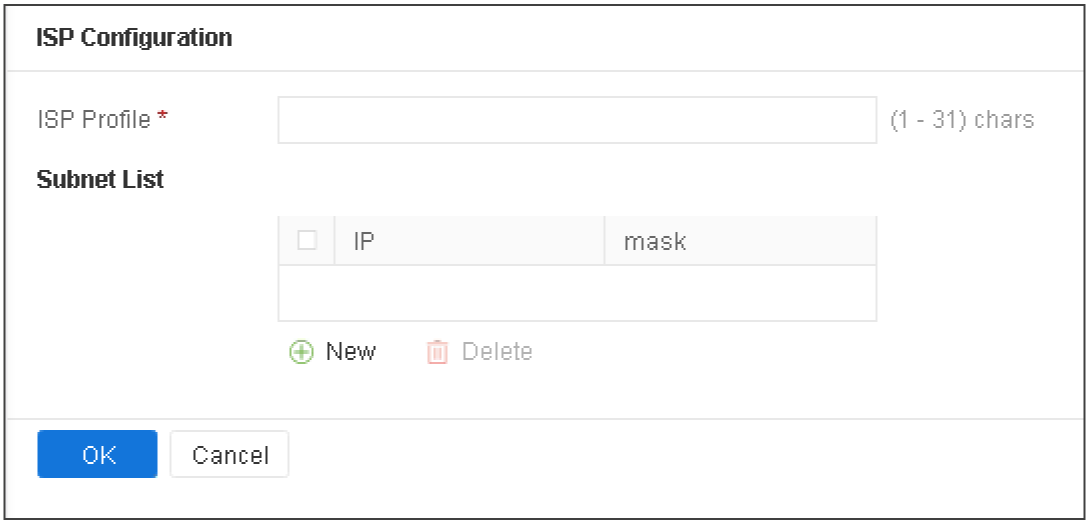
Creating an ISP Profile

To create an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.

2. Click **New**.

In the ISP Configuration page, enter values.



ISP Configuration

ISP Profile * ____ (1 - 31) chars

Subnet List

□	IP	mask

Option	Description
ISP Profile	Type the name for the new ISP profile into the textbox.
Subnet Prefix	Type the IP address for the subnet into the textbox.
Netmask	Type the subnet mask into the textbox.

Option	Description
New	Add the subnet to the ISP profile. The subnet will be displayed in the ISP subnet list below. If needed, repeat the steps to add multiple subnets for the ISP profile.
Delete	Delete the selected ISP profiles.

3. Click **OK**.

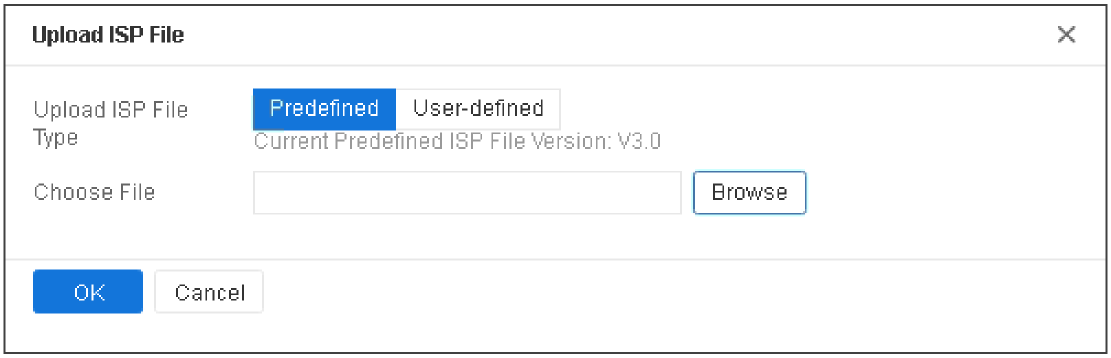
Uploading an ISP Profile

To upload an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.

2. Click **Upload**.

   In the Upload ISP File page, enter values.



Upload ISP File

Upload ISP File Type: Predefined (selected) | User-defined

Current Predefined ISP File Version: V3.0

Choose File:

Option	Description
Upload Predefined ISP File	To update the predefined IPS file: 1. Select **Upload Predefined IPS File**. 2. Click **Browse** to select an ISP profile in your PC.
User-defined	To update the user-defined IPS file:

Option	Description
ISP File	1. Select **Upload Predefined IPS File**. 2. Click **Browse** to select an ISP profile in your PC.

3. Click **Upload** to upload the selected ISP profile to device.

Saving an ISP Profile

To save an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.

2. Click **Save**.

3. In the Save User-defined ISP Configuration page, select an ISP profile from the **ISP profile** drop-down list.

4. Click **Save** to save the profile to a specified location in PC.

ISP Route

Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not have the function based on the traffic's direction. For such a scenario, the device provides the ISP route, which allows traffic from different ISPs to take their proprietary routes, thus accelerating network access.

To configure an ISP route, first you need to add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information.

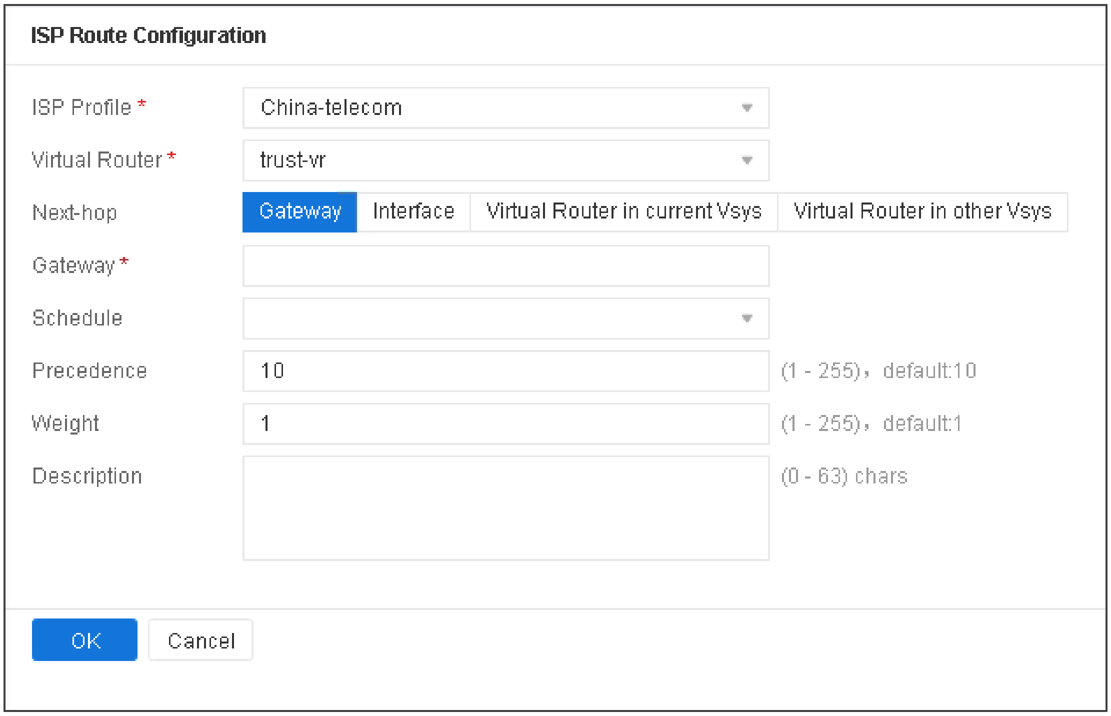
Creating an ISP Route

To create an ISP route, take the following steps:

1. Select **Network** > **Routing** > **ISP Route**.

2. Click **New**.

   In the ISP Configuration page, enter values.



ISP Route Configuration

ISP Profile * China-telecom

Virtual Router * trust-vr

Next-hop Gateway

Gateway *

Schedule

Precedence 10 (1 - 255), default:10

Weight 1 (1 - 255), default:1

Description (0 - 63) chars

Option	Description
ISP Profile	Select an ISP profile name from the drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Next-hop	To specify the type of next hop, click **Gateway**, **Current VRouter**, **Interface**, or **Other VRouter**. • Gateway: Type the IP address into the **Gateway** text box. • Current VRouter: Select a name from the **Virtual Router** drop-down list. • Interface: Select a name from the **Interface** drop-

Option	Description
	down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below. - Other VRouter: Select a name from the **Vsys** drop-down list. Select a name from the **Virtual Router** drop-down list.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 10. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description

Option	Description
	text box if necessary.

3. Click **OK**.

Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet.

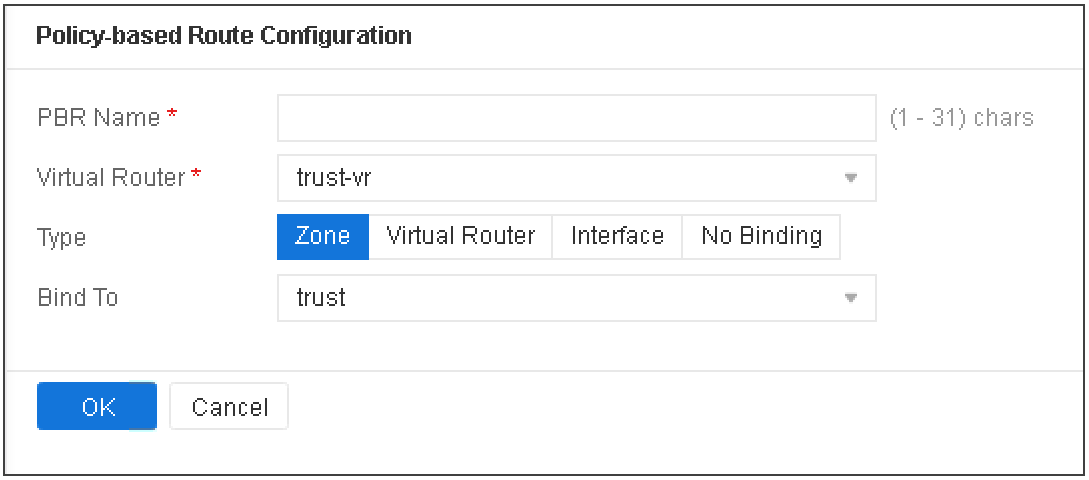
Creating a Policy-based Route

To create a Policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**. Select **PBR** from the drop-down list.

   In the Policy-based Route Configuration page, configure the following.



Policy-based Route Configuration

PBR Name * (1 - 31) chars

Virtual Router * trust-vr

Type: Zone | Virtual Router | Interface | No Binding

Bind To: trust

Option	Description
PBR Name	Specifies a name for the policy-based route.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	Specifies the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface**

Option	Description
	or **No Binding**. - Zone: Click this option button and select a zone from the **Bind To** drop-down list. - Virtual Router: Click this option button and show the virtual router that the policy-based route bind to. - Interface: Click this option button and select a interface from the **Bind To** drop-down list. - No Binding: This policy-based route is no binding.

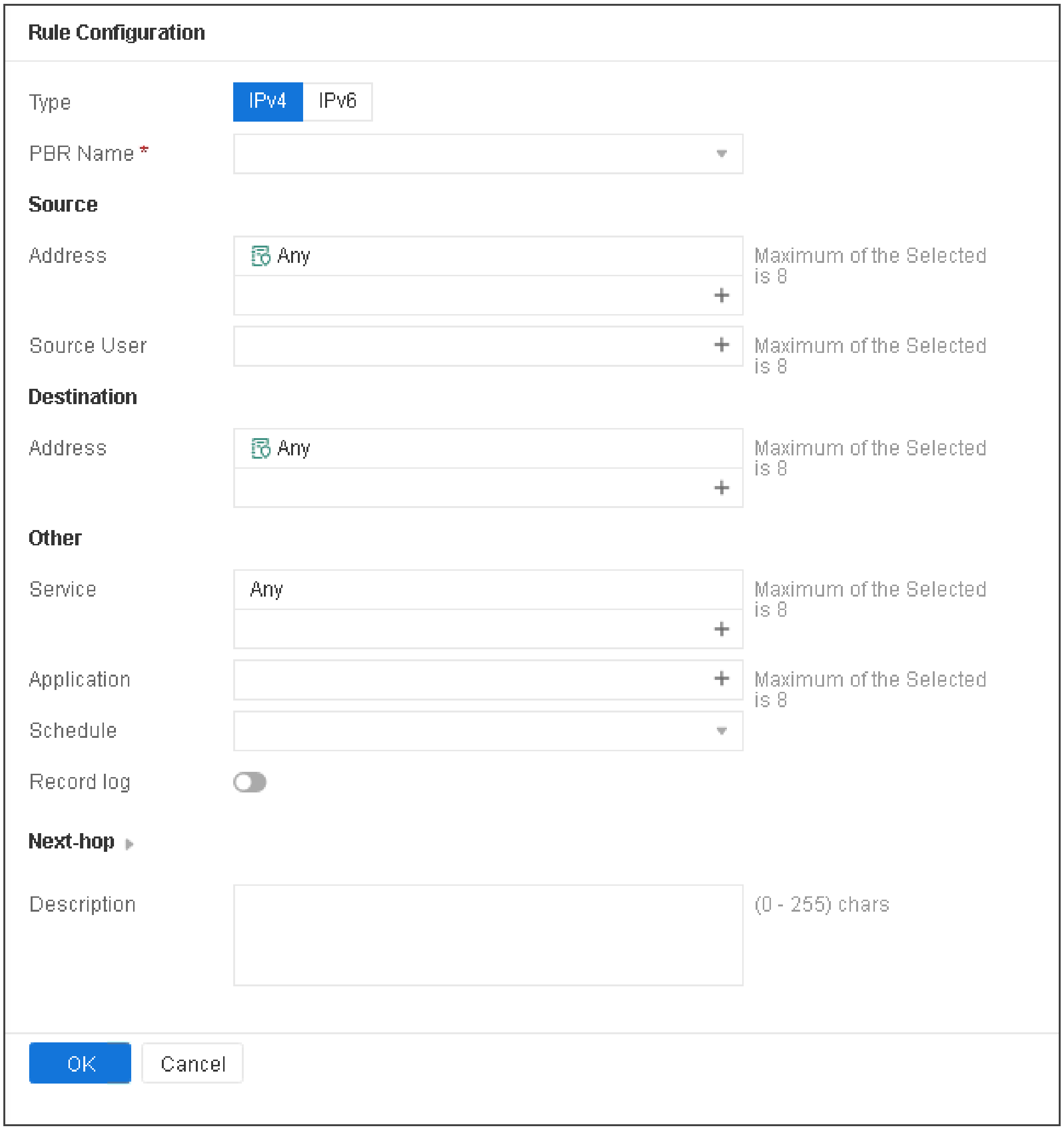
3. Click **OK**.

Creating a Policy-based Route Rule

To create a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**. Select **Rule** from the drop-down list.



Rule Configuration

Type	IPv4 / IPv6
PBR Name *	
Source	
Address	Any
Source User	
Destination	
Address	Any
Other	
Service	Any
Application	
Schedule	
Record log	
Next-hop	
Description	

Maximum of the Selected is 8
Maximum of the Selected is 8
Maximum of the Selected is 8
Maximum of the Selected is 8
Maximum of the Selected is 8
(0 - 255) chars
OK
Cancel

In this page, configure the following.

Option	Description
PBR Name	Specifies a name for the policy-based route.

Option	Description
Description （Optional）	Type information about the PBR rule.
Source	
Address	Specifies the source addresses of PBR rule. 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**. You can also perform other operations: - When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. - The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
User	Specifies a role, user or user group for the PBR rule. 1. From the **User** drop-down menu, select the AAA server which the users and user groups belongs to. To specify a role, select **Role** from the **AAA Server** drop-down list.

Option	Description
	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, enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add them to the left panes. 4. After adding the desired objects, click the **Close** to complete the user configuration.
Destination	
Address	Specifies the destination addresses of PBR rule. 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 panes. 4. After adding the desired addresses, click **Close**. You can also perform other operations: - When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. - The default address configuration is any. To restore the configuration to this default one, select the **any**

Option	Description
	check box.
Other	
Service	Specifies a service or service group. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search 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 left panes. 4. After adding the desired objects, click **Close**. You can also perform other operations: - To add a new service or service group, select **User-defined** from the **Predefined** drop-down listr, and click ⊕ button. - The default service configuration is any. To restore the configuration to this default one, select the **any** check box.
Application	Specifies an application/application group/application filters. 1. From the **Application** drop-down menu, you can search the desired application/application group/application filter, expand the list of applic-

Option	Description
	ations/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click them to add them to the left panes. 3. After adding the desired objects, click **Close** to complete the application configuration. You can also perform other operations: - To add a new application group, click **New AppGroup**. - To add a new application filter, click **New AppFilter**.
Schedule	Specifies a schedule when the PBR rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click **Close** to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Record log	Click the **Enable** button to enable the logging function for PBR rules.

Expand Next-hop, configure the following.

Option	Description
Set Next-hop	To specify the type of next hop, click **IP Address**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**.

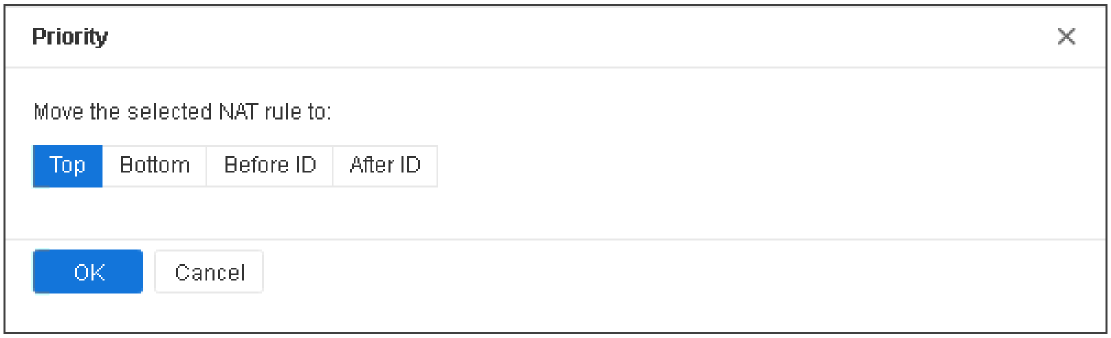
Option	Description
	• IP Address: Type IP address into the **IP address** text box and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. • Virtual Router in current Vsys: Select a name from the **Next-Hop Virtual Router** drop-down list and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. • Interface: Select an interface from the **Interface** drop-down list and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. • Virtual Router in other Vsys: Check the radio button to specify a virtual router in the current VSYS as the next hop. Select a virtual router from the **Virtual Router** drop-down list and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value.
Track Object	Select the track object from the drop-down list. See

Option	Description
	"Track Object" on Page 654.
Weight	Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, system will distribute the traffic in proportion to the corresponding weight.
Add	Click to add the specified next hop.
Delete	Select next-hop entries from the next hop table and click this button to delete.

Adjusting Priority of a PBR Rule

To adjust priority of a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Select the rule you want to adjust priority from the list below, click **Priority**.
4. In the Priority page, enter values.


Priority

Move the selected NAT rule to:

Option	Description
Top	Click this option button to move the PBR rule to the top.
Bottom	Click this option button to move the PBR rule to the bottom.
Before ID	Click this option button and type the ID into the box to move the PBR rule to the position before the ID.
After ID	Click this option button and type the ID into the box to move the PBR rule to the position after the ID.

Notes: Each PBR rule is labeled with a unique ID. When traffic flows into a Hillstone device, the device will query for PBR rules by turn, and process the traffic according to the first matched rule. However, the PBR rule ID is not related to the matching sequence during the query. You can move a PBR rule's location up or down at your own choice to adjust the matching sequence accordingly.

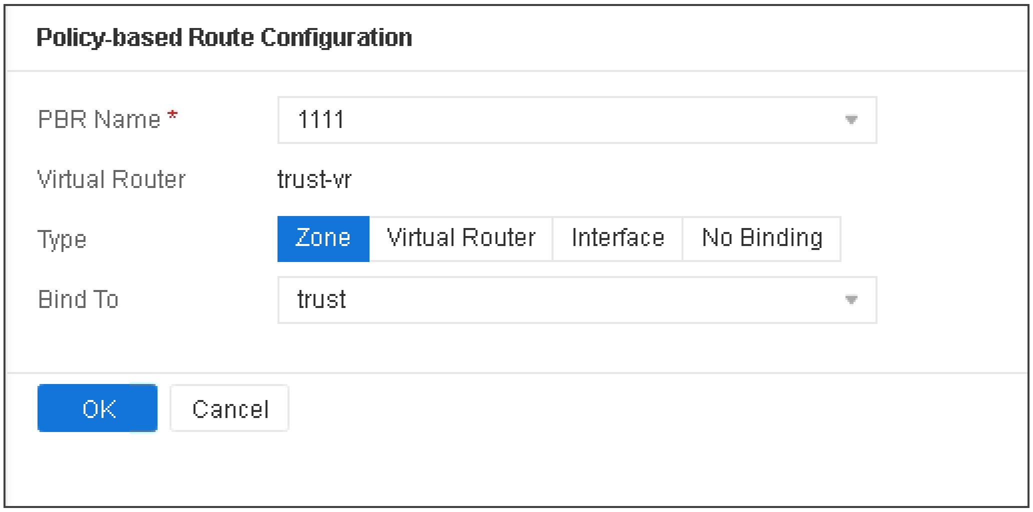
Applying a Policy-based Route

You can apply a policy-based route by binding it to an interface, virtual router or zone.

To apply a policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Click **Bind to**.

   In the Policy-based Route Configuration page, enter values.



Policy-based Route Configuration

PBR Name * 1111

Virtual Router trust-vr

Type Zone

Bind To trust

Option	Description
PBR Name	Select a route from the PBR name drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	Specifies the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface** or **No Binding**. • Zone: Click this option button and select a zone from the **Bind To** drop-down list. • Virtual Router: Click this option button and show

Option	Description
	the virtual router that the policy-based route binds to. • Interface: Click this option button and select a interface from the **Bind To** drop-down list. • No Binding: This policy-based route is no binding.

4. Click **OK**.

DNS Redirect

System supports the DNS redirect funtion, which redirects the DNS requests to a specified DNS server. For more information about specifying IP addresses of the DNS server, see Configuring a DNS Server. Currently, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy based route working together, system can redirect the Web video traffic to different links, improving the user experience.

To enable the DNS redirect function, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. Click **Enable DNS Redirect**.

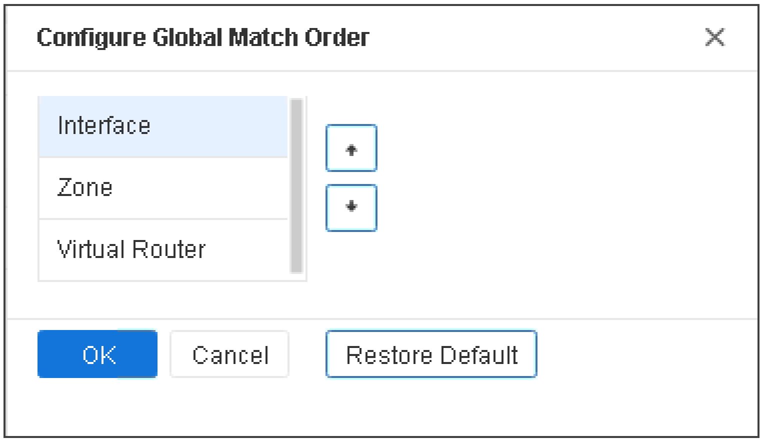
Configuring the Global Match Order

By default, if the PRB rule is bound to both an interface , VRouter and the security zone the interface belongs to, the traffic matching sequence will be: Interface > Zone > VRouter. You can configure the global match order of PBR.

To configure the global match order, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **Config Global Match Order**.



3. Select the items that need to be adjusted, and click ↑ and ↓.

4. To restore the default matching sequence, click **Restore Default**.

5. Click **OK**.

RIP

RIP, Routing Information Protocol, is an internal gateway routing protocol that is designed to exchange routing information between routers. Currently, devices support both RIP versions, i.e., RIP-1 and RIP-2.

RIP configuration includes basic options, redistribute, Passive IF, neighbor, network and distance. You will also need to configure RIP parameters for different interfaces, including RIP version, split horizon, and authentication mode.

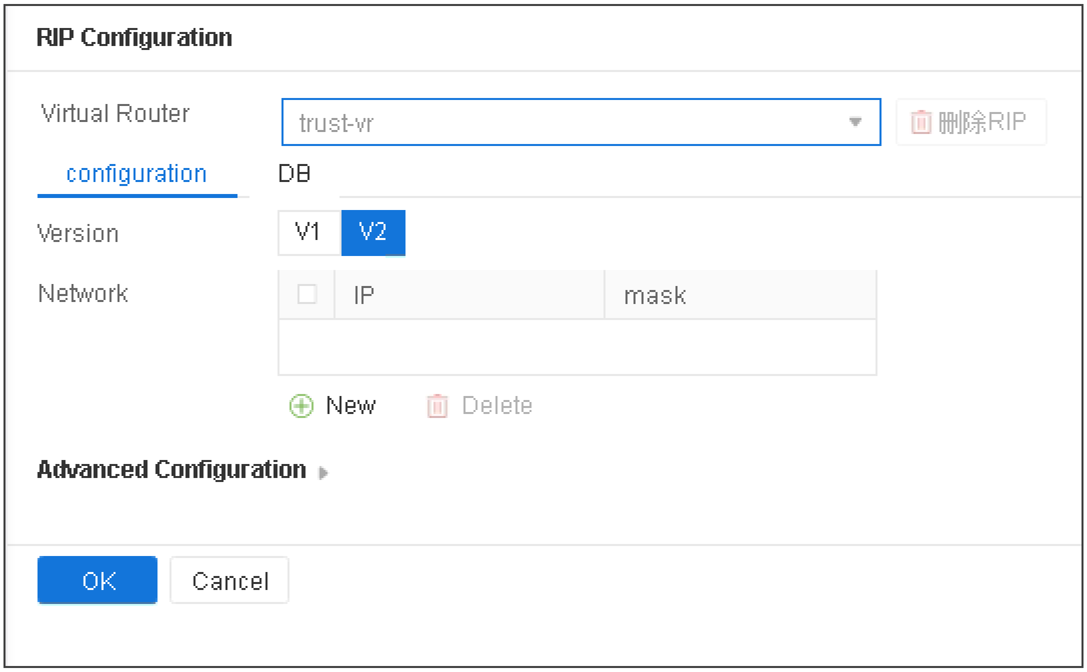
Creating RIP

To create RIP, take the following steps:

1. Select **Network** > **Routing** > **RIP**.

2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.

3. Click **New**.



RIP Configuration

Virtual Router: trust-vr

Version: V2

□	IP	mask

In the configuration tab, configure the following.

Option	Description
Version	Specifies a RIP version. Hillstone devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. Select a version from the drop-down list. The default version is RIP-2.
Network	
Network (IP/netmask)	Type the IP address and netmask into the **Network (IP/netmask)** box.
New	Click **New** to add the network. All the networks that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more networks. To delete a network, select the entry you want to delete from the list, and click **Delete**.

Click Advanced Configuration, configure the following.

Option	Description
Metric	Specifies a default metric. The value range is 1 to 15. If no value is specified, the value of 1 will be used. RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, increment is 1 for every additional router between them. The max metric is 15, and the network with metric larger than 15 is not

Option	Description
	reachable. The default metric will take effect when the route is redistributed.
Distance	Specifies a default distance. The value range is 1 to 255. If no value is specified, the value of 120 will be used.
Default-info originate	Specifies if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. Click the **Enable** button to redistribute the default route.
Update interval	Specifies an interval in which all RIP routes will be sent to all the neighbors. The value range is 0 to 16777215 seconds. The default value is 30.
Invalid time	If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The value range is 1 to 16777215 seconds. The default value is 180.
Hold-down time	If the metric becomes larger (e.g., from 2 to 4) after a route has been updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The value range is 1 to 16777215 seconds. The default value is 180.
Flush time	System will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the end of flush time, it will be deleted from the RIP information data-

Option	Description
	base. The value range is 1 to 16777215 seconds. The default value is 240.
Redistribute	
Protocol	Select a protocol type for the route from the **Protocol** drop-down list. The type can be Connected, Static, OSPF or BGP.
New	Click **New** to add the Redistribute route entry. All the entries that have been added will be displayed in the Redistribute Route list below.
Delete	Repeat the above steps to add more Redistribute route entries. To delete a Redistribute route entry, select the entry you want to delete from the list, and click **Delete**.
Neighbor	
Neighbor IP	Type the neighbor IP into the **Neighbor IP** box.
New	Click **New** to add the neighbor IP. All the neighbor IPs that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more neighbor IPs. To delete a neighbor IP, select the entry you want to delete from the list, and click **Delete**.
Distance	
Distance	Type the distance into the **Distance** box. The priority of the specified distance is higher than than the default distance.

Option	Description
Network (IP/netmask)	Type the IP prefix and netmask into the **Network(IP/netmask)** box.
New	Click **New** to add the distance. All the distances that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more distances. To delete a distance, select the entry you want to delete from the list, and click **Delete**.

Click **Interface Configuration**, configure the following.

Option	Description
Edit	Select the check box of an interface from the Interface page, and click **Edit** to open the Interface Configuration page.

In the DB tab, view the database of the RIP route .

All the route entries that can reach target network are stored in the database.

4. Click **OK**.

Notes: Configuration for RIP on Hillstone device's interfaces includes: RIP version, split horizon and authentication mode. For more information on how to configure RIP on an interface, see "Creating a PPPoE Interface" on Page 81.

OSPF

OSPF, the abbreviation for Open Shortest Path First, is an internal gateway protocol based on link state developed by IETF. The current version of OSPF is version 2 (RFC2328). OSPF is applicable to networks of any size. Its quick convergence feature can send update message immediately after the network topology has changed, and its algorithm assures it will not generate routing loops. OSFP also have the following characteristics:

- Area division: divides the network of autonomous system into areas to facilitate management, thereby reducing the protocol’ s CPU and memory utilization, and improving performance.
- Classless routing: allows the use of variable length subnet mask.
- ECMP: improves the utilization of multiple routes.
- Multicasting: reduces the impact on non-OSPF devices.
- Verification: interface-based packet verification ensures the security of the routing calculation.

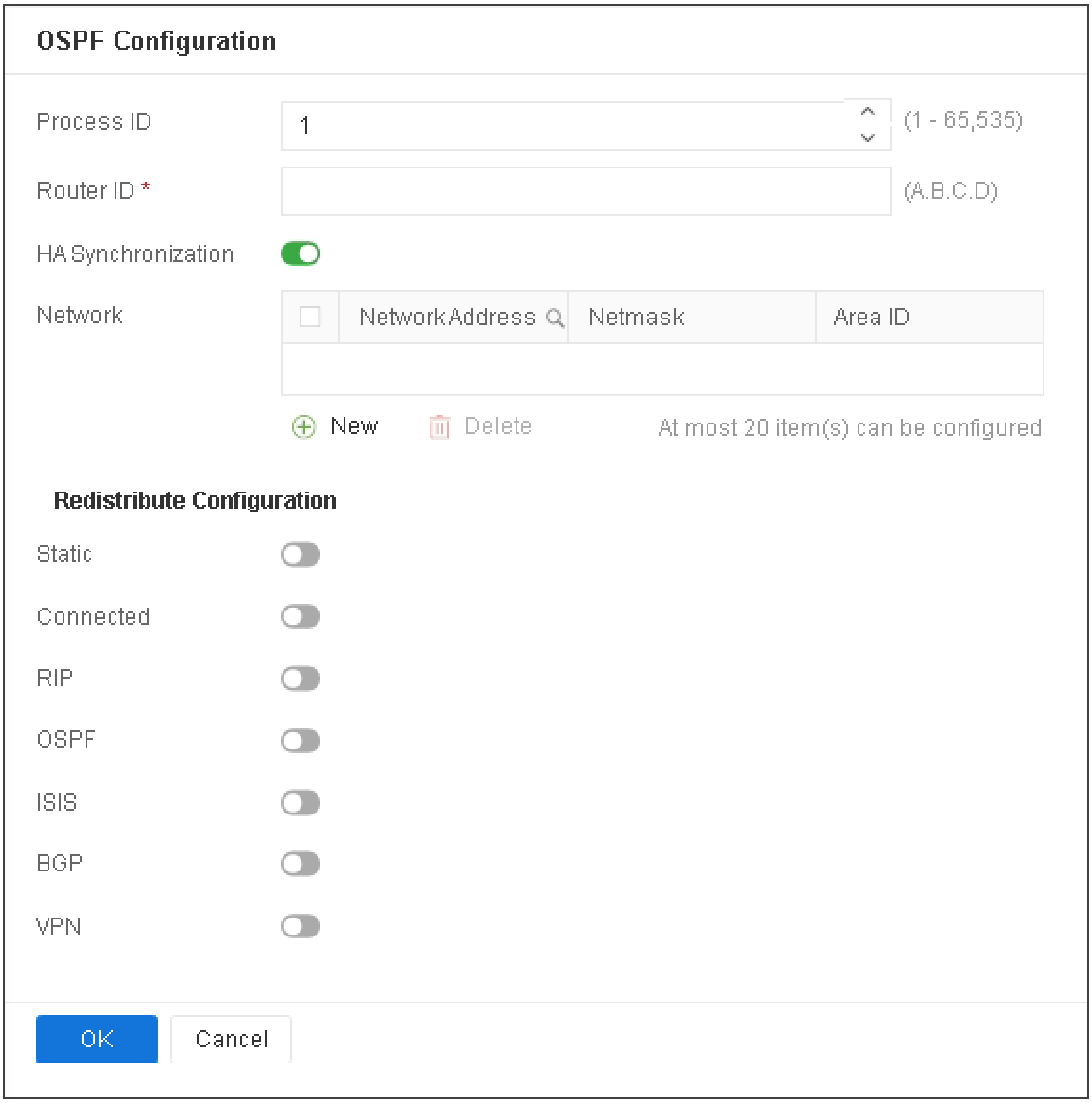
Note: Autonomous system is a router and network group under the control of a management institution. All routers within an autonomous system must run the same routing protocol.

Creating OSPF

To create OSPF, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.

3. Click **New**.



OSPF Configuration

Process ID: 1 (1 - 65,535)

Router ID *: (A.B.C.D)

HA Synchronization: ●

Network

☐	Network Address	Netmask	Area ID

Redistribute Configuration

Static ○
Connected ○
RIP ○
OSPF ○
ISIS ○
BGP ○
VPN ○

In this page, configure the following.

Option	Description
Process ID	Enter the OSPF process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPF process is individual, and has its own link state database and the related OSPF routing

Option	Description
	table. Each VRouter supports up to 4 OSPF processes and multiple OSPF processes maintain a routing table together. When specifying the OSPF process ID, note the following matters: • When running multiple OSPF processes in a VRouter, the network advertised in interfaces in each OSPF process cannot be same. • When route entries with the same prefix exist in multiple OSPF processes, the system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table. • If the OSPF route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPF will not be redistributed.

Option	Description
Router ID	Enter the Router ID used by OSPF protocol. Each router running OSPF protocol should be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPF domain, represented in the form of an IP address.
HA Synchronization	Click the **Enable** button to enable HA synchronization. The OSPF configuration of the master and backup will be synchronized.
Network	Configure the network interface that enables OSPF and add the network to the specified area. Click **New**, and enter the network address, network mask and area ID. • Network Address: Enter the IP address of network interface that enables OSPF protocol. • Network Mask: Enter the mask of IP address. • Area ID: Enter the area ID the network will be added to, in form of a 32-bit digital number, or an IP address.
Redistribute Configuration	
Static	Click the **Enable** button to introduce the static

Option	Description
	route protocol into the OSPF route and redistribute.
Connected	Click the **Enable** button to introduce the connected route protocol into the OSPF route and redistribute.
RIP	Click the **Enable** button to introduce the RIP route protocol into the OSPF route and redistribute.
OSPF	Click the **Enable** button to introduce the OSPF route protocol into the OSPF route and redistribute.
ISIS	Click the **Enable** button to introduce the ISIS route protocol into the OSPF route and redistribute.
BGP	Click the **Enable** button to introduce the BGP route protocol into the OSPF route and redistribute.
VPN	Click the **Enable** button to introduce the VPN route into the OSPF route and redistribute.

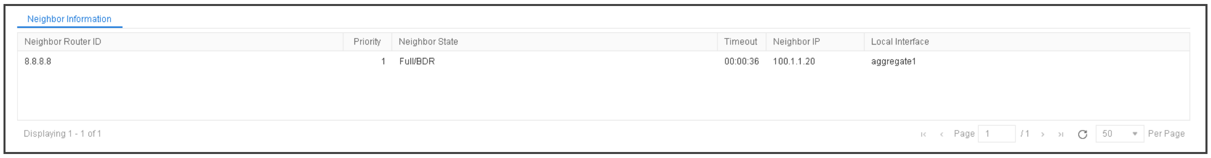
4. Click **OK**.

Notes: Configuration for OSPF on Hillstone device's interfaces includes: hello transmission interval, dead time, LSA transmit interval and LSU transmit delay time. For more information on how to configure OSPF on an interface, see "Creating a PPPoE Interface" on Page 81.

Viewing the Neighbor Information

To view the neighbor information, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.
2. Select the process ID check box, and the neighbor information will be displayed in the list below.



Neighbor Router ID	Priority	Neighbor State	Timeout	Neighbor IP	Local Interface
8.8.8.8	1	Full/BDR	00:00:36	100.1.1.20	aggregate1

Displaying 1 - 1 of 1

- Neighbor Router ID: Shows the router ID of OSPF neighbors.
- Priority: Shows the router priority. The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and broadcast the received link information.
- Neighbor State: Shows the OSPF neighbor state. The OSPF neighbor state includes 8 types: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full. The Full state includes Full/DR and Full/BDR.
- Timeout: Shows the neighbor timeout, which is the difference between dead time and hello transmission interval. The unit is second. If the OSPF doesn't receive the Hello packets from neighbor, the neighbor ship cannot be established continually.

- Neighbor IP: Shows the IP address of neighbor router.

- Local Interface: Shows the interface sends the Hello packets to the neighbor router.

Configuring OSPFv3

OSPFv3 is the third version of Open Shortest Path First and mainly provides the support of IPv6. Before configuring OSPFv3, you need to enable IPv6 at **Network** > **Interface** > **New**, and configure an OSPFv3 interface. For how to configure the OSPFv3 interface, refer to **Configuring an Interface**.

The similarities between OSPFv3 and OSPFv2 are as follows:

- Both protocols use 32 bits Router ID and Area ID.
- Both protocols use the Hello packets, DD (database description) packets, LSR (link state request) packets, LSU (link state update) packets, and LSAck (link state acknowledgment) packets.
- Both protocols use the same mechanisms of finding neighbors and establishing adjacencies.
- Both protocols use the same mechanisms of LSA flooding and aging.

The differences between OSPFv3 and OSPFv2 are as follows:

- OSPFv3 runs on a per-link basis and OSPFv2 is on a per-IP-subnet basis.
- OSPFv3 supports multiple instances per link.
- OSPFv3 identifies neighbors by Router ID, and OSPFv2 identifies neighbors by IP address.

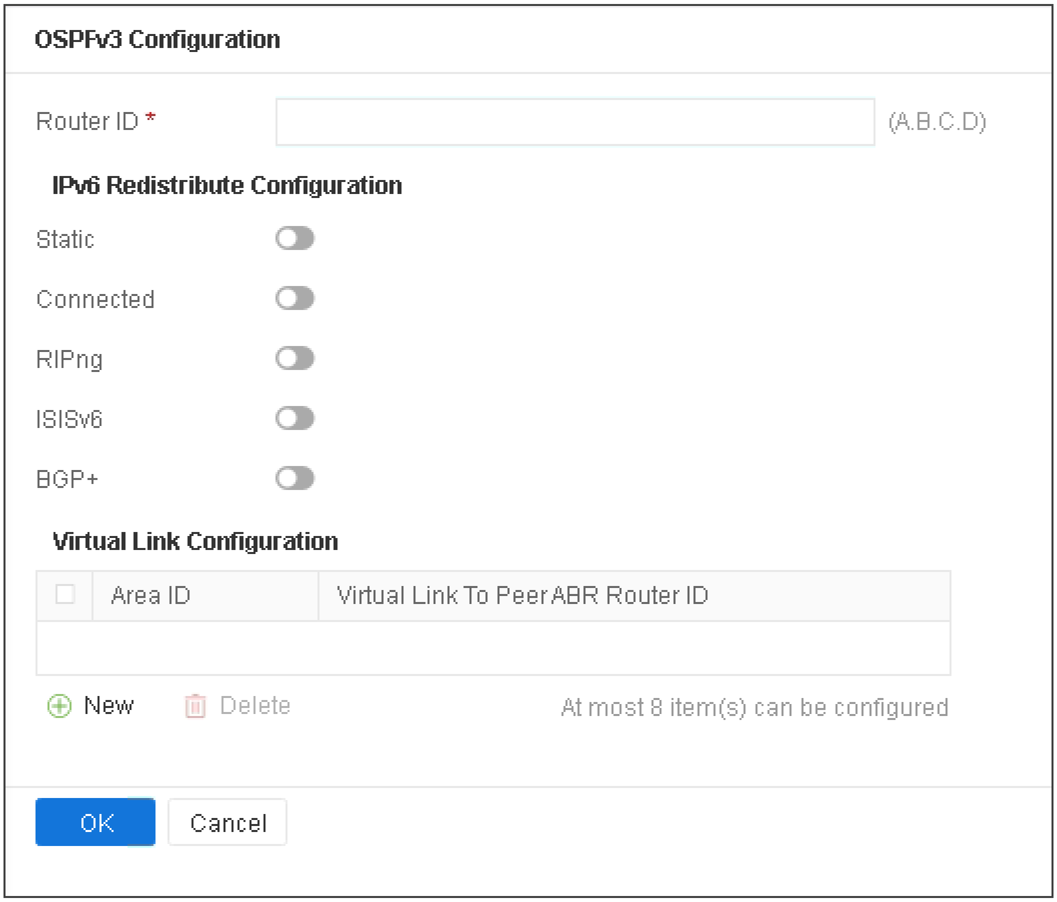
You can configure the OSPFv3 protocol for each VRouter respectively.

Creating OSPFv3

To create the OSPFv3 process, take the following steps:

1. Select **Network** > **Routing** > **OSPFv3**.
2. Select a VR from the **Virtual Router** drop-down list.

3. Click **New** to open the **OSPFv3 Configuration** page.



OSPFv3 Configuration

Router ID * (A.B.C.D)

IPv6 Redistribute Configuration

Static

Connected

RIPng

ISISv6

BGP+

Virtual Link Configuration

□	Area ID	Virtual Link To Peer ABR Router ID

In this page, configure as follows:

Option	Description
Router ID	Specifies the router ID of the router running the OSPFv3. The router ID is the unique identifier of an router in the OSPFv3 domain. The router ID should be in the format of IP address.
IPv6 Redistribute Configuration	
Static	Click the **Enable** button to introduce the static route protocol into the OSPFv3 route and redis-

Option	Description
	tribute.
Connected	Click the **Enable** button to introduce the connected route protocol into the OSPFv3 route and redistribute.
RIPng	Click the **Enable** button to introduce the RIPng route protocol into the OSPFv3 route and redistribute.
ISISv6	Click the **Enable** button to introduce the ISISv6 route protocol into the OSPFv3 route and redistribute.
BGP+	Click the **Enable** button to introduce the BGP+ route protocol into the OSPFv3 route and redistribute.
Virtual Link Configuration	
Area ID	Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
Virtual Link To Peer ABR Router ID	Virtual link always connect two area border routers. You need to configure the router ID of the area border routers respectively.

4. Expand **Interface Configuration**, configure the following.

Option	Description
Edit	Select the check box of an interface from the Interface page, and click **Edit** to open the Interface Configuration page.
Interface Area Configuration	Configure the area and instance where the OSPFv3 interface belongs to. • **Area ID**: Specifies the area ID that the interface belongs to. The area ID is in form of a 32-bit digital number, or an IP address. • **Interface**： Specifies the interface running OSPFv3. • **Instance ID**： Specifies the instance ID that the interface belongs to. To establish the neighbor relationship, interfaces must belong to the same instance. The value ranges from 0 to 255. The default value is 0.

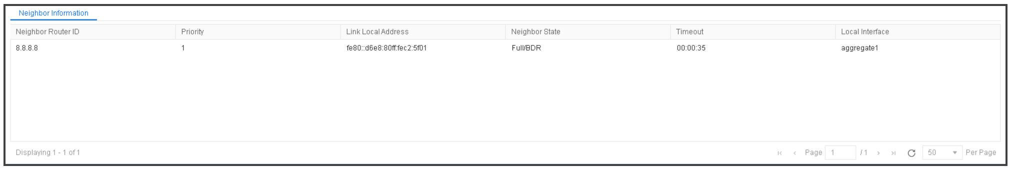
5. Click **OK** to save the configurations and the created OSPFv3 process will be displayed in the list.

Viewing Neighbor Information

To view the neighbor information of the created OSPFv3 process, take the following steps:

1. Select **Network** > **Routing** > **OSPFv3**.

2. Select an OSPFv3 process and the neighbor information will be displayed below.



Neighbor Router ID	Priority	Link Local Address	Neighbor State	Timeout	Local Interface
8.8.8.8	1	fe80::d6e8:80ff:fec2:5f01	Full/BDR	00:00:35	aggregate1

Displaying 1 - 1 of 1

- Neighbor Router ID: Displays the ID of neighbor router.

- Priority: Displays the router priority. The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and send the received link information.

- Link Local Address: Displays the Link-local of the neighbor router interface.

- Neighbor State: Displays the OSPFv3 neighbor state. The OSPFv3 neighbor state includes 8 types: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full. The Full state includes Full/DR and Full/BDR.

- Timeout: Displays the neighbor timeout, which is the difference between dead time and hello transmission interval. The unit is second. If the OSPFv3 doesn't receive the Hello packets from neighbor, the neighbor ship cannot be established continually.

- Local Interface: Displays the interface sending the Hello packets to the neighbor router.

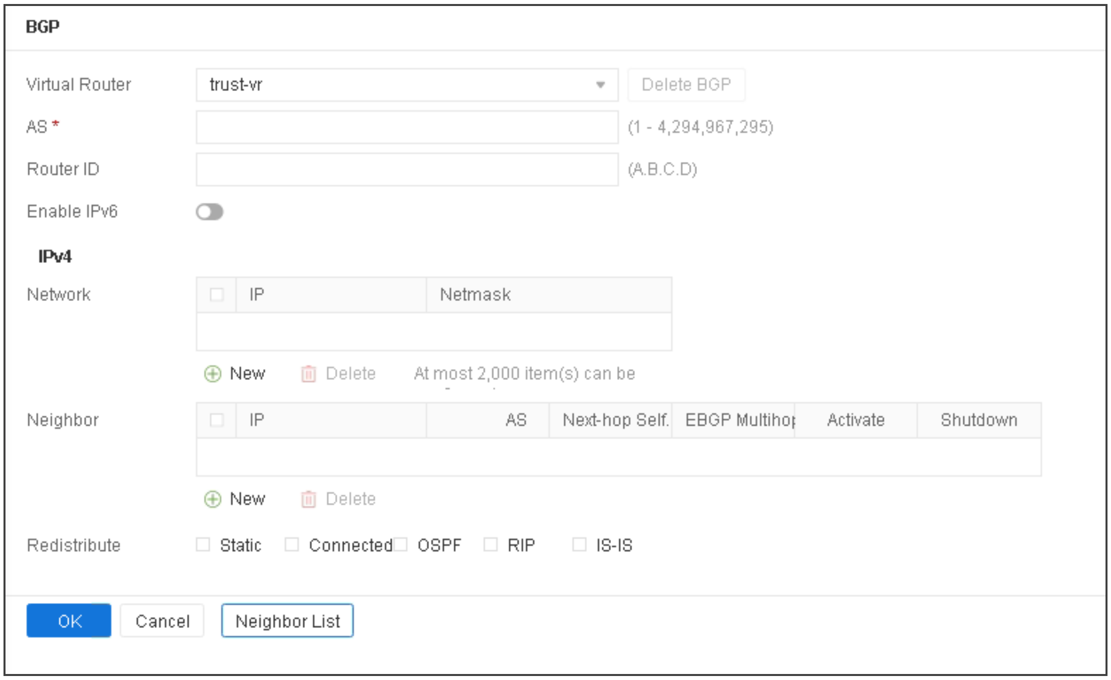
Configuring BGP

BGP, the abbreviation for Border Gateway Protocol, is a routing that is used to exchange dynamic routing information among the autonomous systems. Autonomous system means the router and network group under the control of a management institute. When BGP runs within the autonomous system, it is called IBGP (Internal Border Gateway Protocol); when BGP runs between the autonomous systems, it is called EBGP (External Border Gateway Protocol).

Basic

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.



BGP

Virtual Router: trust-vr

4. Configure the options as follows:

Option	Description
AS	Specifies the number of Autonomous System, ranging from 1 to 4294967295.
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, 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.
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 the ⊕ button, and specify the

Option	Description
	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 the 🗑 button.
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 the ⊕ button and enter the information as follows. • **IP**: Enter the IP address of the specified neighbor router. • **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.

Option	Description
	• **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 information will be cleared. By default, the function is disabled. • Delete: To delete the specified neighbor router, click the 🗑 button.
Redistribute	When IPv4 is supported, the following routing protocols can be introduced and redistributed. • **Static**: Select the check box to introduce the static route protocol into the BGP route

Option	Description
	and redistribute. • **Connected**: Select the check box to introduce the connected route protocol into the BGP route and redistribute. • **OSPF**: Select the check box to introduce the OSPF route protocol into the BGP route and redistribute. • **RIP**: Select the check box to introduce the RIP route protocol into the BGP route and redistribute. • **IS-IS**: Select the check box to introduce the IS-IS route protocol into the BGP route and redistribute. When IPv6 is supported, the following routing protocols can be introduced and redistributed. • **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

Option	Description
	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.

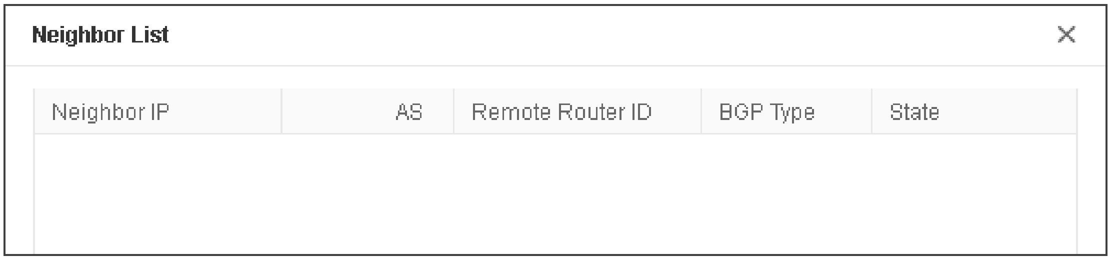
5. Click **OK** to save the configurations. The newly-created nwighbor router will be displayed in the list.

Neighbor List

To view the created neighbor router, take the following steps:

1. Select **Network** > **Routing** > **BGP**.

2. In the **Neighbor List** page, view the information of neighbor routers.



Neighbor List

Neighbor IP	AS	Remote Router ID	BGP Type	State

- **Neighbor IP**: Displays the IP address of the neighbor router.

- **AS**: Displays the autonomous system number of the neighbor router.

- **Remote Router ID**: When the neighbor router is connected with the peer router, the router ID of the peer router will be displayed.
- **BGP Type**: Displays the running type of BGP. When BGP runs between different AS, it displays as EBGP; when BGP runs within an AS, it displays as IBGP.
- **State**: Displays the status of connection between the neighbor router and its router, including Idle, Connect, Active, OpenSent, OpenConfirm and Established.

Delete BGP

To delete the BGP process, take the following steps:

1. Select **Network** > **Routing** > **BGP**.
2. Click the **Delete BGP** button, and all BGP configurations will be deleted.

Chapter 7 Authentication

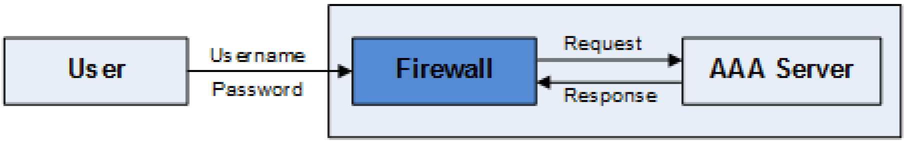
Authentication is one of the key features for a security product. When a security product enables authentication, the users and hosts can be denied or allowed to access certain networks.

From a user's point of view, authentication is divided into the following categories:

- If you are a user from an internal network who wants to access the Internet, you can use:
  - "Web Authentication" on Page 302
  - "1Single Sign-On" on Page 314
  - "PKI" on Page 362
- If you are a user from the Internet who wants to visit an internal network (usually with VPN), you can use:
  - "SSL VPN" on Page 410
  - "IPSec VPN" on Page 372 (IPSec VPN (with radius server)+Xauth)
  - "L2TP VPN" on Page 523 (L2TP over IPsec VPN)

Authentication Process

A user uses his/her terminal to connect to the firewall. The firewall calls the user data from the AAA server to check the user's identity.



- User (authentication applicant): The applicant initiates an authentication request, and enters his/her username and password to prove his/her identity.

- Authentication system (i.e. the firewall in this case):The firewall receives the username and password and sends the request to the AAA server. It is an agent between the applicant and the AAA server.

- "AAA Server" on Page 589: This server stores user information like the username and password, etc. When the AAA server receives a legitimate request, it will check if the applicant has the right to the user network services and send back the decision. For more information, refer to "AAA Server" on Page 589. AAA server has the following four types:

  - Local server
  - Radius server
  - LDAP server
  - AD server
  - TACACS+server

Web Authentication

After the Web authentication (WebAuth) is configured, when you open a browser to access the Internet, the page will redirect to the WebAuth login page. According to different authentication modes, you need to provide corresponded authentication information. With the successful Web authentication, system will allocate the role for IP address according to the policy configuration, which provides a role-based access control method.

Web authentication means you will be prompted to check the identity on the authentication page. It includes the following four modes:

- Password Authentication: Using username and password during the Web authentication.
- SMS Authentication: Using SMS during the Web authentication. In the login page, you need to enter the mobile number and the received SMS verification code. If the SMS verification code is correct, you can pass the authentication.
- NTLM Authentication: System obtains the login user information of the local PC terminal automatically, and then verifies the identity of the user. For more configurations, see NTLM Authentication.

Notes: NTLM authentication mode only supports the Active Directory servers deployed in Windows Server 2008 or older versions.

Enabling the WebAuth

To enable the Web authentication, take the following steps:

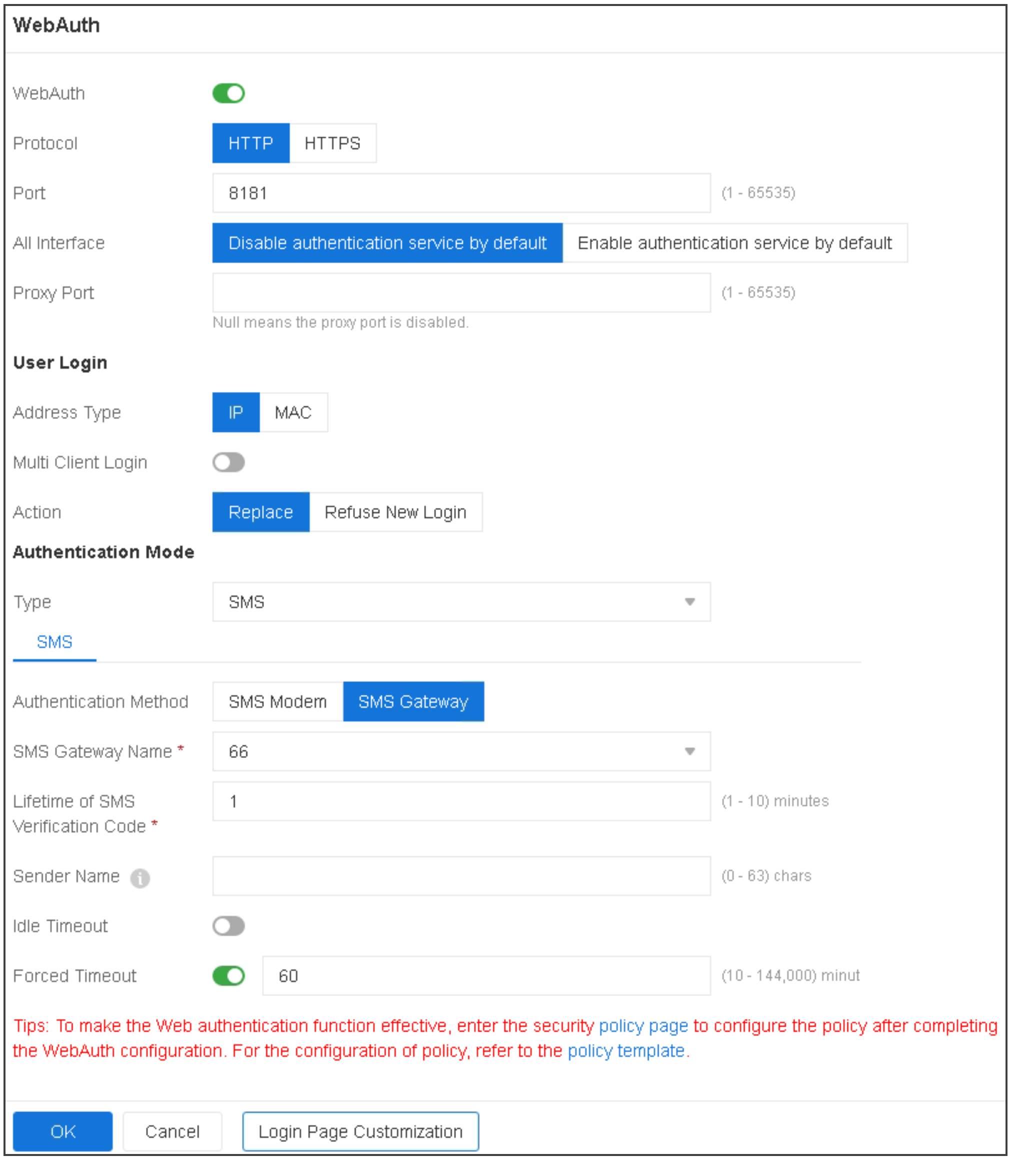
1. Click **Network** > **WebAuth** > **WebAuth**.
2. Select the **Enable** check box of **WebAuth** to enable the WebAuth function.

Configuring Basic Parameters for WebAuth

The basic parameters are applicable to all WebAuth polices.

To configure WebAuth basic parameters, take the following steps:

1. Click **Network > WebAuth > WebAuth**,click the **Enable** button.



WebAuth

WebAuth: on

Protocol: HTTP | HTTPS

Port: 8181 (1 - 65535)

All Interface: Disable authentication service by default | Enable authentication service by default

Proxy Port: (1 - 65535)

Null means the proxy port is disabled.

User Login

Address Type: IP | MAC

Multi Client Login: off

Action: Replace | Refuse New Login

Authentication Mode

Type: SMS

SMS

Authentication Method: SMS Modem | SMS Gateway

SMS Gateway Name *: 66

Lifetime of SMS Verification Code *: 1 (1 - 10) minutes

Sender Name: (0 - 63) chars

Idle Timeout: off

Forced Timeout: on 60 (10 - 144,000) minut

Tips: To make the Web authentication function effective, enter the security policy page to configure the policy after completing the WebAuth configuration. For the configuration of policy, refer to the policy template.

2. In the Basic Configuration tab, configure the following options

Basic Configuration	
HTTP	Select the HTTP authentication methods. Port: Specifies the HTTP protocol transmission port number of the authentication server. The range is 1 to 65535, and the default value is 8181.
HTTPS	Select the HTTPS authentication methods. HTTPS is encrypted, and can avoid information leakage. Port: Specify the HTTPS protocol transmission port number of the authentication server. The range is 1 to 65535, and the default value is 44433. Trust Domain: Specifies the HTTPS trust domain. This domain is previously created in PKI and has imported international CA certified certificate.
All Interface	After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. You can specify the Webauth global default configuration of all interfaces, including **Disable authentication service by default** and **Enable authentication service by default**. For more information about configuring the WebAuth of interface, see "Creating a PPPoE Interface" on Page 81.
Proxy Port	Specifies the port number for HTTPS, HTTPS and SSO proxy server. The port number applies to all. If it changes in any page, the other mode will also use the new port. The range is 1 to 65535.
User Login	

Basic Configuration	
Address Type	Specifies IP address or MAC address as the address type of authentication user. By default, the address type of authentication user is IP address **Note**: When the MAC is specified as the address type of authentication user, the device needs to be deployed in the same Layer 2 network environment with the client. Otherwise, system will fail to get the MAC address of the client or get an incorrect MAC address.
Multiple Login	If you disable the multiple login, one account cannot login if it has already logged in elsewhere. You can click **Replace** to kick out the registered user or you can click **Refuse New Login** to prevent the same user from logging in again. If you enable multiple login, more than one clients can login with the same account. But you can still set up the maximum number of clients using one account.
Authentication Mode	
Password: Specifies the password authentication mode as the authentication mode.	
Idle Timeout	If there is no traffic during a specified time period after the successful authentication, system will disconnect the connection. By default, system will not disconnect the connection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value

Basic Configuration	
	into the text box. Clear the check box to disable the idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check box to disable the forced timeout function.
Heartbeat Timeout	When authentication is successful, the system will automatically refresh the login page before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time, you will log off from the system at the smaller value. Select the **Heartbeat Timeout** check box to enable the heartbeat timeout function, and type the heartbeat timeout value into the text box. Clear the check box to disable the heartbeat timeout function.
Re-Auth Interval	System can re-authenticate a user after a successful authentication. By default, the re-authentication function is inactive. Select the **Re-Auth Interval** check box to enable the re-auth function, and type the re-auth interval into the text box. Clear the check box to disable the re-auth function.
Redirect URL	The redirect URL function redirects the client to the specified URL after successful authentication. You need to turn off the pop-up blocker of your web browser to ensure this function can work properly.

Basic Configuration	
	Notes: - You can specify the username and password in the URL address. When the specified redirect URL is the application system page with the authentication needed in the intranet, you do not need the repeat authentication and can access the application system. The corresponding keywords are $USER, $PWD, or $HASHPWD. Generally, you can select one keyword between $PWD and $HASHPWD. The formart of the URL is "URL" +"user-name=$USER&password=$PWD". - When entering the redirect URL in CLI, add double quotations to the URL address if the URL address contains question mark. For example, "http://192.10.5.201/oa/-login.-do?user-name-

Basic Configuration	
	=$USER&password=$HASHPWD"
SMS: Specifies the SMS authentication mode as the authentication mode.	
Authentication Method	Select the method to send authentication SMS, SMS Modem or SMS Gateway.
Lifetime of SMS Verification Code	When using SMS authentication, users need to use the SMS verification code received by the mobile phone, and the verification code will be invalid after the timeout value reaches. After the timeout value reaches, if the verification code is not used, you needs to get the new SMS verification code again. Specifies the verification code interval, the range is 1 to 10 minutes. The default value is 1 minute.
Sender Name	The user can specify a message sender name to display in the message content. Specifies the sender name. The range is 1 to 63. **Note**: 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.
Idle Timeout	If there is no traffic during a specified time period after the successful authentication, system will disconnect the connection. By default, system will not disconnect the con-

Basic Configuration	
	nection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value into the text box. Clear the check box to disable the idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check box to disable the forced timeout function.
NTLM: Specifies the NTLM authentication mode as the authentication mode.	
Idle Timeout	If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, the system will not disconnect the connection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value into the text box. Clear the check box to disable the idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check

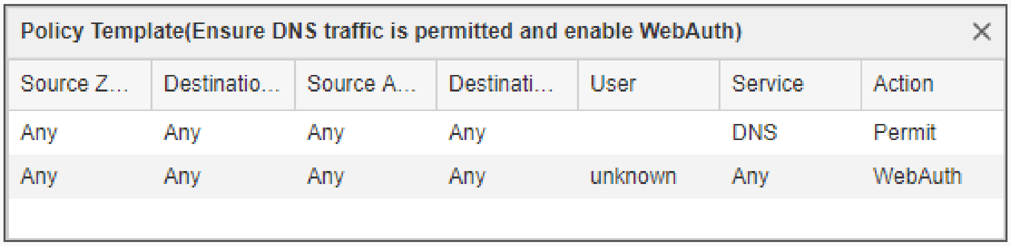
Basic Configuration	
	box to disable the forced timeout function.
When NTLM Fails	It will define the next action when user fails to pass SSO login. Select **Use Password Mode**, and the next step is to use password authentication to continue authentication. Select **No Action**, and the users will fail to login in.
Password/ SMS: Specifies the password authentication or the SMS authentication as the authentication mode.	
Password	Click the **Password** tab, and configure the related parameters for password authentication . For description of options, see "Password" section.
SMS	Click the **SMS** tab, and configure the related parameters for SMS authentication . For description of options, see "SMS" section.
SMS: Specifies the SMS authentication mode.	
SMS	Click the **SMS** tab, and configure the related parameters for SMS authentication . For description of options, see "SMS" section.

3. Click **Apply**.

Notes:

- If the WebAuth success page is closed, you can log out not only by timeout, but also by visiting the WebAuth status page (displaying online users, online times and logout button). You can visit it through "http (https):// IP-Address: Port-Number". In the URL, IP-Address refers to the IP address of the WebAuth interface, and Port-Number refers to HTTP/HTTPS port. By default, the HTTP port is 8181, the HTTPS port is 44433. The WebAuth status page will be invalid if there are no online users on the client or the WebAuth is disabled.

- After basic configurations, you should create two policy rules in "Security Policy" on Page 768 to make WebAuth effective, and then adjust the priority of the two policies to the highest. The WebAuth policies need to be configured according to the following policy template:



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

Source Z...	Destinatio...	Source A...	Destinati...	User	Service	Action
Any	Any	Any	Any		DNS	Permit
Any	Any	Any	Any	unknown	Any	WebAuth

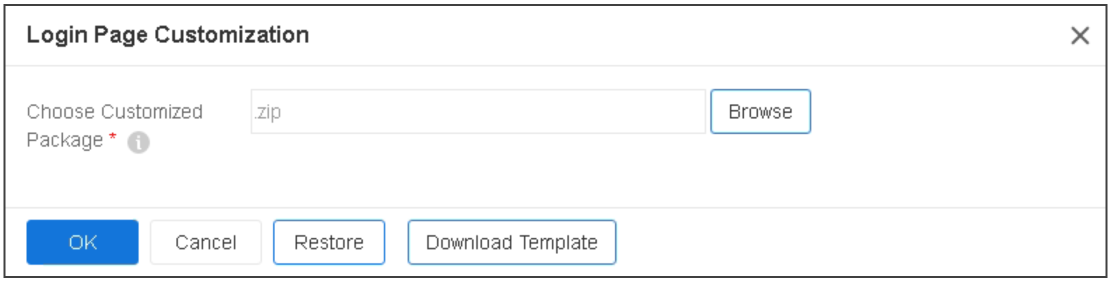
- After WebAuth is configured, the users who matched the WebAuth policy are recommended to input the correct username and password, and then the users can access the network. System takes actions to avoid illegal users from getting usernames and passwords by brute-force. If one fails to log in through the same host three times in two minutes, that host will be blocked for 2 minutes.

Customizing WebAuth Page

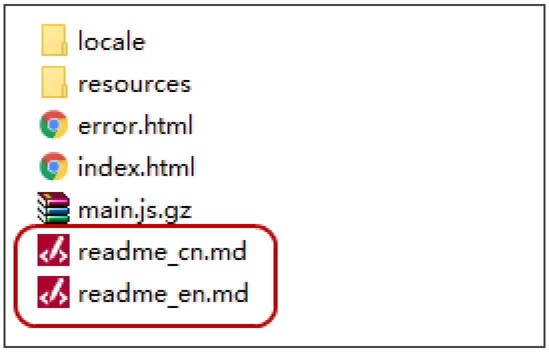
The WebAuth page is the redirected page when an authenticated user opens the browser. By default, you need to enter the username and password in the WebAuth page. You can also select the SMS authentication mode .

1. Click **Network > WebAuth > WebAuth**.

2. Click **Login Page Customization** tab, and click **Download Template** to download the zip file "webauth" of the default WebAuth login page, and then unzip the file.



3. Open the source file and modify the content(including style, picture, etc.)according to the requirements. For more detailed information, see the file of **readme_cn.md** or **readme_en.md**.



4. Compress the modified file and click **Upload** to upload the zip file to system.

Notes:

- After upgrading the previous version to the 5.5R6 version, the WebAuth login page you already specified will be invalid and restored to the default page. You should re-download the template after the version upgrade and customize the login page.

  - After upgrading the system version, you should re-download the template, modify the source file, and then upload the custom page compression package. If the uploaded package version is not consistent with the current system version, the function of the custom login page will not be used normally.

- The zip file should comply with the following requirements: the file format should be zip; the maximum number of the file in the zip file is 50; the upper limit of the zip file is 1M; the zip file should contain "index.html" .

- System can only save one file of the default template page and the customized page. When you upload the new customized page file, the old file will be covered. You are suggested to back up the old file.

- If you want trigger WebAuth through HTTPS request, you need import the root certificate (certificate of the device) to the browser firstly. Triggering WebAuth through HTTPS requests depends on the feature of SSL proxy . If the devrice does not support the SSL proxy. Triggering WebAuth through HTTPS requests will not work and you can then trigger WebAuth through HTTP requests.

1Single Sign-On

When the user authenticates successfully for one time, system will obtain the user's authentication information. Then the user can access the Internet without authentication later.

SSO can be realized through three methods, which are independent from each other, and they all can achieve the "no-sign-on"(don't need to enter a user name and password) authentication.

Method	Installing Software or Script	Description
SSO Radius	---	After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.
AD Scripting	Logonscript.exe	This method needs to install the script "Logonscript.exe" on the AD server. The triggered script can also send user information to StoneOS. This method is recommended if you have a higher accuracy requirement for statistical monitoring and don't mind to change the AD server.
Radius Snooping	---	The Remote Authentication Dial-In Up Service (RADIUS) is a protocol

Method	Installing Software or Script	Description
		that is used for the communication between NAS and AAA server. The RADIUS packet monitoring function analyzes the RADIUS packets that are mirrored to the device and the device will automatically obtain the mappings between the usernames of the authenticated users and the IP addresses, which facilitates the logging module for providing the auditing function for the authenticated users.
AD Polling	---	After enabling the AD Polling function, system will regularly query the AD server to obtain the login user information and probe the terminal PC to verify whether the users are still online, thus getting correct authentication user information to achieve SSO. This method is recommended if you don't want to change the AD server.
SSO Monitor	---	After enabling SSO Monitor, StoneOS will build connection with the third-party authentication server

Method	Installing Software or Script	Description
		through SSO-Monitor protocol, as well as obtain user online status and information of the group that user belongs to. System will also update the mapping information between user name and IP in real time for online user.
AD Agent	AD Security Agent	This method needs to install AD Security Agent software on the AD server or other PCs in the domain. The software can send user information to StoneOS. This method is recommended if you don't want to change the AD server.
TS Agent	Hillstone Terminal Service Agent	This method needs to install and run Hillstone Terminal Service Agent in the Windows server. After the TS Agent is configured, when users log in the Windows server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of

Method	Installing Software or Script	Description
		traffic IPs, port ranges and users, and achieve the "no-sign-on" authentication.

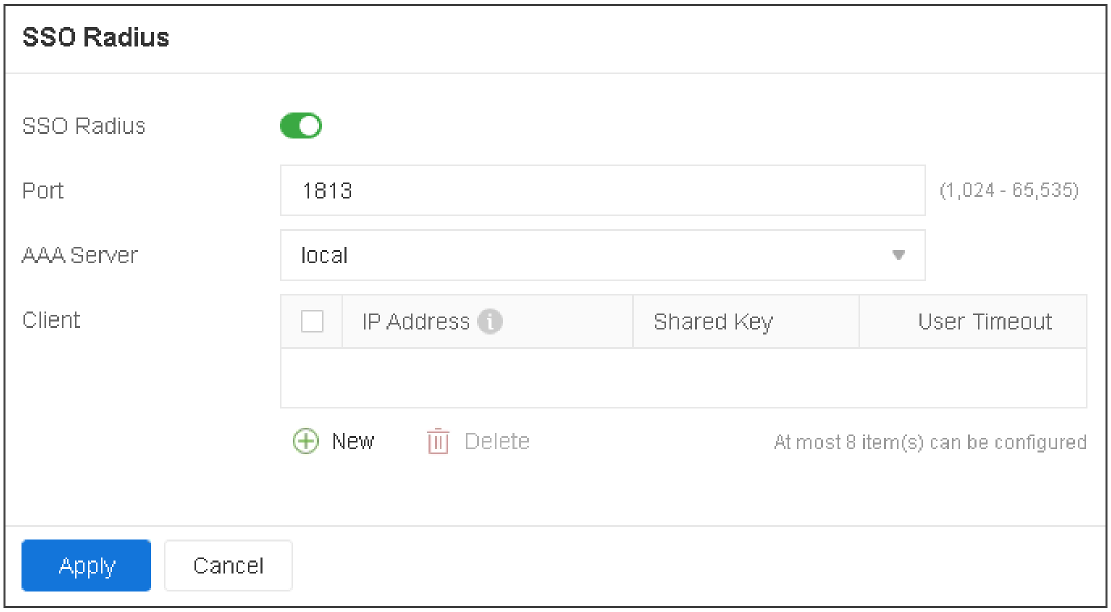
Enabling SSO Radius for SSO

After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.

To configure the SSO Radius function, take the following steps:

1. Click **Object >SSO Server >SSO Radius** and enter **SSO Radius** page. By default, SSO Radius is disabled.

2. Click the **Enable** button to enable the SSO Radius function.



SSO Radius

SSO Radius: enabled

Port: 1813 (1,024 - 65,535)

AAA Server: local

Client

□	IP Address	Shared Key	User Timeout

3. Specify the Port to receive Radius packets for StoneOS (Don' t configure port in non-root VSYS). The range is 1024 to 65535. The default port number is 1813.

4. 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.

5. Specify the IP Address, Shared Secret and Idle Interval of SSO Radius client which is allowed to access system. You can configure up to 8 clients.

   - IP Address: Specify the IPv4 address of SSO Radius client. If the IPv4 address is 0.0.0.0, it means that system receives the packets sent from any Radius client.

   - Shared Key: Specify the shared secret key of SSO Radius client. The range is 1 to 31 characters. System will verify the packet by the shared secret key, and parse the packet after verifying successfully. If system fails to verify the packet, the packet will be dropped. The packet can be verified successfully only when SSO Radius client is configured the same shared secret key with system or both of them aren't configured a shared secret key.

   - User Timeout(minute): Configure the idle interval for the authentication information of Radius packet in the device. If there’ s no update or delete packet of the user during the idle interval, the device will delete the user authentication information. The range is 0 to 1440 minutes. The default value is 30. 0 means the user authentication information will never timeout.

6. Click **Apply** button to save all the configurations.

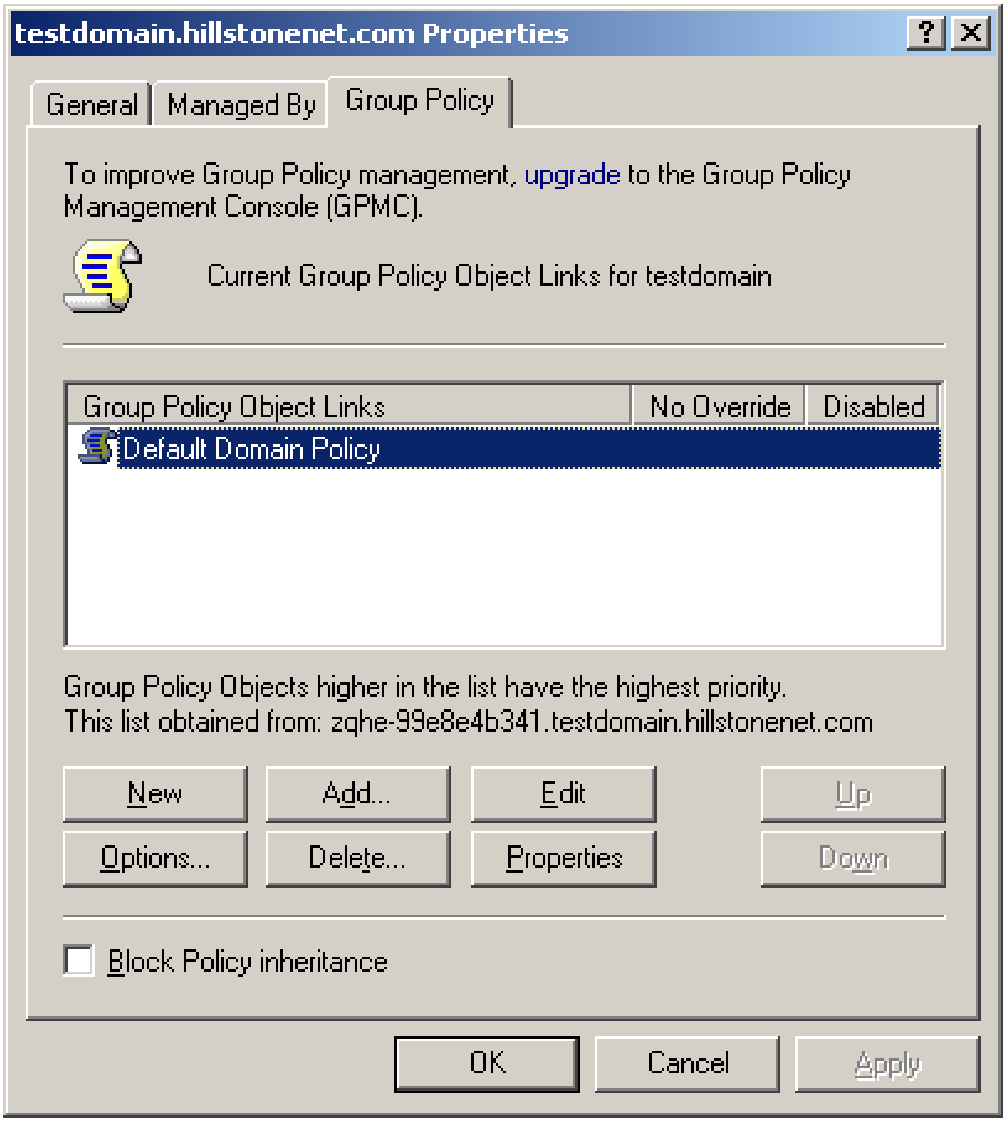
Using AD Scripting for SSO

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" , and save it in a directory where all domain 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.



testdomain.hillstonenet.com Properties

To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

Current Group Policy Object Links for testdomain

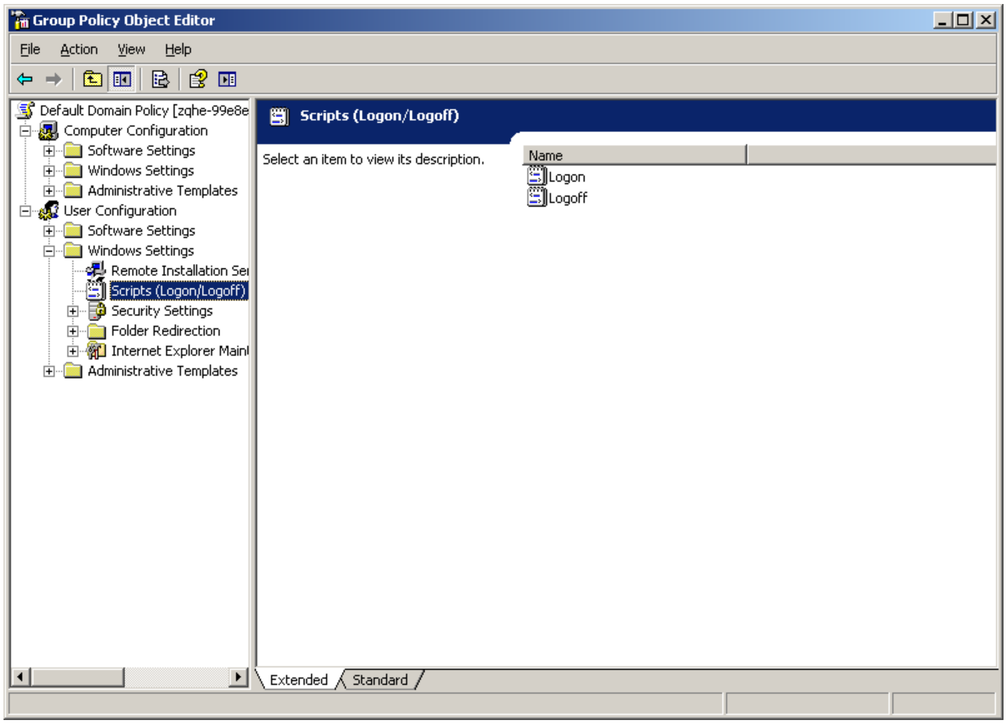
Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: zqhe-99e8e4b341.testdomain.hillstonenet.com

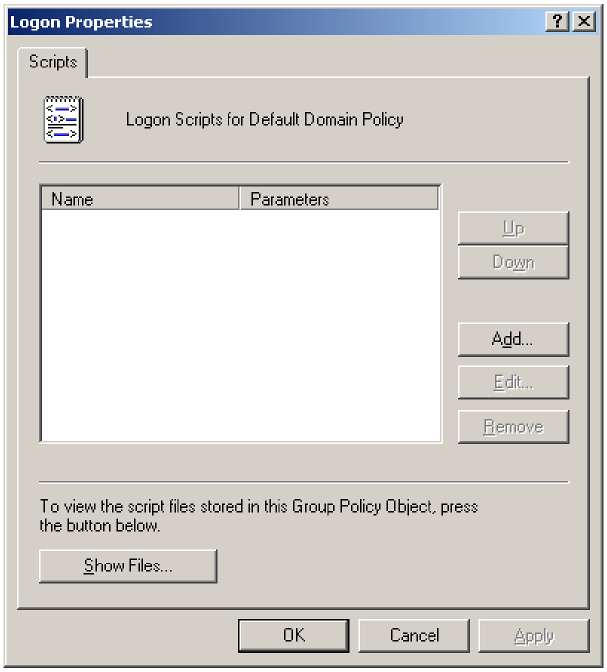
☐ Block Policy inheritance

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>**

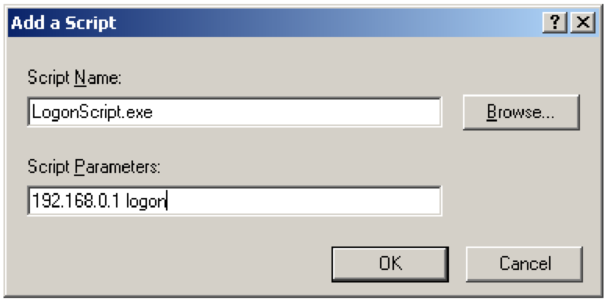
Script (Logon/Logout).



5. Double-click **Logon** on the right window, and click **Add** in the pop-up <logon properties> dialog box.


Logon Properties
Scripts
Logon Scripts for Default Domain Policy
Name
Parameters
Up
Down
Add...
Edit...
Remove
To view the script files stored in this Group Policy Object, press the button below.
Show Files...
OK
Cancel
Apply

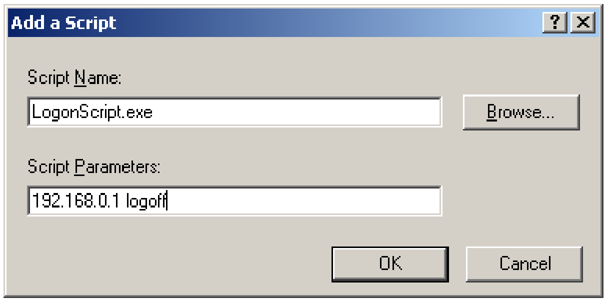
6. In the <Add a Script> dialog box, click **Browse** to select the logon script (logonscript.exe) for the Script Name; enter the authentication IP address of StoneOS and the text "logon" for the Script Parameters(the two parameters are separated by space). Then, click **OK**.



Script Name: LogonScript.exe

Script Parameters: 192.168.0.1 logon

7. Take the steps of 5-6 to configure the script for logging out, and enter the text "logoff" in the step 6.



Script Name: LogonScript.exe

Script Parameters: 192.168.0.1 logoff

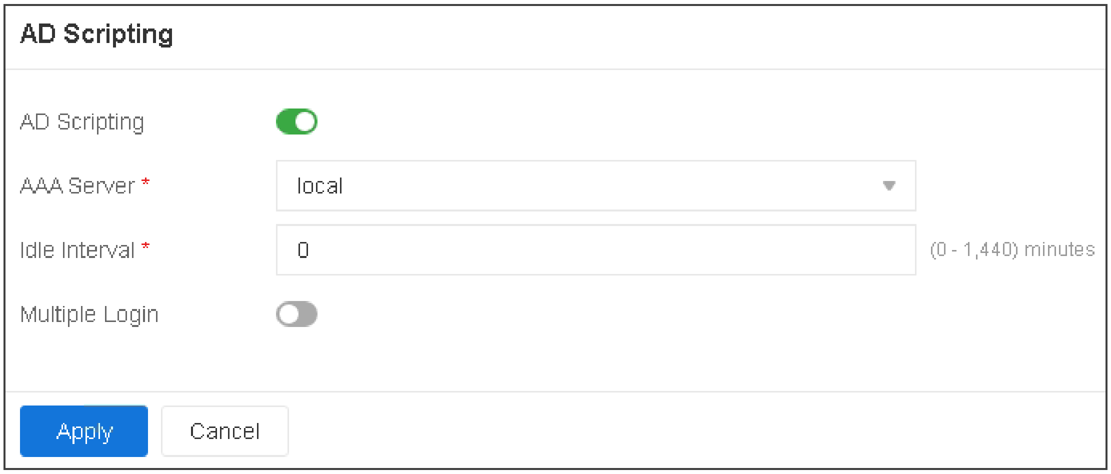
Notes: The directory of saving the script should be accessible to all domain users, otherwise, when a user who does not have privilege will not trigger the script when logs in or out.

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.



AD Scripting

AD Scripting

AAA Server * local

Idle Interval * 0 (0 - 1,440) minutes

Multiple Login

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.

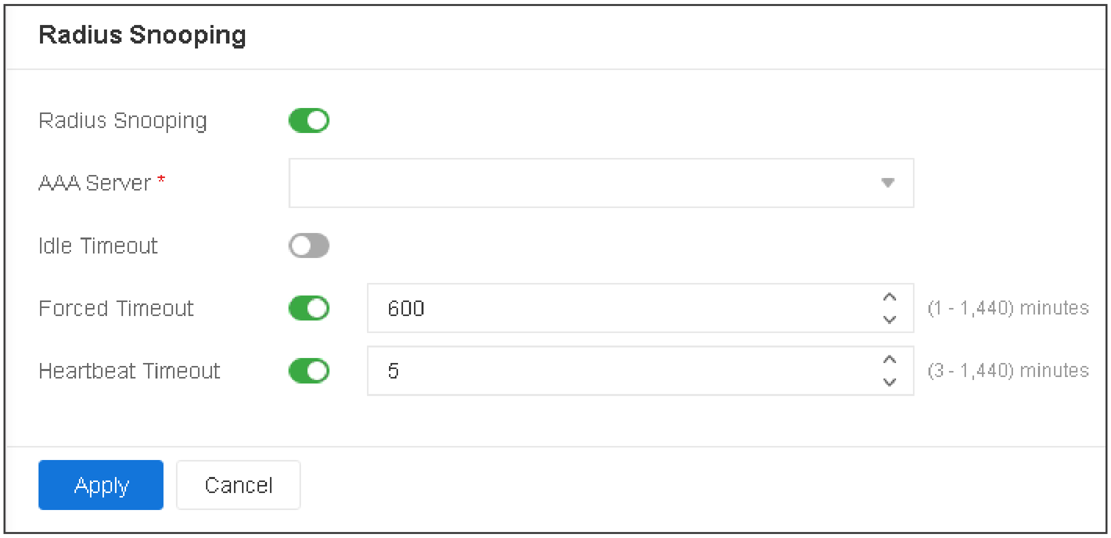
After completing the above two steps, the script can send the user information to StoneOS in real time. When users log in or out, the script will be triggered and send the user behavior to StoneOS.

Radius Snooping

The Remote Authentication Dial-In Up Service (RADIUS) is a protocol that is used for the communication between NAS and AAA server. The RADIUS packet monitoring function analyzes the RADIUS packets that are mirrored to the device and the device will automatically obtain the mappings between the usernames of the authenticated users and the IP addresses, which facilitates the logging module for providing the auditing function for the authenticated users.

To configure Radius Snooping, take the following steps:

1. Click **Object> SSO Server > Radius Snooping** to enter the Radius Snooping page. The Radius Snooping function is disabled by default.



Radius Snooping

Radius Snooping

AAA Server *

Idle Timeout

Forced Timeout 600 (1 - 1,440) minutes

Heartbeat Timeout 5 (3 - 1,440) minutes

2. Select the **Enable** button of Radius Snooping 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 time. If the device does not receive the mirrored RADIUS packets within the specified time period, it will delete the mappings between the usernames and the IP addresses. The value ranges from 1 to 1440. By default, system will not delete the user authentication information if there is no traffic.

5. Specify the forced logout time. When the online time of a user exceeds the configured force timeout time, system will kick out the user and force the user to log out. The range is 0 (the function is disabled) to 1440 minutes, and the default value is 600 minutes.

6. Specify the heartbeat timeout value. When authentication is successful, the system will automatically reconfirm login information before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time, you will log off from the system at the smaller value. The value range is 3 to 1440 minutes. The default value is 5 minutes.

7. Click **Apply** to save the changes.

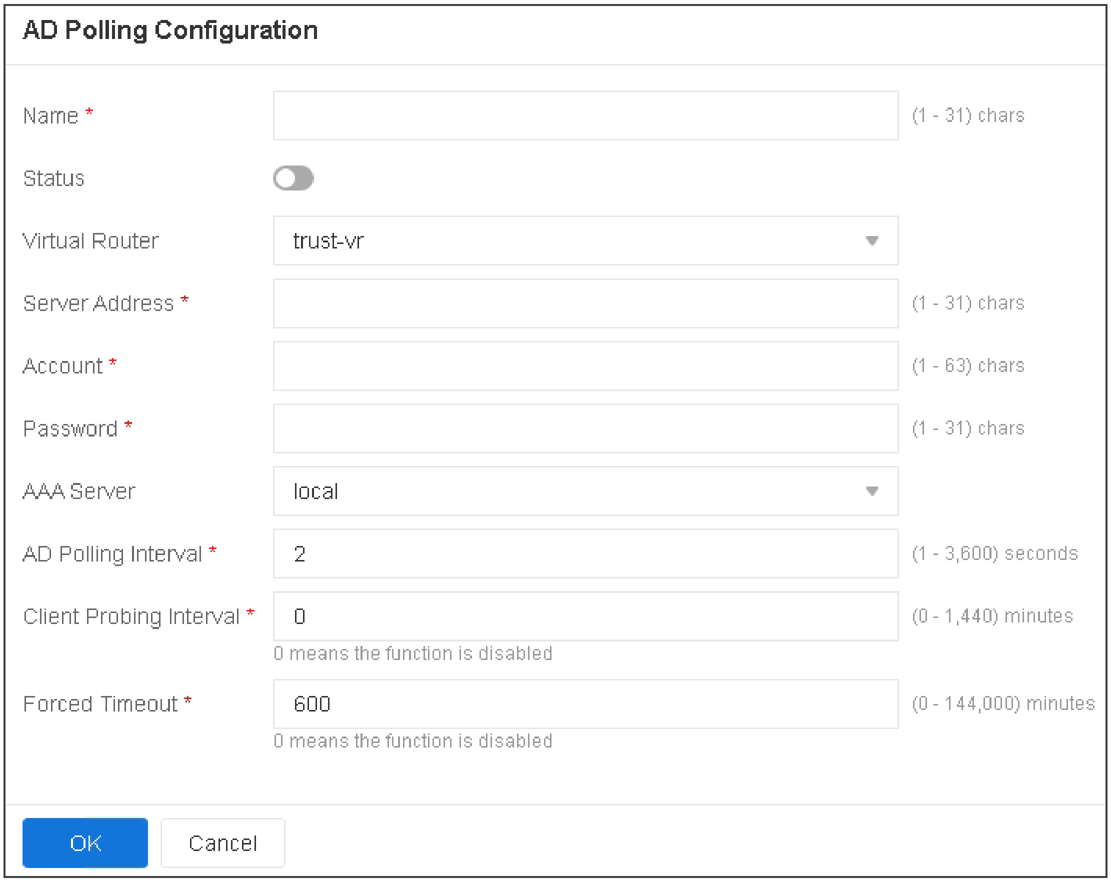
Using AD Polling for SSO

When the domain user logs in the AD server, the AD server will generate login logs. After enabling the AD Polling function, system will regularly query the AD server to obtain the user login information and probe the terminal PCs to verify whether the users are still online, thus getting correct authentication user information to achieve SSO.

Before using AD Polling for SSO, you should make sure that the Active Directory server is set up first. To use AD Polling for SSO, take the following steps:

1. Click **Object >SSO Client >AD Polling** to enter the AD Polling page.

2. Click the ⊕ New button on the upper left corner of the page, and the **AD Polling Configuration** dialog box pops up.



AD Polling Configuration

Name *		(1 - 31) chars
Status	○	
Virtual Router	trust-vr ▾	
Server Address *		(1 - 31) chars
Account *		(1 - 63) chars
Password *		(1 - 31) chars
AAA Server	local ▾	
AD Polling Interval *	2	(1 - 3,600) seconds
Client Probing Interval *	0 0 means the function is disabled	(0 - 1,440) minutes
Forced Timeout *	600 0 means the function is disabled	(0 - 144,000) minutes

In the AD Polling Configuration dialog box, configure the following:

Option	Description
Name	Specifies the name of the new AD Polling profile. The range is 1 to 31 characters
Status	Click **Enable** button to enable the AD Polling function. After enabling, system will query the AD server to obtain the user information and probe the terminal PC to verify

Option	Description
	whether the online users are online regularly. When queries for the first time, system will obtain the online user information on the AD server in the previous 8 hours . If fails to obtain the previous information, system will obtain the following online user information directly.
Server Address	Enter the IP address of authentication AD server in the domain. You can only select AD server. After specifying the authentication AD server, when the domain users log in the AD server, the AD server will generate the login logs. The range is 1 to 31 characters.
Virtual Router	Select the virtual router that the AD server belongs to in the drop-down list.
Account	Enter a domain user name to log in the AD server. The format is domain\username, and the range is 1 to 63 characters. The user is required to have permission to query security logs on the AD server, such as the user of Administrator whose privilege is Domain Admins on the AD server.
Password	Enter a password corresponding to the domain user name. The range is 1 to 31 characters.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 589. You are suggested to select the configured authentication AD server. After

Option	Description
	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,.
AD Polling Interval	Configure the interval for regular AD Polling probing. System will query the AD server to obtain the online user information at interval. The range is 1 to 3600 seconds, and the default value is 2 seconds. You are suggested to configure 2 to 5 seconds to ensure to obtain online user information in real time.
Client Probing Interval	Configure the interval for regular client probing. System will probe whether the user is still online through WMI at interval, and kick out the user if cannot be probed. The range is 0 to 1440 minutes, and the default value is 0 minute(the function is disabled). You are suggested to configure a larger probing interval to save the system performance, if you have low requirements for the offline users.
Force Timeout	Configure the forced logout time. When the user's online time exceeds the configured timeout time, system will kick out the user and force the user to log out. The range is 0（the function is disabled）to 144000 minutes, and the default value is 600 minutes.

3. Click **OK** button to finish the configuration of AD Polling.

Notes:

- When system is restarted or the configuration of AD Polling (except the account, password and force timeout) is modified, system will clear the existed user information and obtain the user information according to the new configuration.
- To realize the AD Polling function, you need to enable the WMI of the PC where the AD server is located and the terminal PC. By default, the WMI is enabled. To enable WMI, you need to enter the **Control Panel >Administrative Tools> Services** and enable the WMI performance adapter.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the RPC service and remote management should be enabled. By default, the RPC service and remote management is enabled. To enable the RPC service, you need to enter the **Control Panel >Administrative Tools> Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security> Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.

- To use the offline function, you should make sure that the time of the PC where the AD server is located and the terminal PCs is the same. To enable the function of Synchronize with an Internet time server, select **Control Panel > Clock, Language, and Region > Date and Time**, and the Date and Time dialog box pops up. Then, click **Internet Time** tab, and check **Synchronize with an Internet time server**.

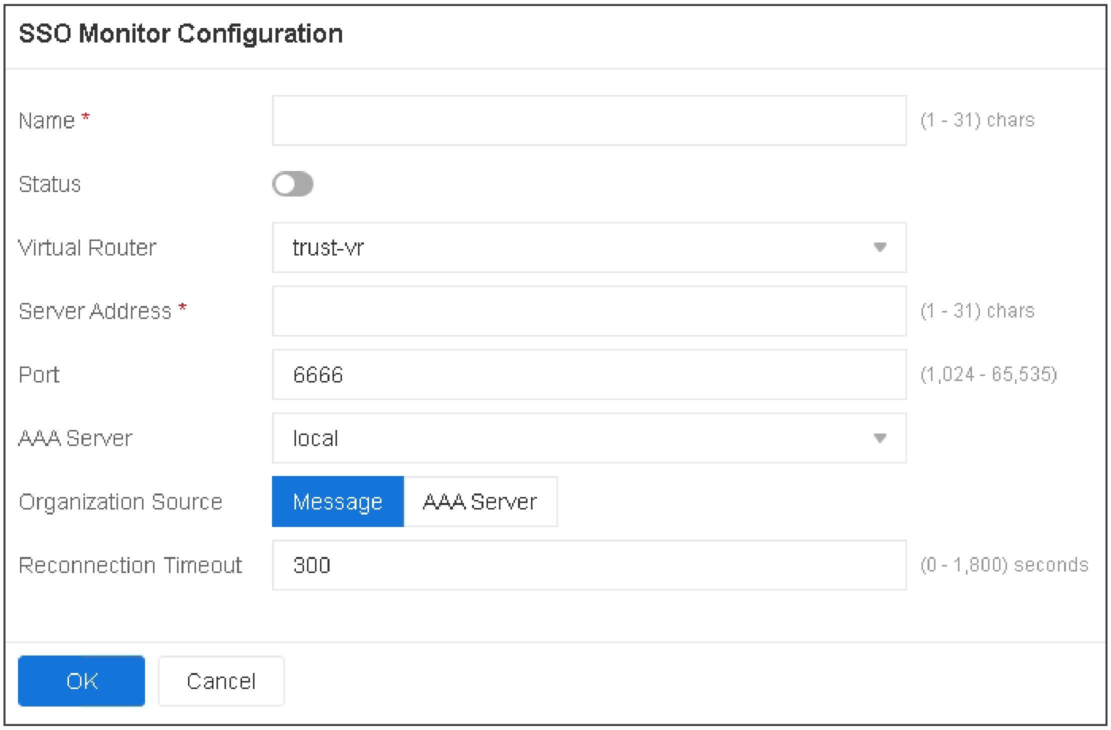
Using SSO Monitor for SSO

When user logs in through the third-party authentication server, the authentication status will be saved on the server. StoneOS will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of group that user belongs to.

To use SSO Monitor for SSO, take the following steps:

1. Click **Object >SSO Client > SSO Monitor** to enter **SSO Monitor** page.

2. Click the ⊕ New button and the **SSO Monitor Configuration** dialog box pops up.



SSO Monitor Configuration

Name * (1 - 31) chars

Status

Virtual Router: trust-vr

Server Address * (1 - 31) chars

Port: 6666 (1,024 - 65,535)

AAA Server: local

Organization Source: Message | AAA Server

Reconnection Timeout: 300 (0 - 1,800) seconds

In the SSO Monitor Configuration dialog box, configure the following:

Name	Specify the name of the new SSO Monitor. The range is 1 to 31 characters.
Status	Click **Enable** button to enable the SSO Monitor function. After enabling the function, system will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of group that user belongs to. The machine will generate authentication user according to the authentication information.

Server Address	Enter the IP address of the authentication server. The range is 1 to 31 characters. You can select the third-party custom authentication server which supports SSO-Monitor protocol. After specifying the authentication server, when user logs in the specified server, the server will save user’ s authentication information.
Virtual Router	Select the virtual router that the authentication server belongs to in the drop-down list.
Port	Specifies the port number of the third-party authentication server. System will obtain user information through the port number. The default number is 6666. The range is 1024 to 65535.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 589 for configuration method. 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.
Organization Source	Select the method to synchronize user organization structure with system, including Message and AAA Server. When Message is selected, StoneOS will use the user

	group of authentication information as the group that user belongs to. It's usually used in the scenario of the third-party authentication server saving user group. When AAA Server is selected, StoneOS will use the user organization structure of AAA server as the group that user belongs to. It's usually used in the scenario of the third-party authentication server being authenticated by AAA server and the user organization structure being saved in the AAA server.
Reconnection Timeout	Configure the reconnection timeout. When StoneOS disconnects with the third-party authentication server due to timeout, system will wait during the disconnection timeout. If system still fails to connect within the configured time, it will delete online users. The range is 0 to 1800 seconds. The default value is 300. 0 means the user authentication information will never timeout.

3. Click **OK** button to finish SSO Monitor configuration.

Notes: You can configure different numbers of SSO Monitor on different servers. When the configured number exceeds the limit, system will pops up the alarm information.

Using AD Agent Software for SSO

Before using AD Security Agent for SSO, make sure you have established your Active Directory server first. To use AD Security Agent for SSO, take the following steps:

Step 1: Installing and Running AD Security Agent on a PC or Server

AD Security Agent can be installed on an AD server or a PC in the domain. If you install the software on an AD server, the communication only includes "AD Security Agent →StoneOS"; If you install the software on a PC in the domain, the communication includes both process in the following table. The default protocol and port used in the communication are described as follows:

Communication direction		**AD Security Agent→AD Server**	**AD Security Agent→StoneOS**
Protocol		TCP	TCP
Port	StoneOS	---	6666
	AD Security Agent	1935、1984	6666
	AD Server	445	---

To install the AD Security Agent to an AD server or a PC in the domain, take the following steps:

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-adagent to download an AD Security Agent software, and copy it to a PC or a server in the domain.

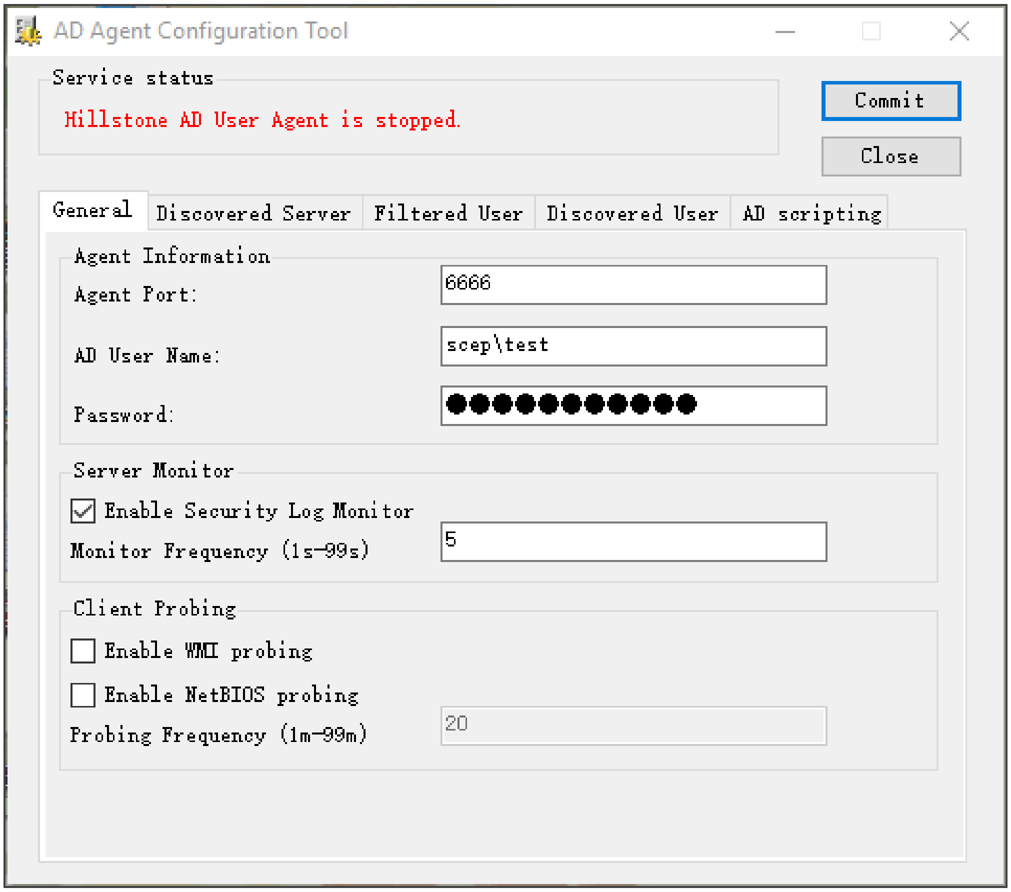
2. Double-click ADAgentSetup.exeto open it and follow the installation wizard to install it.

3. Start AD Security Agent through one of the two following methods:

   - Double-click the AD Agent Configuration Tool shortcut on the desktop.

   - Click **Start** menu, and select **All app > Hillstone AD Agent >AD Agent Configuration Tool**.

4. Click the <General> tab.



Service status

Hillstone AD User Agent is stopped.

Agent Information

Agent Port: 6666

AD User Name: scep\test

Password: ●●●●●●●●●●●●

Server Monitor

☑ Enable Security Log Monitor

Monitor Frequency (1s-99s) 5

Client Probing

□ Enable WMI probing

□ Enable NetBIOS probing

Probing Frequency (1m-99m) 20

On the <General> tab, configure these basic options.

Option	Description
Agent Port	Enter agent port number. AD Security Agent uses this port to communicate with StoneOS. The range is 1025 to 65535. The default value is 6666. This port must be the same with the configured monitoring port in StoneOS, otherwise, the AD Security Agent and StoneOS cannot communicate with each other.
AD User	Enter user name to log in the AD server. If AD Security

Option	Description
Name	Agent is running on the other PCs of the domain, this user should have high privilege to query event logs in AD server, such as the user of Administrator whose privilege is Domain Admins on AD server.
Password	Enter the password that matched with the user name. If the AD Security Agent is running on the device where the AD server is located, the user name and password can be empty.
Server Monitor	
Enable Security Log Monitor	Select to enable the function of monitoring event logs on AD Security Agent. The default query interval is 5 seconds. The function must be enabled if the AD Security Agent is required to query user information.
Monitor Frequency	Specifies the polling interval for querying the event logs on different AD servers. The default value is 5 seconds. When finishing the query of a AD server, the AD Security Agent will send the updated user information to system.
Client probing	
Enable WMI probing	Select the check box to enable WMI probing. • To enable WMI to probe the terminal PCs, the ter-

Option	Description
	minal PCs must open the RPC service and remote management. To enable the RPC service, you need to enter the **Control Panel >Administrative Tools> Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**. • WMI probing is an auxiliary method for security log monitor. which will probe all IPs in Discovered Users list. When the probed domain name does not match with the stored name, the stored name will be replaced by the probed name.
Probing Frequency	Specifies the interval of active probing action. The range is 1 to 99 minutes and the default value is 20 minutes.

5. On the <Discovered Server> tab, click **Auto Discover** to start automatic scanning the AD servers in the domain. Besides, you can click **Add** to input IP address of server to add it manually.
   When querying event logs in multiple AD servers, the query order is from top to bottom in the list.

6. On the <Filtered User> tab, type the user name need to be filtered into the **Filtered user** text box. Click **Add**, and the user will be displayed in the Filtered User list. You can configure 100 filtered users, which are not case sensitive.

7. Click the <Discovered User> tab to view the corresponding relationship between the user name and user address that has been detected.

   Tip: The user added into the Filtered User list will not be displayed in the Discovered User list.

8. On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe". (For introduction and installation of this script, refer to "Using AD Scripting for SSO" on Page 318）.

9. Click **Commit** to submit all settings and start AD Security Agent service in the mean time.

> **Notes:** After you have committed, AD Agent service will be running in the background all the time. If you want to modify settings, you can edit in the **AD Agent Configuration Tool** and click **Commit**. The new settings can take effect immediately.

Step 2: Configuring AD server for StoneOS

To ensure that the AD Security Agent can communicate with StoneOS, take the following steps to configure the AD server:

1. Click **Object >AAA Server** to enter the AAA server page.

2. Choose one of the following two methods to enter the Active Directory server configuration page:

   - Click the ⊕ New button on the upper left corner of the page, and choose **Active Directory Server** in the drop-down list.
   - Choose the configured AD server and click the ✎ Edit button on the upper left corner of the page.

3. For basic configuration of AD server, see Configuraing Active Directory Server.

   The following configurations should be matched with the AD Security Agent:

   - **Server Address**: Specify the IP address or domain name of AD server. It should be the same with the IP address of the device installed AD Security Agent.
   - **Security Agent**: Check the checkbox to enable SSO function, and the server can send the user online information to StoneOS.
     - **Agent Port**: Specify the monitoring port. StoneOS communicates with the AD Security Agent through this port. The range is 1025 to 65535. The default value is 6666. This port should be the same with the configured port of AD Security Agent, or system will fail to communicate with the AD Agent.
     - **Reconnection Timeout**: Specifies the timeout time of deleting user binding information. The range is 0 to 1800 seconds. The default value is 300 seconds. 0 means never timeout.
4. Click **OK** to finish the related configuration of AD server.

After completing the above two steps, when domain user logs in the AD server, the AD Security Agent will send the user name, address and online time to the StoneOS.

Using TS Agent for SSO

The configurations of TS Agent for SSO include:

- Configuring the TS Agent server: Installing and running Hillstone Terminal Service Agent in Windows server.
- Configuring the TS Agent client: Configuring TS Agent parameters in StoneOS.

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

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-tsagent to download a Hillstone Terminal Service Agent installation program, and copy it to the Windows server.

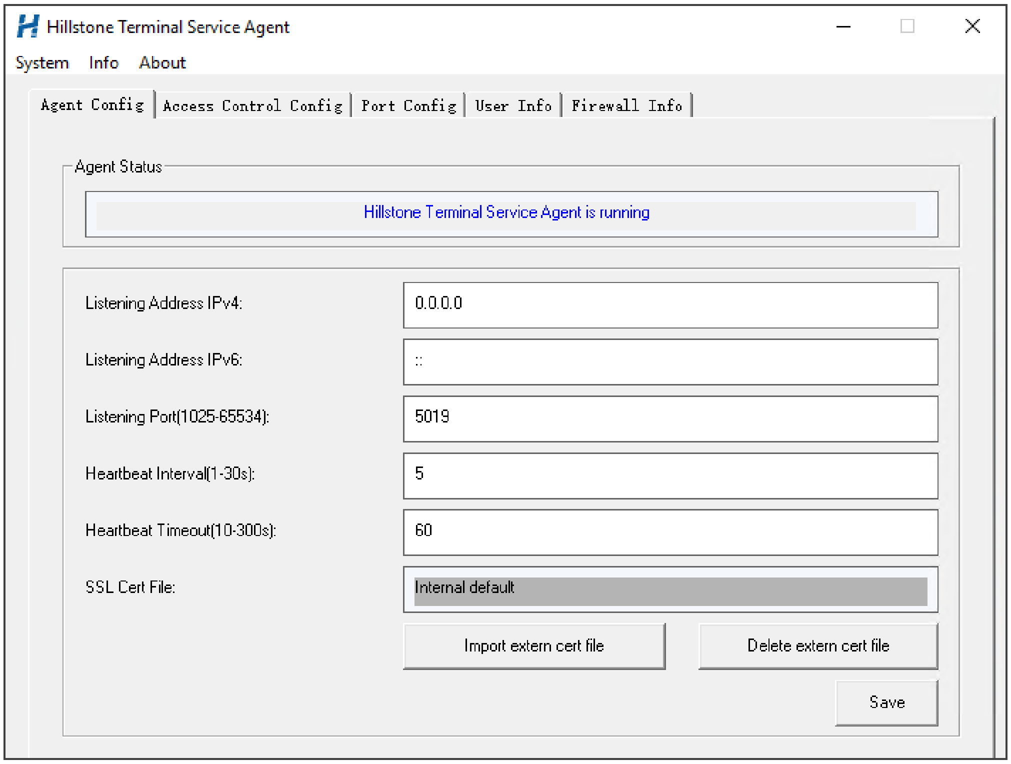
> **Notes:**
>
> - Windows Server 2008 R2, Windows Server 2016, and Windows Server 2019 are currently supported. Windows Server 2008 R2 Service Pack 1 and KB3033929 must be installed if Windows Server 2008 R2 is used.
> - It's recommended to close the anti-virus software before installing Hillstone Terminal Service Agent in Windows server.

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

3. Start Hillstone Terminal Service Agent through one of the two following methods:

   - Double-click the Hillstone Terminal Service Agent shortcut on the desktop.
   - Click **Start** menu, and select **All app** > **Hillstone Terminal Service Agent**.

4. Click the **Agent Config** tab.



Agent Status

Hillstone Terminal Service Agent is running

Listening Address IPv4: 0.0.0.0

Listening Address IPv6: ::

Listening Port(1025-65534): 5019

Heartbeat Interval(1-30s): 5

Heartbeat Timeout(10-300s): 60

SSL Cert File: Internal default

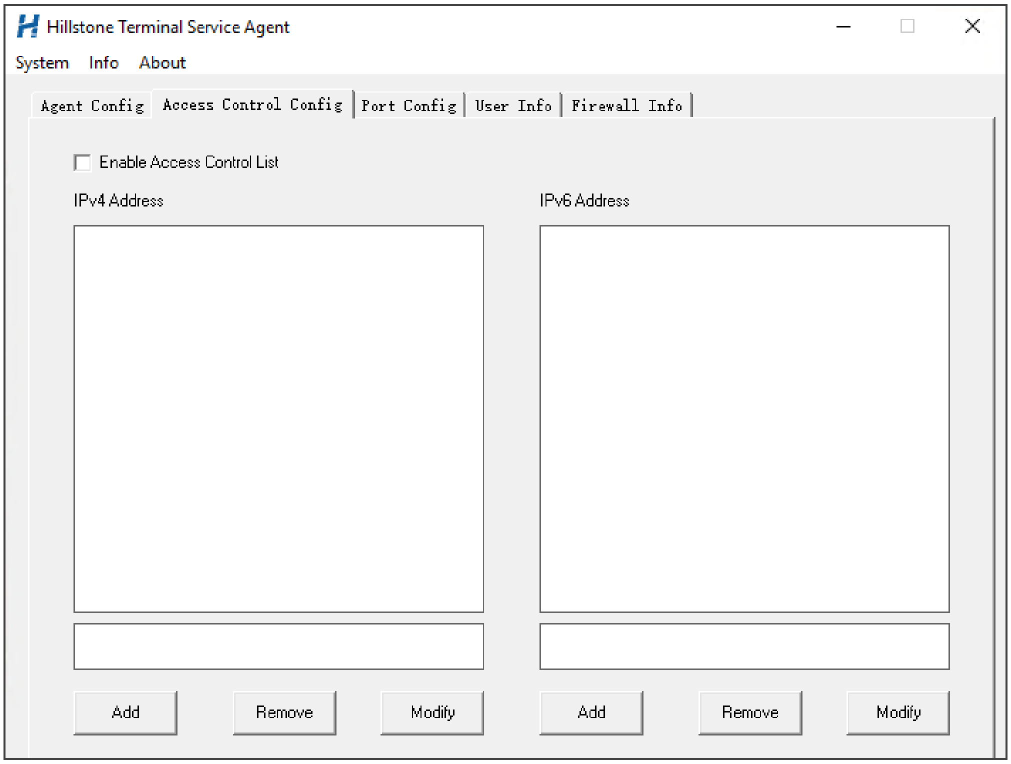
In the Agent Config tab, configure the following options.

Option	Description
Agent Status	Shows Hillstone Terminal Service Agent running status.
Listening Address IPv4	Specifies the IPv4 address to be listened. The default value is 0.0.0.0, which means listening all the IPv4 addresses.
Listening Address IPv6	Specifies the IPv6 address to be listened. The default value is ::, which means listening all the IPv6 addresses.
Listening Port	Specifies the listening port number. The range is 1025 to 65534. The default value is 5019. This port must be the

Option	Description
	same with the TS Agent server port configured in StoneOS, otherwise, the TS Agent client and the TS Agent server cannot communicate with each other.
Heartbeat Interval	Specifies the interval of sending heartbeat from the TS Agent client to the TS Agent server. The range is 1 to 30 seconds. The default value is 5 seconds.
Heartbeat Timeout	The TS Agent client will disconnect with the TS Agent server if it doesn't receive the heartbeat response from the server within the configured time. The range is 10 to 300 seconds. The default value is 60 seconds.
SSL Cert File	The TS Agent client synchronizes information with the TS Agent server through SSL connection. You can use the internal default SSL cert file or import external SSL cert file.
Import extern cert file	Click this button to import a new SSL cert file through the <Import extern cert file> dialog box. The encryption standard of the imported cert is PKCS12. The file is in .pfx format. To import the external cert file, you should create a PKI trust domain and import the CA certificate.
Delete extern cert file	Click this button to delete the external SSL cert file. After deletion, you need to restart the Hillstone Terminal Service Agent to make the default SSL cert file take effect. To restart the Hillstone Terminal Service Agent, click **Restart Agent Server** from the **System** drop-down

Option	Description
	menu.

5. Click the **Access Control Config** tab.

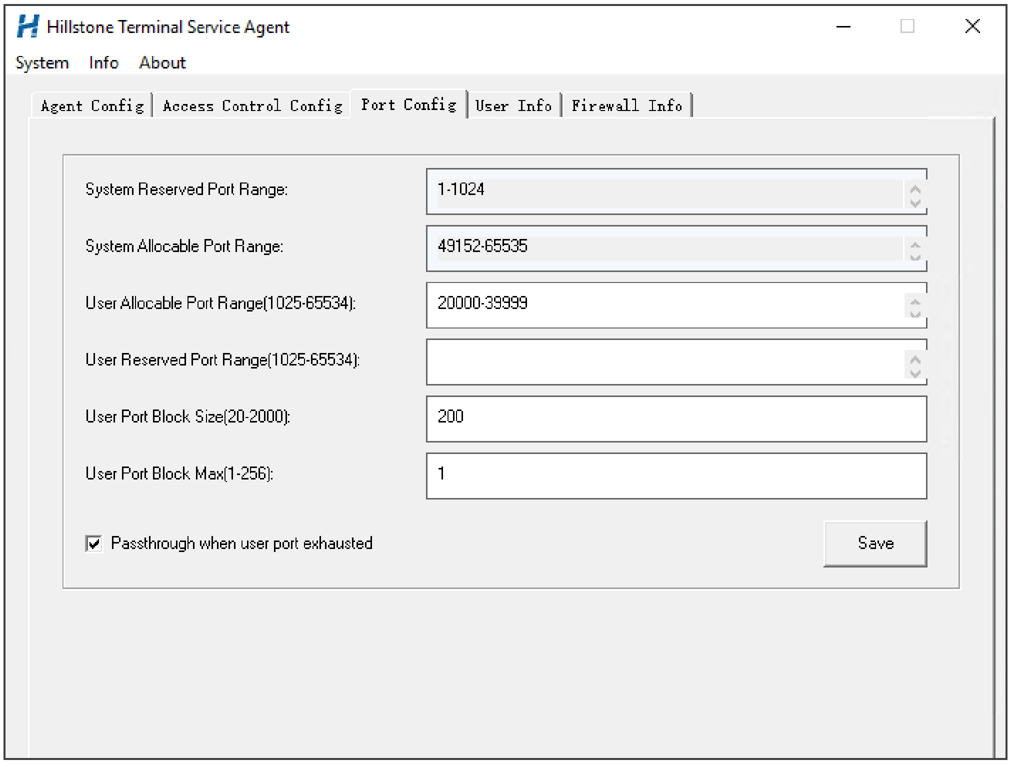


In the Access Control Config tab, configure the following options.

Option	Description
Enable Access Control List	Select this check box to check if the newly accessed IP address of StoneOS is in the IPv4 address list or IPv6 address list below, if not, the access will be denied. This function is disabled by default.
IPv4 Address	When the access control list feature is enabled, IPv4 addresses that are not in the list will be access denied.
IPv6	When the access control list feature is enabled, IPv6

Option	Description
Address	addresses that are not in the list will be access denied.
Add	Enter an IP address in the text box above **Add**, and clicks **Add** to add the IP address into the IPv4 addresses list or IPv6 addresses list.
Remove	Select an IP address in the IPv4 addresses list or IPv6 addresses list, and clicks **Remove** to delete the IP address from the list.
Modify	Select an IP address in the IPv4 addresses list or IPv6 addresses list, modifies the address in the text box below, and then clicks **Modify** to add the address into the list.

6. Click the **Port Config** tab.



System Reserved Port Range: 1-1024

System Allocable Port Range: 49152-65535

User Allocable Port Range(1025-65534): 20000-39999

User Reserved Port Range(1025-65534):

User Port Block Size(20-2000): 200

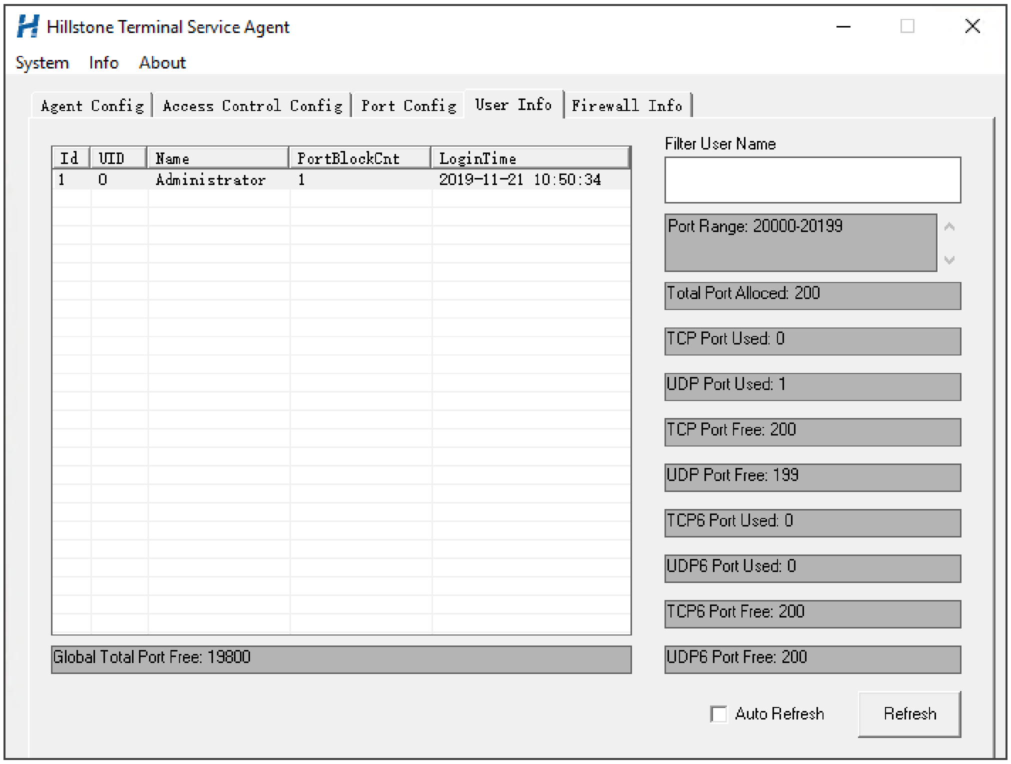
User Port Block Max(1-256): 1

☑ Passthrough when user port exhausted

In the Port Config tab, configure the following options.

Option	Description
System Reserved Port Range	The range of ports reserved by the system, which is read from the system registry and cannot be modified.
System Allocable Port Range	The range of ports used by the system to dynamically allocate to users, which is read from the system registry and cannot be modified.
User Allocable Port Range	The total port range that can be allocated to the users. The range is 1025 to 65534. The default value is from 20000 to 39999. Only one port range can be configured each time, the minimum range size is the specified user port block size, and the maximum range size is 40960.
User Reserved Port Range	The user-defined reserved range of ports. The range is 1025 to 65534. The default value is NULL. You can configure more than one port ranges with each separated by a comma, such as 2000-3000,3500,4000-4200.
User Port Block Size	The number of ports allocated to the user each time. The range is 20 to 2000. The default value is 200.
User Port Block Max	The maximum number of port blocks allocated to each user. The range is 1 to 256. The default value is 1.
Passthrough when user port exhausted	Select the check box, and when the ports in the User Allocable Port Range are exhausted, system will allocate ports to users from the System Allocable Port Range. This option is checked by default.

7. Click the **User info** tab.



Id	UID	Name	PortBlockCnt	LoginTime
1	0	Administrator	1	2019-11-21 10:50:34

Global Total Port Free: 19800

Port Range: 20000-20199

Total Port Alloced: 200

TCP Port Used: 0

UDP Port Used: 1

TCP Port Free: 200

UDP Port Free: 199

TCP6 Port Used: 0

UDP6 Port Used: 0

TCP6 Port Free: 200

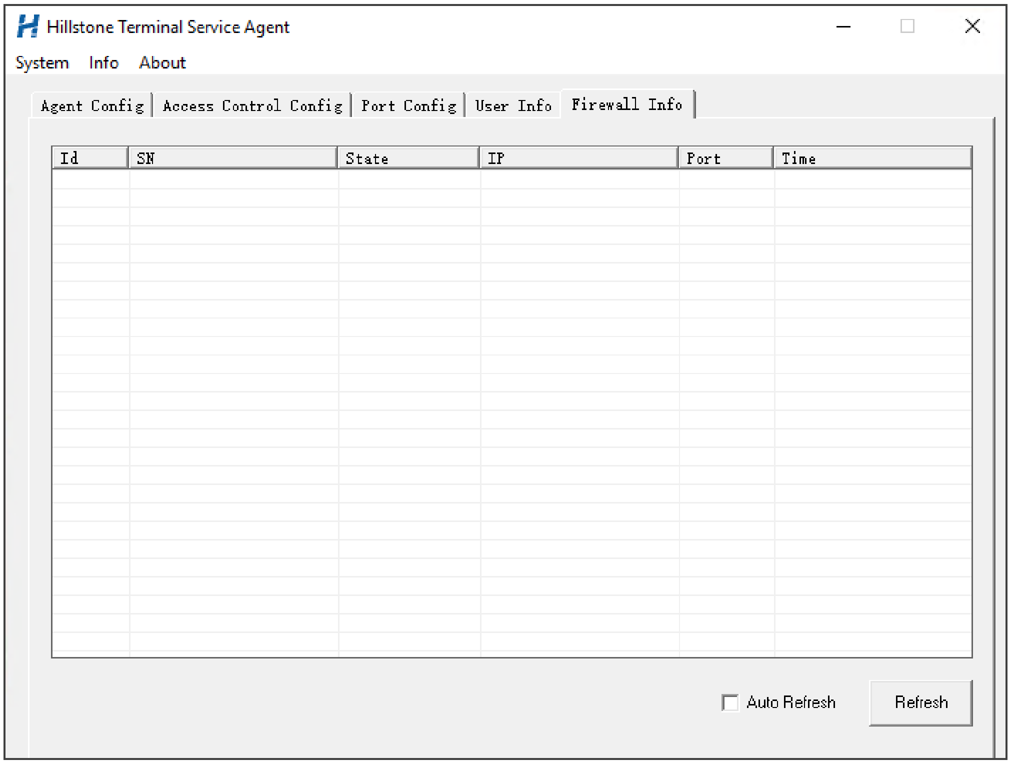
UDP6 Port Free: 200

In the User Info tab, view information about users.

Option	Description
User Info. List	Shows the login user information, including ID, UID, user name, port block count and the login time. When users log in the TS Agent server using remote desktop services, Hillstone Terminal Service Agent will record the user info. in the list. It can record up to 2000 users info.
Filter User Name	Enter the user name in the text field, and click Refresh, the searched user info. will be

Option	Description
	displayed in the user info. list. The user name is case sensitive.
Global Total Port Free	The number of remaining ports available to the users.
Port Range	The port range already allocated to login users. After the user logs off, the system reclaims all the port ranges allocated to this user.
Total Port Alloced	Total number of ports allocated to the login users.
TCP/UDP/TCP6/UDP6 Port Used	The number of ports already used by users. After the user's connection to the Internet is disconnected, the system reclaims the ports.
TCP/UDP/TCP6/UDP6 Port Free	The number of ports available to the user when creating a new connection
Auto Refresh	Check the check box, the port statistics will be refreshed every 5 seconds.

8. Click the **Firewall Info** tab.



In the Firewall Info tab, view information about StoneOS.

Option	Description
Connected Device List	Displays StoneOS info. currently connected to TS Agent server, including ID, SN, connected status, IP address, port and time.
Auto Refresh	Check the check box, information of the connected devices will be refreshed every 5 seconds.

9. Configure related functions and view information using the Menu bar.

Menu bar options introduction.

System	
Restart agent server	Click this option to restart Hillstone Terminal Service Agent. When Hillstone Terminal Service Agent is being restarted, **Agent Status** on the **Agent Config** tab shows "Hillstone Terminal Service Agent is stopped". When the restart is completed, **Agent Status** on the **Agent Config** tab shows "Hillstone Terminal Service Agent is running".
Info	
Open log info	Click this option, you can perform following operations in the pop-up Log Info dialog box: • Check one or more check boxes in the Info Select section, corresponding logs will be displayed in the log info list. • Select a log in the log info list, the complete info. of this log will be displayed in the text box at the lower left corner. • Type the character string in the **Filter** text box, and click **Refresh**, the log info. containing the character string will be displayed in the log info list. • Check the ID of one ore more logs in the log info. list, and click **Delete** to delete selected logs. • Click **Export to text** to export the log info. as a text file.

System	
	- Click and drag the scroll slider at the lower left corner left or right to scroll through the log info. page quickly. The text field below displays the total number of log information, the total number of log information pages, and the current page.
Log enable set	Click this option, and check or uncheck the type of log info., system will record or not record corresponding type of log info. The system record the Event, Alarm and Config log info. by default.
Open debug info	Click this option, the SMP (Service Process Module) debug info. file and the KM (Kernel Module) debug info. file display in the pop-up Debug Info dialog box. You can perform following operations: - Double-click the file name to open the file. - Select the file name, and press the Delete key on your keyboard to delete the file.
SPM debug level set	Click this option, and check the level of the SMP debug info., system will record the info. at or above the selected level. The default level is Event. You can view the SMP debug info. in the Debug Info dialog box: the SMP debug info. at Critical and Error level display in the SPM error section; the SMP debug info. at other levels display in the SPM info section.

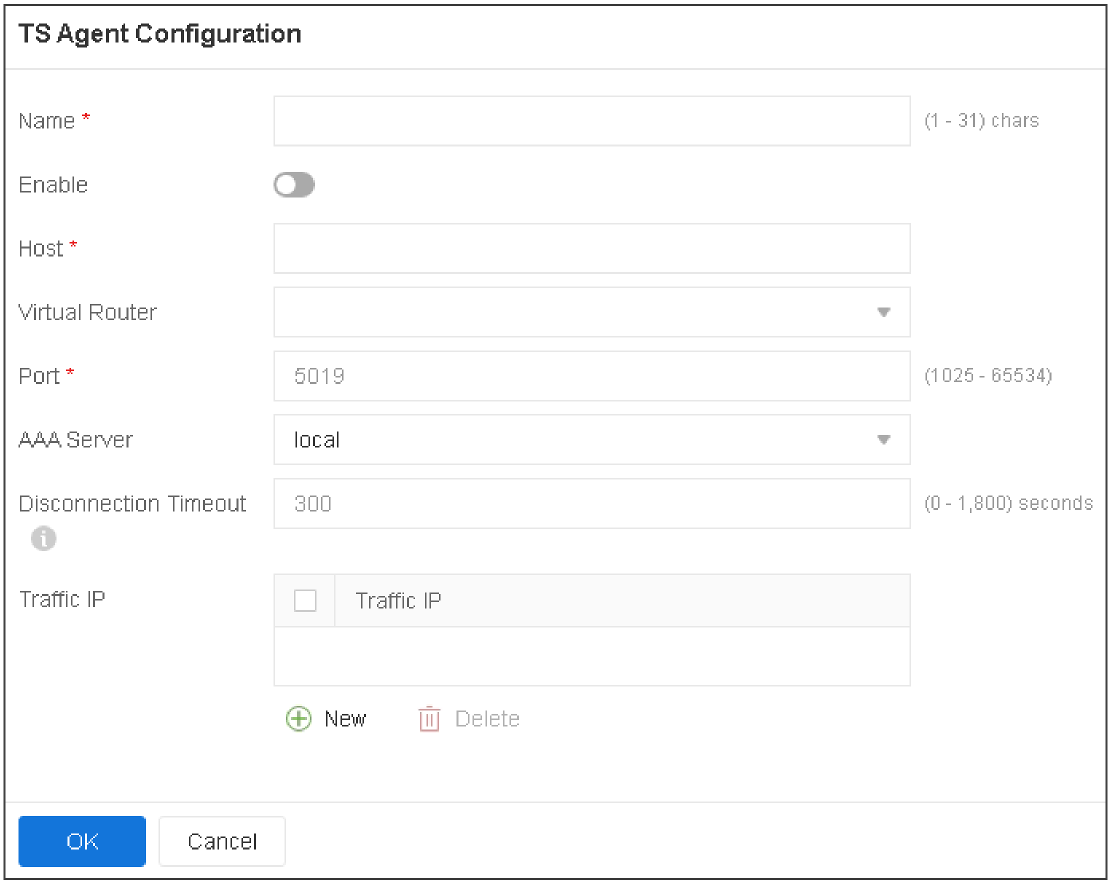
System	
KM debug level set	Click this option, and check the level of the KM debug info., system will record the info. at or above the selected level. The default level is Critical. You can view the KM debug info. in the Debug Info dialog box: the KM debug info. at Critical and Error level display in the KM error section; the KM debug info. at other levels display in the KM info section.
About	
About	Displays the information of version, copyright, etc.

Step 2: Configuring TS Agent parameters in StoneOS

To configure the TS Agent parameters in StoneOS, take the following steps:

1. Select **Object > SSO Client > TS Agent**.

2. Click **New**.



TS Agent Configuration

Name * (1 - 31) chars

Enable

Host *

Virtual Router

Port * 5019 (1025 - 65534)

AAA Server local

Disconnection Timeout 300 (0 - 1,800) seconds

Traffic IP □ Traffic IP

In the TS Agent Configuration dialog box, configure the following options.

Option	Description
Name	Specifies the name of the new TS Agent. The range is 1 to 31 characters.
Status	Select **Enable** button to enable the TS Agent function. After enabling, StoneOS will establish SSL connection with the TS Agent server, as well as obtain user and port range information. System will also update the mapping

Option	Description
	information of traffic IPs, port ranges and user names in real time for online users.
Host	Specifies the management address of the TS Agent server. It can be a domain name, or an IPv4 or IPv6 address.
Virtual Router	Select the virtual router that the TS Agent server belongs to in the drop-down list.
Port	Specifies the port number of the TS Agent server. The default number is 5019. The range is 1025 to 65534. This port number must be the same with the listening port number of Hillstone Terminal Service Agent, otherwise, the TS Agent client and the TS Agent server cannot communicate with each other.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 589. 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.
Disconnection Timeout	When StoneOS disconnects with the TS Agent server, system will wait during the disconnection timeout. If system still fails to connect within the configured time, it will delete online user. The range is 0 to 1800

Option	Description
	seconds. The default value is 300. 0 means delete the online user immediately.
Traffic IP	Specifies the traffic IP address, that is the network interface IP address of the TS Agent server. It cab be an IPv4 or IPv6 address. You can specify up to 4 IP addresses. Enter an IP address in the text field, and click **Add** to add the IP address into the Traffic IP list below. Check an IP address in the Traffic IP list, and click **Delete** to delete the IP address.

3. Click **OK** to finish the configuration of TS Agent.

After all the above configurations are finished, when users log in the TS Agent server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users.

802.1x

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

802.1X is a standard defined by IEEE for Port-based Network Access Control. It uses Layer-2 based authentication (protocol: EAPOL, Extensible Authentication Protocol over LAN) to verify the legality of the users accessing the network through LAN. Before authentication, the security device only allows the 802.1X message to pass through the port. After authentication, all of the normal traffic can pass through.

The AAA servers for 802.1x are Local server and Radius server. Other types of AAA servers like AD or LDAP server do not support 802.1x.

The authenticating process is the same with other authentication, please refer to "Chapter 7 Authentication" on Page 300.

Configuring 802.1x

A complete configuration for 802.1x authentication includes the following points:

- Prerequisite: Before configuration, you should already have the AAA server you want (only local or Radius server is supported for 802.1x). The AAA server has been added in the firewall system (refer to AAA server), and the interface or VLAN for authentication has been bound to a security zone (refer to interface or VLAN).
- Configuration key steps:
    1. Creating a 802.1x profile.
    2. Creating a security policy to allow accessing.
- In the user's PC, modify the network adapter's properties: If the computer is connected to the 802.1x interface, this computer should enable its authentication function on its LAN port (right click **LAN** and select **Properties**, in the prompt, under the <Authentication> tab, select **MD5-Challenge** or **Microsoft: Protected EAP (PEAP)**, and click **OK** to confirm.)

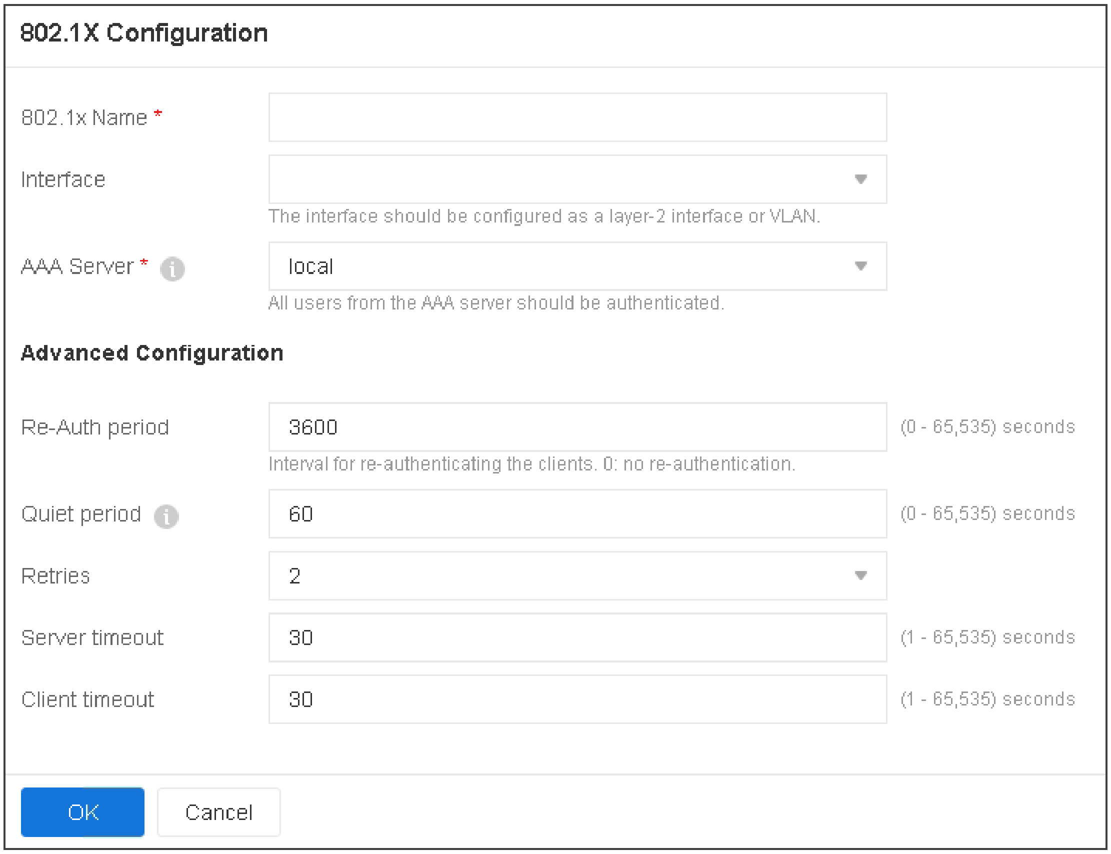
Notes: Early versions of Windows have enabled 802.1x by default, but Windows 7 and Window 8 do not have this feature enabled. To enable 802.1x, please search online for a solution that suits your system.

Creating 802.1x Profile

To create a 802.1x profile, take the following steps:

1. Select **Network > 802.1X > 802.1X**.

2. Click **New** and a prompt appears.



802.1X Configuration

802.1x Name *

Interface
The interface should be configured as a layer-2 interface or VLAN.

AAA Server * local
All users from the AAA server should be authenticated.

Advanced Configuration

Re-Auth period 3600 (0 - 65,535) seconds
Interval for re-authenticating the clients. 0: no re-authentication.

Quiet period 60 (0 - 65,535) seconds

Retries 2

Server timeout 30 (1 - 65,535) seconds

Client timeout 30 (1 - 65,535) seconds

Under the Basic tab and Advanced tab, enter values

Basic Configuration	
802.1x Name	Enter a name for the 802.1x profile
Interface	Select the interface for 802.1x authentication. It should be a Layer-2 interface or a VLAN interface.
AAA Server	Select the AAA server for 802.1x authentication. It should be a local server or a Radius server.
Access Mode	Select an access mode. If you select **Port** and one of the clients connected to 802.1x interface has passed authentication, all clients can access the Internet. If you select **MAC**, every client must pass authentication before using Internet.
Advanced Configuration	
Port authorized	If you select Auto, system will allow users who have successfully passed authentication to connect to network; If you select Force-unauthorized, system will disable the authorization of the port; as a result, no client can connect to the port, so there is no way to connect to the network.
Re-auth period	Enter a time period as the re-authentication time. After a user has successfully connected to the network, system will automatically re-auth the user's credentials. The range is from 0 to 65535 seconds. If the value is set to 0, this function is disabled.
Quiet period	If the authentication fails, it will take a moment before system can process the authenticating request from the

Basic Configuration	
	same client again. The range is 0 to 65535 seconds, and the default value is 60 seconds. If this value is set to 0, system will not wait, and will immediately process the request from the same client.
Retries	Specifies a number for retry times. If the authentication system does not receive any response from the client, system will try to require user's credentials again. When system has tried for the specified times, it will stop trying. The range is 1 to 10 times, and the default is 2 times.
Sever timeout	Specifies a server timeout value. The authenticator transmits the client's credentials to the authentication server. If the server does not answer the authenticator within a specified time, the authenticator will resend request to the authentication server. The range is 1 to 65535 seconds, the default value is 30 seconds.
Client timeout	When the authenticator sends a request to ask the client to submit his/her username, the client needs to respond within a specified period. If the client does not respond before timeout, system will resend the authentication request message. The range is 1 to 65535 seconds, and the default value is 30 seconds.

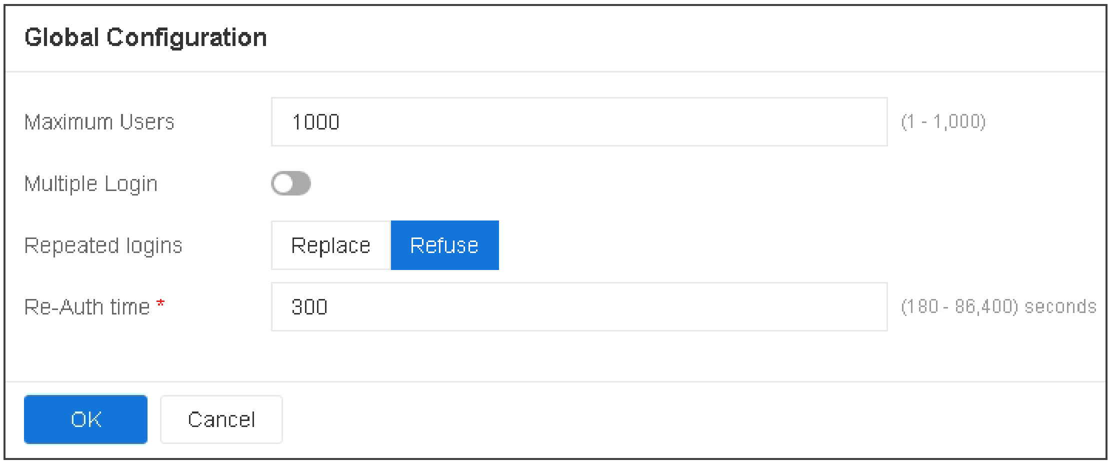
3. Click **OK**.

802.1x Global Configuration

Global parameters apply to all 802.1x profiles.

To configure global parameters, take the following steps:

1. Select **Network** > 802.1X > **Global Configuration**.



Global Configuration

Maximum Users: 1000 (1 - 1,000)

Multiple Login: ○

Repeated logins: Replace [✓ Refuse]

Re-Auth time *: 300 (180 - 86,400) seconds

In the Global Configuration dialog box, specify the parameters that will be applicable for all

802.1x profiles.

Option	Description
Maximum Users	The maximum user client number for a authentication port.
Multiple logins	You may choose to allow or disable one account to login from different clients. - **Disable**: If you select Disable, one account can only login from one client simultaneously. Then, when you want to kick off the old login user, you should select **Replace**; if you want to disallow new login user, select **Refuse**. - **Enable**: If you select **Enable**, different clients can use one account to login. If you do not limit the login client number, select **Unlimited**; if you want to set up a maximum login number, select **Max attempts** and enter a value for maximum user client number.
Re-Auth time	Specify a time for authentication timeout value. If the client does not respond within the timeout period, the client will be required to re-enter its credentials. The range is 180 to 86400 seconds, the default value is 300 seconds.

2. Click **OK**.

Viewing Online Users

To view which authenticated users are online:

1. Select **Network > 802.1X > Online user**.

2. The page will show all online users. You can set up filters to view results that match your conditions.

PKI

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over the Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over the Internet. A PKI system consists of Public Key Cryptography, CA (Certificate Authority), RA (Certificate Authority), Digital Certificate and related PKI storage library.

PKI terminology:

- Public Key Cryptography: A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is only known to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by the other key of the key pair.

- CA: A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.

- RA: The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.

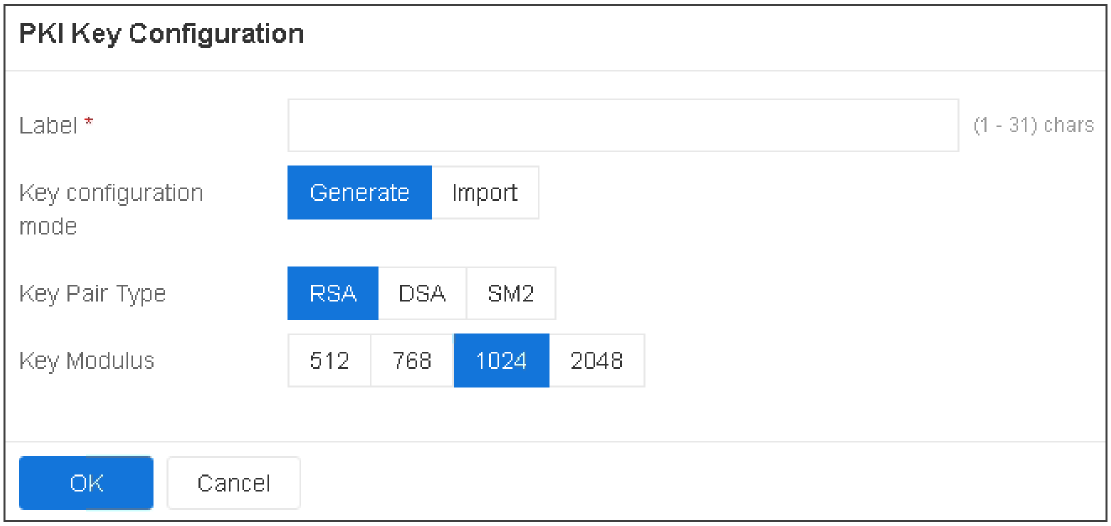
- CRL: Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

PKI is used in the following two situations:

- IKE VPN: PKI can be used by IKE VPN tunnel.
- HTTPS/SSH: PKI applies to the situation where a user accesses a Hillstone device over HTTPS or SSH.
- "Sandbox" on Page 971: Support the verification for the trust certification of PE files.

Creating a PKI Key

1. Select **System** > **PKI** > **Key**.
2. Click **New**.



PKI Key Configuration

Label * (1 - 31) chars

Key configuration mode: Generate | Import

Key Pair Type: RSA | DSA | SM2

Key Modulus: 512 | 768 | 1024 | 2048

OK | Cancel

In the PKI Key Configuration dialog, configure the following.

Option	Description
Label	Specifies the name of the PKI key. The name must be unique.
Key configuration mode	Specifies the generation mode of keys, which includes Generate and Import.

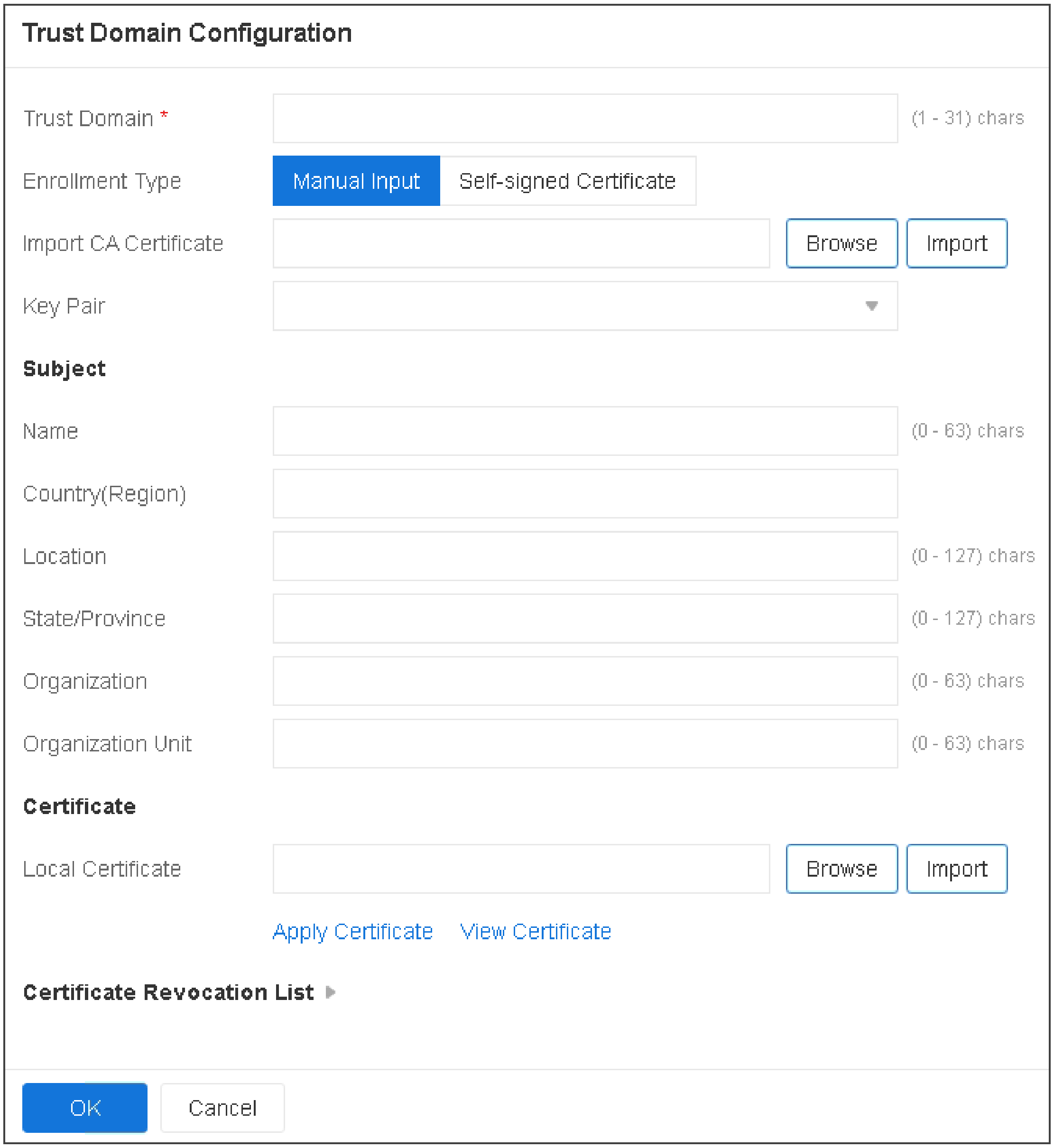
Option	Description
Key Pair Type	Specifies the type of key pair, either RSA, DSA or SM2.
Key Modulus	Specifies the modulus of the key pair. The modulus of RSA and DSA is 1024 (the default value), 2048, 512 or 768 bits, and the modulus of SM2 is 256.
Type	Specifies the type of key , including Encryption Key and Key Pair . • Encryption Key - Protects the signing key pair by digital envelope. If you select this option, you should specify the signing key pair when importing key. • Key Pair - If you select this option, you should specify the imported key pair type as RSA, DSA or SM2.
Import Key	Browse your local file system and import the key file.

3. Click **OK**.

Creating a Trust Domain

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

2. Click **New**.



Trust Domain Configuration

Trust Domain * (1 - 31) chars

Enrollment Type: Manual Input | Self-signed Certificate

Import CA Certificate

Key Pair

Subject

Name (0 - 63) chars

Country(Region)

Location (0 - 127) chars

State/Province (0 - 127) chars

Organization (0 - 63) chars

Organization Unit (0 - 63) chars

Certificate

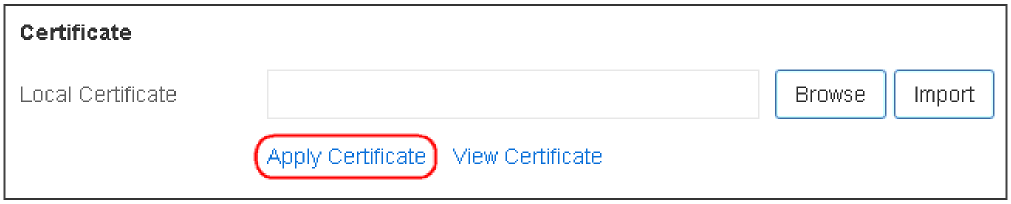
Local Certificate

Certificate Revocation List

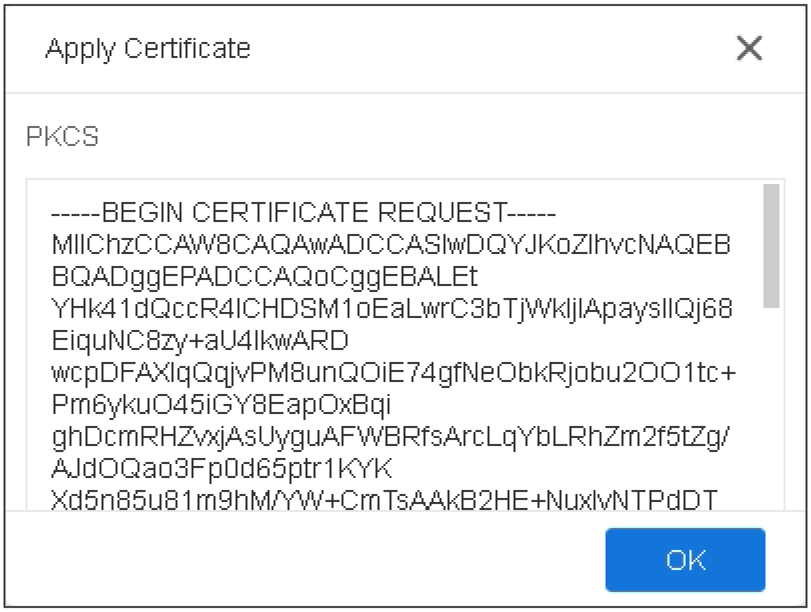
In the Basic Configuration tab, configure values for basic properties.

Option	Description
Basic	
Trust Domain	Enter the name of the new trust domain.
Enrollment Type	Use one of the two following methods: • Select **Manual Input**, and click **Browse** to find the certificate and click **Import** to import it into system. • Select **Self-signed Certificate**, and the certificate will be generated by the device itself.
Key Pair	Select a key pair.
Subject	
Name	Enter a name of the subject.
Country (Region)	Enter the name of applicant's country or region. Only an abbreviation of two letters are allowed, like CN.
Location	Optional. The location of the applicant.
State/Province	Optional. State or province name.
Organization	Optional. Organization name.
Organization Unit	Optional. Department name within applicant's organization.

3. Click **Apply Certificate**, and a string of code will appear.

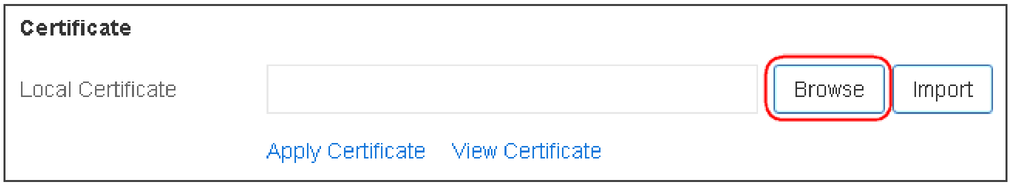


4. Copy this code and send it to CA via email.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIChzCCAW8CAQAwADCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALEt
YHk41dQccR4ICHDSM1oEaLwrC3bTjWkljlApaysIlQj68
EiquNC8zy+aU4IkwARD
wcpDFAXlqQqjvPM8unQOiE74gfNeObkRjobu2OO1tc+
Pm6ykuO45iGY8EapOxBqi
ghDcmRHZvxjAsUyguAFWBRfsArcLqYbLRhZm2f5tZg/
AJdOQao3Fp0d65ptr1KYK
Xd5n85u81m9hM/YW+CmTsAAkB2HE+NuxlvNTPdDT
```

5. When you receive the certificate sent from CA. Click **Browse** to import the certificate.



6. (Optional) In the CRL tab, configure the following.

Certification Revocation List	
Check	- No Check - System does not check CRL. This is the default option.

Certification Revocation List	
	- Optional - System accepts certificating from peer, no matter if CRL is available or not. - Force - System only accepts certificating from peer when CRL is available.
URL 1-3	The URL address for receiving CRL. At most 3 URLs are allowed, and their priority is from 1 to 3. - Select **http://** if you want to get CRL via HTTP. - Select **ldap://** if you want to get CRL via LDAP. - If you use LDAP to receive CRL, you need to enter the login-DN of LDAP server and password. If no login-DN or password is added, the transmission will be anonymous.
Auto Update	Update frequency of CRL list.
Manually Update	Get the CRL immediately by clicking **Obtain CRL**.

7. Click **OK**.

Importing/Exporting Trust Domain

To simplify configurations, you can export certificates (CA or local) and private key (in the format of PKSC12) to a computer and import them to another device.

To export a PKI trust domain, take the following steps:

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

2. Select a domain from drop-down menu.

3. Select the radio button of the item you want to export, and click **Export**.

   If you choose PKCS, you need to set up password.

4. Click **OK**, and select a storage path to save the item.

To import the saved trust domain to another device, take the following steps:

1. Log in the other device, select **System > PKI > Trust Domain Certificate**.

2. Select a domain from drop-down menu.

3. Select the radio button of the item you want to import, and click **Import**.

   If you choose PKCS, you need to enter the password when it was exported.

4. Click **Browse** and find the file to import.

5. Click **OK**. The domain file is imported.

Importing Trust Certification

System will not detect the PE file whose certification is trusted. To import trust certification of PE files, take the following steps:

1. Select **System > PKI > Trusted Root Certificate**.

2. Click **Import** and choose a certificate file in your PC.

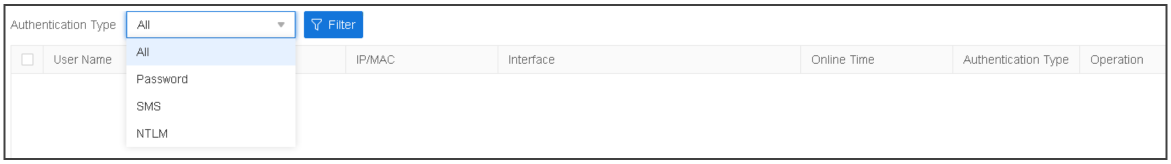
3. Click **OK** and then the file will be imported.

Online Users

To view the online authenticated users, take the following steps:

1. Select **Network >WebAuth > Online Users**.

2. The page will show all online users. You can set up filters to views results that match your conditions.



- User Name: Displays the name of online users.

- IP/MAC: Displays the IP or MAC address of online users.

- Interface: Displays the authentication interface of online users.

- Online Time: Displays the online time of online users.

- Authentication Type: Displays the authentication type of online users.

- Operation: Displays the executable operation of online users.

Chapter 8 VPN

System supports the following VPN functions:

- "IPSec VPN" on Page 372: IPSec is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications. It is a Layer 3 virtual private network (VPN) technology that transmits data in a secure tunnel established between two endpoints.
- "SSL VPN" on Page 410: SSL provides secure connection services for TCP-based application layer protocols by using data encryption, identity authentication, and integrity authentication mechanisms.
- "L2TP VPN" on Page 523: L2TP is one protocol for VPDN tunneling. VPDN technology uses a tunneling protocol to build secure VPNs for enterprises across public networks. Branch offices and traveling staff can remotely access the headquarters’ Intranet resources through a virtual tunnel over public networks.

IPSec VPN

IPSec is a widely used protocol suite for establishing a VPN tunnel. IPSec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPSec protocol defines how to choose the security protocols and algorithms, as well as the method for exchanging security keys among communicating peers, while offering the upper layer protocols with network security services, including access control, data source authentication, data encryption, etc.

Basic Concepts

- Security association
- Encapsulation modes
- Establishing SA
- Using IPSec VPN

Security Association (SA)

IPSec provides encrypted communication between two peers which are known as IPSec ISAKMP gateways. Security Association (SA) is the basis and essence of IPSec. SA defines some factors of communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the life cycle of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

Encapsulation Modes

IPSec supports the following IP packet encapsulation modes:

- Tunnel mode - IPSec protects the entire IP packet, including both the IP header and the payload. It uses the entire IP packet to calculate an AH or ESP header, and then encapsulates the original IP packet and the AH or ESP header with a new IP header. If you use ESP, an ESP trailer will also be encapsulated. Tunnel mode is typically used for protecting gateway-to-gateway communications.
- Transport mode - IPSec only protects the IP payload. It only uses the IP payload to calculate the AH or ESP header, and inserts the calculated header between the original IP header and payload. If you use ESP, an ESP trailer is also encapsulated. The transport mode is typically used for protecting host-to-host or host-to-gateway communications.

Establishing SA

There are two ways to establish SA: manual and IKE auto negotiation (ISAKMP).

- Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.
- IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic networks. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

Using IPSec VPN

To apply VPN tunnel feature in the device, you can use policy-based VPN or route-based VPN.

- Policy-based VPN - Applies the configured VPN tunnel to a policy so that the data flow which conforms to the policy settings can pass through the VPN tunnel.
- Route-based VPN - Binds the configured VPN tunnel to the tunnel interface and define the next hop of static route as the tunnel interface.

Configuring an IKE VPN

IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

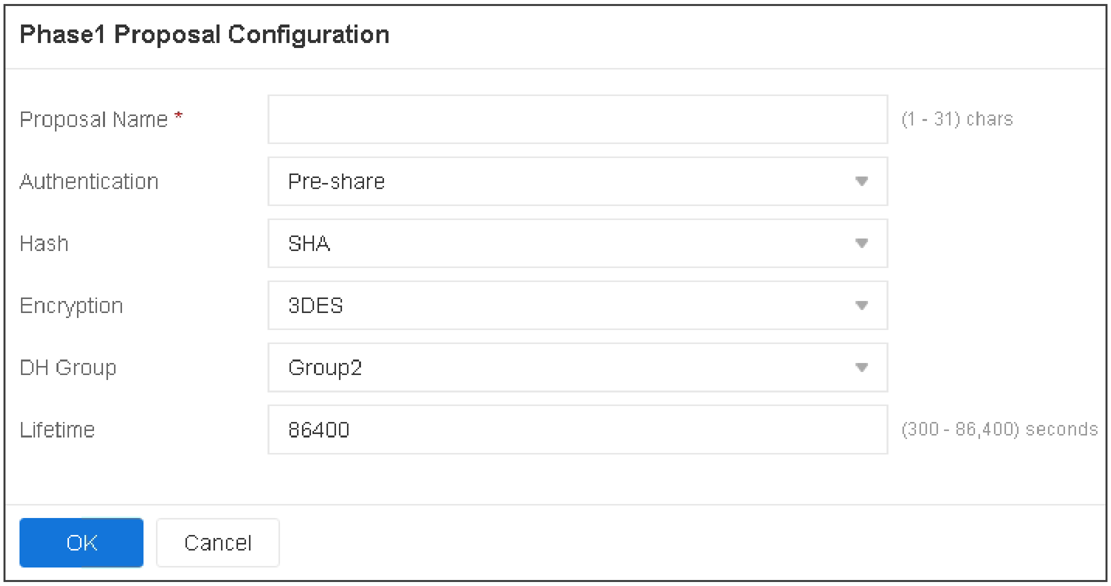
To configure an IKE VPN, you need to confirm the Phase 1 proposal, the Phase 2 proposal, and the VPN peer. After confirming these three contents, you can proceed with the configuration of IKE VPN settings.

Configuring a Phase 1 Proposal

The P1 proposal is used to negotiate the IKE SA. To configure a P1 proposal, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the P1 Proposal tab, click **New**.



Phase1 Proposal Configuration

Proposal Name * (1 - 31) chars

Authentication: Pre-share

Hash: SHA

Encryption: 3DES

DH Group: Group2

Lifetime: 86400 (300 - 86,400) seconds

In the Phase1 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase1 proposal.
Authentication	Specifies the IKE identity authentication method. IKE identity authentication is used to verify the identities of both communication parties. There are three methods for authenticating identity: pre-shared key, RSA signature, DSA signature and GM-DE. The default value is pre-shared key. For pre-shared key method, the key is used to generate a secret key and the keys of both parties must be the same so that it can generate the same secret keys.
Hash	Specifies the authentication algorithm for Phase1. Select the algorithm you want to use. • MD5 – Uses MD5 as the authentication

Option	Description
	algorithm. Its hash value is 128-bit. • SHA – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • SM3 – Use the state password SM3 as the authentication algorithm. Its hash value is 256-bit. It is used for the digital signature and authentication, the generation and authentication of message authentication code, and the generation of random digit, which can meet the security requirement of multiple password applications.
Encryption	Specifies the encryption algorithm for Phase1. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm.

Option	Description
	The key length is 64-bit. • AES − Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 − Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 − Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • SM1 − Uses the state password SM1 as the encryption algorithm. The key length is 128-bit. Only the state password device supports SM1. • SM4 − Uses the state password SM4 as the encryption algorithm. The key length is 128-bit.
DH Group	Specifies the DH group for Phase1 proposal. • Group1 − Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 − Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). Group2 is the default value. • Group5 − Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 − Uses Group14 as the DH group.

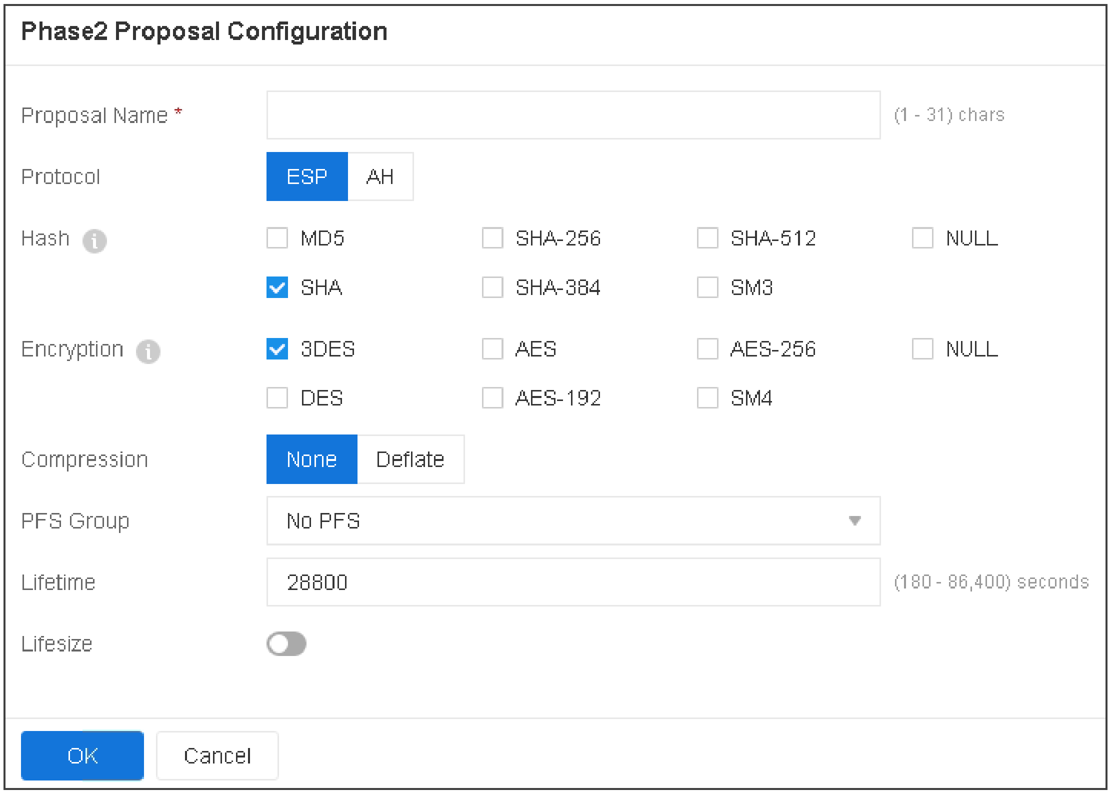
Option	Description
	The key length is 2048-bit (MODP Group). • Group15 − Uses Group5 as the DH group. The key length is 3072-bit (MODP Group). • Group16 − Uses Group5 as the DH group. The key length is 4096-bit (MODP Group). • Group19 - Uses Group 19 as the DH group. The key length is 256 bits (ECP Group). • Group20 - Uses Group 20 as the DH group. The key length is 384 bits (ECP Group). • Group21 - Uses Group 21 as the DH group. The key length is 521 bits (ECP Group). • Group24 - Uses Group 24 as the DH group. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).
Lifetime	Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400. Type the lifetime value into the Lifetime box. When the SA lifetime runs out, the device will send a SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation.

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

Configuring a Phase 2 Proposal

The P2 proposal is used to negotiate the IPSec SA. To configure a P2 proposal, take the following steps:

1. Select **Network** > **VPN** > **IPSec VPN**.
2. In the P2 Proposal tab, click **New**.



Phase2 Proposal Configuration

Proposal Name *	(1 - 31) chars
Protocol	ESP AH
Hash	☐ MD5 ☐ SHA-256 ☐ SHA-512 ☐ NULL ☑ SHA ☐ SHA-384 ☐ SM3
Encryption	☑ 3DES ☐ AES ☐ AES-256 ☐ NULL ☐ DES ☐ AES-192 ☐ SM4
Compression	None Deflate
PFS Group	No PFS
Lifetime	28800 (180 - 86,400) seconds
Lifesize	

OK Cancel

In the Phase2 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase2 proposal.
Protocol	Specifies the protocol type for Phase2. The options are ESP and AH. The default value is ESP.

Option	Description
Hash	Specifies the authentication algorithm for Phase2. Select the algorithm you want to use. • MD5 − Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA − Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 − Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 − Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 − Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • SM3 − Uses the state password SM3 as the authentication algorithm. Its hash value is 256-bit. It is used for the digital signature and authentication, the generation and authentication of message authentication code, and the generation of random digit, which can meet the security requirement of multiple password applications. • Null − No authentication.
Encryption	Specifies the encryption algorithm for Phase2.

Option	Description
	• 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • SM1 – Uses the state password SM1 as the encryption algorithm. The key length is 128-bit. Only the state password device supports SM1. • SM4 – Uses the state password SM4 as the encryption algorithm. The key length is 128-bit. • Null – No authentication.
Compression	Specifies the compression algorithm for Phase2. By default, no compression algorithm is used.
PFS Group	Specifies the PFS function for Phase2. PFS is used to protect DH algorithm. • No PFS - Disables PFS. This is the default value.

Option	Description
	• Group1 – Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 – Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). • Group5 – Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 – Uses Group14 as the DH group. The key length is 2048-bit (MODP Group). • Group15 – Uses Group5 as the DH group. The key length is 3072-bit. • Group16 – Uses Group5 as the DH group. The key length is 4096-bit (MODP Group). • Group19 - Uses Group 19 as the DH group. The key length is 256 bits (ECP Group). • Group20 - Uses Group 20 as the DH group. The key length is 384 bits (ECP Group). • Group21 - Uses Group 21 as the DH group. The key length is 521 bits (ECP Group). • Group24 - Uses Group 24 as the DH group. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).

Option	Description
Lifetime	You can evaluate the lifetime by two standards which are the time length and the traffic volume. Type the lifetime length of P2 proposal into the box. The value range is 180 to 86400 seconds. The default value is 28800.
Lifesize	Select **Enable** to enable the P2 proposal traffic-based lifetime. By default, this function is disabled. After selecting Enable, specifies the traffic volume of lifetime. The value range is 1800 to 4194303 KBs. The default value is 1800. Type the traffic volume value into the box.

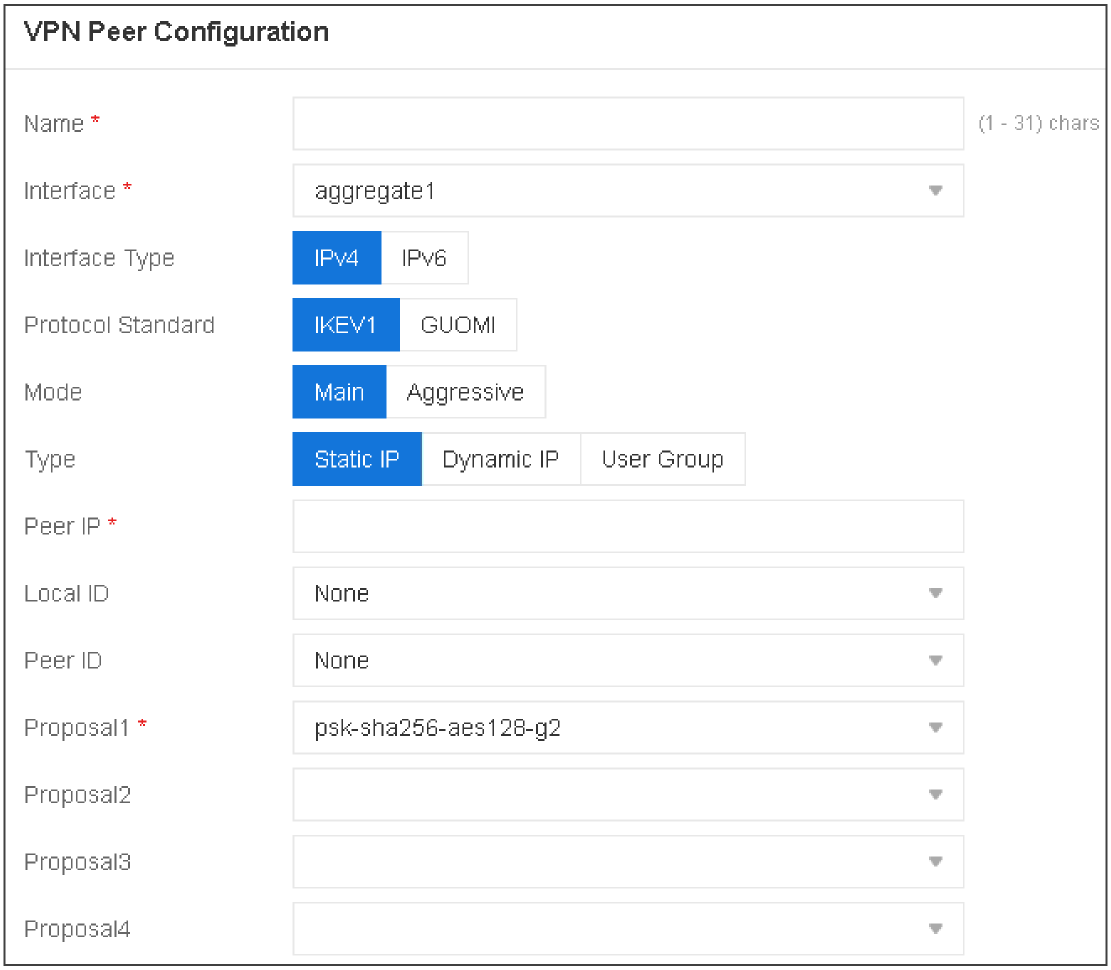
3. Click **OK** to save the settings.

Configuring a VPN Peer

To configure a VPN peer, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the VPN Peer List tab, click **New**.



VPN Peer Configuration

Name * (1 - 31) chars

Interface * aggregate1 ▾

Interface Type [✓ IPv4] IPv6

Protocol Standard [✓ IKEV1] GUOMI

Mode [✓ Main] Aggressive

Type [✓ Static IP] Dynamic IP User Group

Peer IP *

Local ID None ▾

Peer ID None ▾

Proposal1 * psk-sha256-aes128-g2 ▾

Proposal2 ▾

Proposal3 ▾

Proposal4 ▾

In the VPN Peer Configuration dialog box, configure the corresponding options.

Basic Configuration	
Name	Specifies the name of the ISAKMP gateway.
Interface	Specifies interface bound to the ISAKMP gateway.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6

Basic Configuration	
	type interface.
Protocol Standard	Specifies the protocol standard, including IKEv1 and GUOMI . The default protocol standard is IKEv1. If you select GUOMI, specify the version: • v1.0: the version is 1.0. • v1.1: the version is 1.1. • Default: the initiator can negotiate with the peer when the initiator version is v1.0 or v1.1. Note: If you specify the version as 1.0 or 1.1, the version of the two peers which negotiate with each other should be the same, or system will fail to negotiate.
Mode	Specifies the mode of IKE negotiation. There are two IKE negotiation modes: **Main** and **Aggressive**. The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation where the IP address of the center device is static and the IP address of client device is dynamic.
Type	Specifies the type of the peer IP. If the peer IP is static, type the IP address into the **Peer IP** box; if the peer IP type is user group, select the AAA server you need from the **AAA Server** drop-down list.
Local ID	Specifies the local ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for

Basic Configuration	
	license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the **Local ID** box or the **Local IP** box.
Peer ID	Specifies the peer ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the **Peer ID** box or the **Peer IP** box.
Proposal1/2/3/4	Specifies a P1 proposal for ISAKMP gateway. Select the suitable P1 proposal from the **Proposal1** drop-down list. You can define up to four P1 proposals for an ISAKMP gateway.
Pre-shared Key	If you choose to use pre-shared key to authenticate, type the key into the box.
Self-signed Trust Domain	If you choose to use RSA signature or DSA signature, select a trust domain.
Peer Trust Domain	Configure the trust domain of peer certification. The peer certification is used for data encryption and authentication in the negotiation. The initiator should import the peer certification first. Only GUOMI v1.0 supports this option.
Encryption Trust Domain	Configure the trust domain of encryption certification. The encryption certification is used for data encryption in the negotiation. Only GUOMI v1.1 supports this option.

3. If necessary, click the **Advanced Configuration** tab to configure some advanced options.

In the Advanced Configuration tab, configure the corresponding options.

Advanced Configuration	
Connection Type	Specifies the connection type for ISAKMP gateway. • Bidirectional - Specifies that the ISAKMP gateway serves as both the initiator and responder. This is the default value. • Initiator - Specifies that the ISAKMP gateway serves as the only initiator. • Responder - Specifies that the ISAKMP gateway serves as the only responder.
NAT Traversal	This option must be enabled when there is a NAT device in the IPSec or IKE tunnel and the device implements NAT. By default, this function is disabled.
Any Peer ID	Makes the ISAKMP gateway accept any peer ID and not check the peer IDs.
Generate Route	Select the **Enable** check box to enable the auto routing function. By default, this function is disabled. This function allows the device to automatically add routing entries which are from the center device to the branch, avoiding the problems caused by manual configured routing.
DPD	Select the **Enable** check box to enable the DPD (Delegated Path Discovery) function. By default, this function is disabled. When the responder does not receive the peer's packets for a long period, it can enable DPD and initiate a DPD request to the peer so that it can test if the ISAKMP gateway exists.

Advanced Configuration	
	- DPD Interval - The interval of sending DPD request to the peer. The value range is 1 to 10 seconds. The default value is 10 seconds. - DPS Retries - The times of sending DPD request to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD reties. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.
Description	Type the description for the ISAKMP gateway.
XAUTH Server	Select **Enable** to enable the XAUTH server in the device. Then select an address pool from the drop-down list. After enabling the XAUTH server, the device can verify the users that try to access the IPSec VPN network by integrating the configured AAA server.

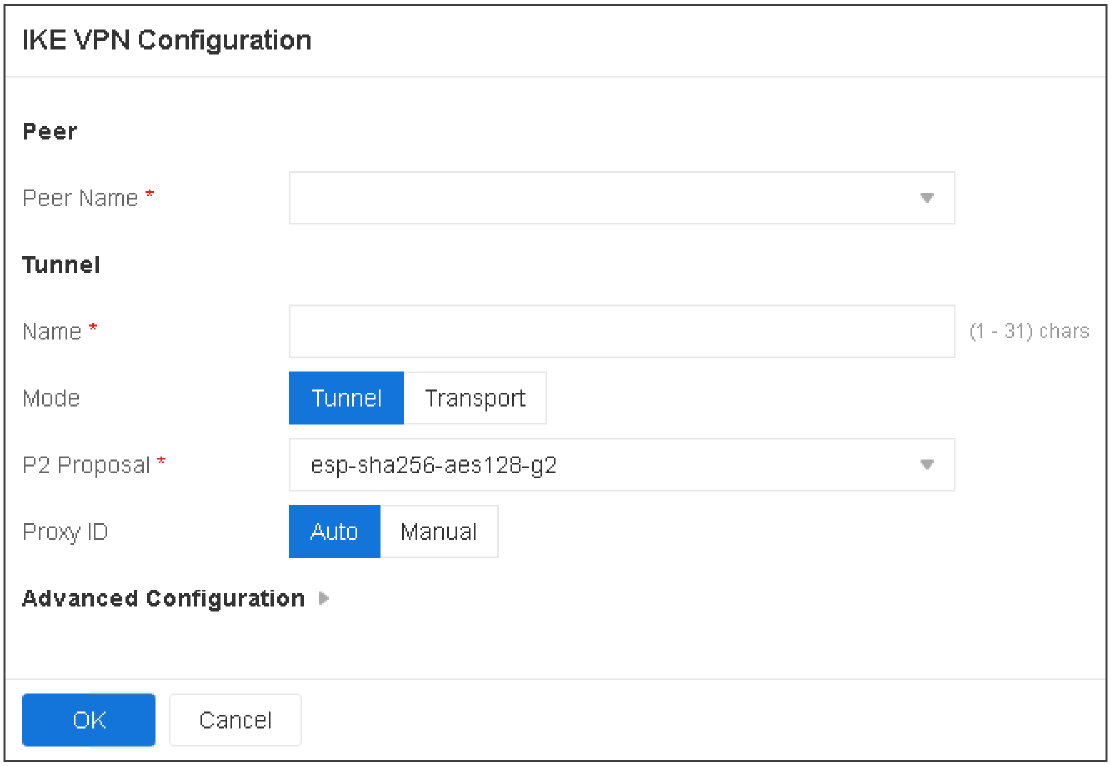
4. Click **OK** to save the settings.

Configuring an IKE VPN

Use IKE to negotiate IPSec SA automatically. To configure IKE VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the IKE VPN List tab, click **New**.



IKE VPN Configuration

Peer

Peer Name *

Tunnel

Name * (1 - 31) chars

Mode: Tunnel | Transport

P2 Proposal *: esp-sha256-aes128-g2

Proxy ID: Auto | Manual

Advanced Configuration

In the Basic Configuration tab, configure the corresponding options.

Peer	
Peer Name	Specifies the name of the ISAKMP gateway. To edit an ISAKMP gateway, click **Edit**.
Information	Shows the information of the selected peer.
Tunnel	
Name	Type a name for the tunnel.
Mode	Specifies the mode, including tunnel mode and transport mode.
P2 Proposal	Specifies the P2 proposal for tunnel.
Proxy ID	Specifies ID of Phase 2 for the tunnel which can be

Peer	
	Auto or Manual. • Auto - The Phase 2 ID is automatically designated. • Manual - The Phase 2 ID is manually designated. Manual configuration of P2 ID includes the following options: • Local IP/Netmask - Specifies the local ID of Phase 2. • Remote IP/Netmask - Specifies the Phase 2 ID of the peer device. • Service - Specifies the service.

3. If necessary, click the **Advanced Configuration** tab to configure some advanced options.

In the Advanced Configuration tab, configure the corresponding options.

Advanced	
DNS1/2/3/4	Specifies the IP address of the DNS server allocated to the client by the PnPVPN server. You can define one primary DNS server and three backup DNS servers.
WINS1/2	Specifies the IP address of WINS server allocated to the client by the PnPVPN server. You can define one primary WINS server and a backup WINS server.
Enable Idle Time	Select the **Enable** check box to enable the idle time function. By default, this function is disabled. This time length is the longest time the tunnel can exist without traffic passing through. When the time is over,

Advanced	
	SA will be cleared.
DF-Bit	Select the check box to allow the forwarding device to execute IP packet fragmentation. The options are: • Copy - Copies the IP packet DF options from the sender directly. This is the default value. • Clear - Allows the device to execute packet fragmentation. • Set - Disallows the device to execute packet fragmentation.
Anti-Replay	Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled. • Disable - Disables this function. • 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.
Commit Bit	Select the **Enable** check box to make the corresponding party configure the commit bit function, which can avoid packet loss and time difference. However, commit bit may slow the responding speed.

Advanced	
Accept-all-proxy-ID	This function is disabled by default. With this function enabled, the device which is working as the initiator will use the peer's ID as its Phase 2 ID in the IKE negotiation, and return the ID to its peer.
Auto Connect	Select the **Enable** check box to enable the auto connection function. By default, this function is disabled. The device has two methods of establishing SA: auto and intrigued traffic mode. When it is auto mode, the device will check SA status every 60 seconds and initiate negotiation request when SA is not established; when it is in intrigued traffic mode, the tunnel will send negotiation request only when there is traffic passing through the tunnel. By default, the intrigued traffic mode is enabled. **Note**: Auto connection works only when the peer IP is static and the local device is the initiator.
Tunnel Route	This item can be modified only after this IKE VPN is created. Click **Choose** to add one or more tunnel routes in the appearing Tunnel Route Configuration dialog box. You can add up to 128 tunnel routes.
Description	Type the description for the tunnel.
Tunnel State Notify	Select the **Enable** check box to enable the tunnel state notification function. With this function enabled, for route-based VPN, system will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route once any VPN tunnel disconnection is detected; for policy-based VPN, system will inform the policy module about the inform-

Advanced	
	ation of the disconnected VPN tunnel and update the tunnel policy once any VPN tunnel disconnection is detected.
VPN Track	Select the **Enable** check box to enable the VPN track function. The device can monitor the connectivity status of the specified VPN tunnel, and also allows backup or load sharing between two or more VPN tunnels. This function is applicable to both route-based and policy-based VPNs. The options are: • Track Interval - Specifies the interval of sending Ping packets. The unit is second. • Threshold - Specifies the threshold for determining the track failure. If system did not receive the specified number of continuous response packets, it will identify a track as failure, i.e., the target tunnel is disconnected. • Src Address - Specifies the source IP address that sends Ping packets. • Dst Address - Specifies the IP address of the tracked object.

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

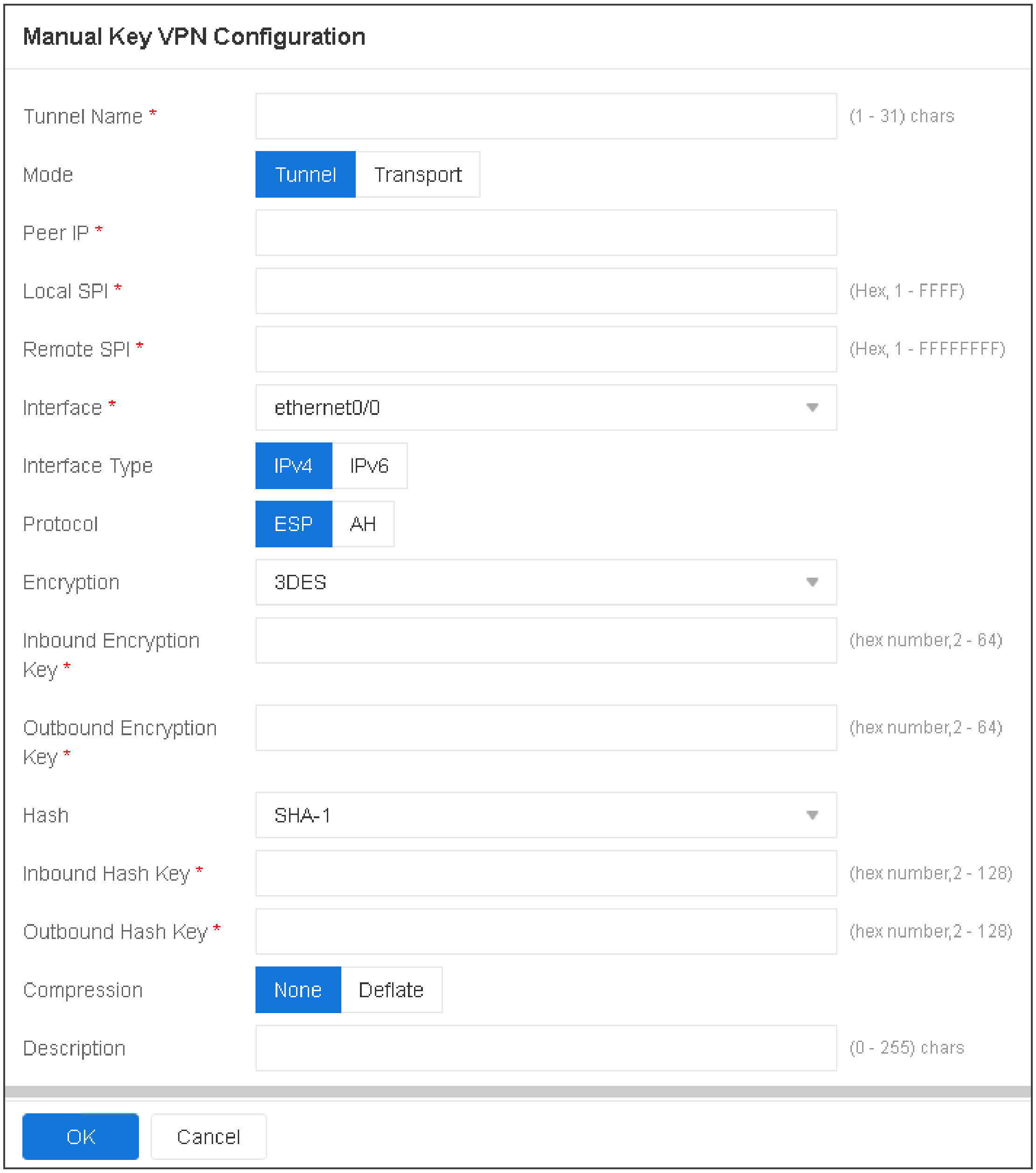
Configuring a Manual Key VPN

Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.

To create a manual key VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the Manual Key VPN Configuration section, click **New**.



Manual Key VPN Configuration

Tunnel Name * (1 - 31) chars

Mode: Tunnel | Transport

Peer IP *

Local SPI * (Hex, 1 - FFFF)

Remote SPI * (Hex, 1 - FFFFFFFF)

Interface * ethernet0/0

Interface Type: IPv4 | IPv6

Protocol: ESP | AH

Encryption: 3DES

Inbound Encryption Key * (hex number,2 - 64)

Outbound Encryption Key * (hex number,2 - 64)

Hash: SHA-1

Inbound Hash Key * (hex number,2 - 128)

Outbound Hash Key * (hex number,2 - 128)

Compression: None | Deflate

Description (0 - 255) chars

In the Manual Key VPN Configuration dialog box, configure the corresponding options.

Basic Configuration	
Tunnel Name	Specifies the name of manually created key VPN.

Basic Configuration	
Mode	Specifies the mode, including Tunnel and Transport. The tunnel mode is the default mode.
Peer IP	Specifies the IP address of the peer.
Local SPI	Type the local SPI value. SPI is a 32-bit value transmitted in AH and ESP header, which uniquely identifies a security association. SPI is used to seek corresponding VPN tunnel for decryption.
Remote SPI	Type the remote SPI value. **Note**: When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.
Interface	Specifies the egress interface for the manual key VPN. Select the interface you want from the **Interface** drop-down list.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type interface.
Encryption	
Protocol	Specifies the protocol type. The options are ESP and AH. The default value is ESP.
Encryption	Specifies the encryption algorithm. • None − No authentication. • 3DES − Uses 3DES as the encryption algorithm.

Basic Configuration	
	The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
Inbound Encryption Key	Type the encryption key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key.
Outbound Encryption Key	Type the encryption key of the outbound direction.
Hash	Specifies the authentication algorithm. Select the algorithm you want to use. • None – No authentication. • MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit.

Basic Configuration	
	• SHA-1 – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Inbound Hash Key	Type the hash key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the peer's inbound hash key.
Outbound Hash Key	Type the hash key of the outbound direction.
Compression	Select a compression algorithm. By default, no compression algorithm is used.
Description	
Description	Type the description for the manual key VPN.

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

Viewing IPSec VPN Monitoring Information

By using the ISAKMP SA table, IPSec SA table, and Dial-up User table, IPSec VPN monitoring function can show the SA negotiation results of IPSec VPN Phase1 and Phase2 as well as information of dial-up users.

To view the VPN monitoring information, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IKE VPN Configuration section, click **IPSec VPN Monitor**.

Options in these tabs are described as follows:

ISAKMP SA

Option	Description
Cookie	Displays the negotiation cookies which are used to match SA Phase 1.
Status	Displays the status of SA Phase1.
Peer	Displays the IP address of the peer.
Port	The port number used by the SA Phase1. 500 indicates that no NAT has been found during the SA Phase 1; 4500 indicates that NAT has been detected.
Algorithm	Displays the algorithm of the SA Phase1, including authentication method, encryption algorithm and verification algorithm.
Lifetime	Displays the lifetime of SA Phase1. The unit is second.

IPSec SA

Option	Description
ID	Displays the tunnel ID number which is auto assigned by the system.
VPN Name	Displays the name of VPN.
Direction	Displays the direction of VPN.
Peer	Displays the IP address of the peer.
Port	The port number used by the SA Phase2.
Algorithm	The algorithm used by the tunnel, including protocol type, encryption algorithm, verification algorithm and depression algorithm.
SPI	Displays the local SPI and the peer SPI. The direction of inbound is local SPI, while outbound is peer SPI.
CPI	Displays the compression parameter index (CPI) used by SA Phase2.
Lifetime (s)	Displays the lifetime of SA Phase2 in seconds, i.e. SA Phase2 will restart negotiations after X seconds.
Lifetime (KB)	Displays the lifetime of SA Phase2 in KB, i.e. SA Phase2 will restart negotiations after X kilobytes of data flow.
Status	Displays the status of SA Phase2.

Dial-up User

Option	Description
Peer	Displays the statistical information of the peer user. Select the peer you want from the Peer drop-down list.

Option	Description
User ID	Displays the IKE ID of the user selected.
IP	Displays the corresponding IP address.
Encrypted Packets	Displays the number of encrypted packets transferred through the tunnel.
Encrypted Bytes	Displays the number of encrypted bytes transferred through the tunnel.
Decrypted Packets	Displays the number of decrypted packets transferred through the tunnel.
Decrypted Bytes	Displays the number of decrypted bytes transferred through the tunnel.

Configuring PnPVPN

IPSec VPN requires sophisticated operational skills and high maintenance cost. To relieve network administrators from the intricate work, system provides an easy-to-use VPN technology - PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer, the PnPVPN Server sends most of the configuration commands to the clients. The device usually works as a PnPVPN Server and one device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by a headquarters engineer, the PnPVPN Client can obtain configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server with simple configurations, such as client ID, password, and server IP settings.

The device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instance and the supported client number of each device may vary according to the platform series.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends his/her own ID and password to the server.
2. The server verifies the ID and password when it receives the request. If the verification succeeds, the server will send the configuration information, including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc,. to the client.
3. The client distributes the received information to corresponding functional modules.

4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be configured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

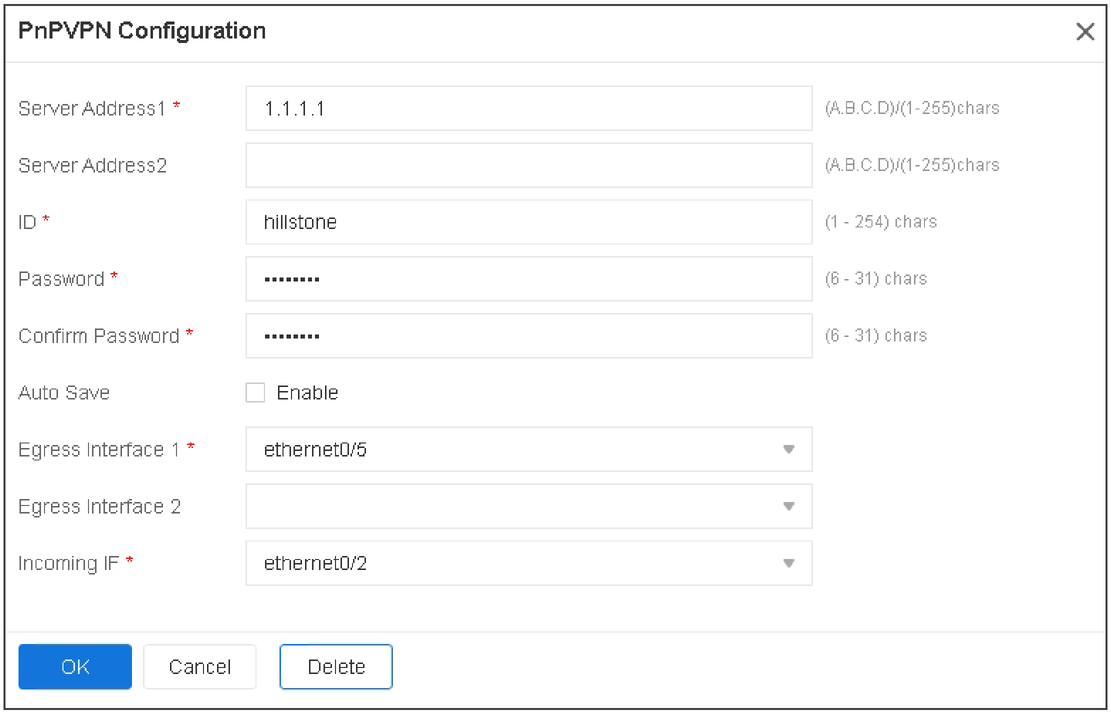
The client supports to configure dual VPN dials and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

Configuring a PnPVPN Client

To configure a PnPVPN client, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. At the top right corner of the IKE VPN Configuration section, click **Configuration**, selcet **PnPVPN Configuration** from the drop-down list.



PnPVPN Configuration

Server Address1 *	1.1.1.1	(A.B.C.D)/(1-255)chars
Server Address2		(A.B.C.D)/(1-255)chars
ID *	hillstone	(1 - 254) chars
Password *	••••••••	(6 - 31) chars
Confirm Password *	••••••••	(6 - 31) chars
Auto Save	□ Enable	
Egress Interface 1 *	ethernet0/5	
Egress Interface 2		
Incoming IF *	ethernet0/2	

In the PnPVPN Configuration dialog box, configure the following options.

Option	Description
Server Address1	Type the IP address of PnPVPN Server into the box. PnPVPN client supports dual link dials to the server side. This option is required.
Server Address2	Type the IP address of PnPVPN Server into the box. The server address 1 and the server address 2 can be the same or different. It is optional.
ID	Specifies the IKE ID assigned to the client by the server.
Password	Specifies the password assigned to the client by the server.
Confirm Password	Enter the password again to confirm.
Auto Save	Select Enable to auto save the DHCP and WINS inform-

Option	Description
	ation released by the PnPVPN Server.
Egress Interface 1	Specifies the interface connecting to the Internet. This option is required.
Egress Interface 2	Specifies the interface connecting to the Internet. The IF1 and the IF2 can be the same or different. It is optional.
Incoming IF	Specifies the interface on the PnPVPN Client accessed by the Intranet PC or the application servers.

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

Notes:

- Server Addresses1 and Egress IF1 both need to be configured. If you want to configure a backup link, you need to configure both the Server Address2 and Egress IF2.
- If the server addresses or the Egress IFs are different, two separate VPN links will be generated.
- The configuration of the two servers can be configured on one device, and can also be configured on two different devices. If you configure it on two devices, you need to configure AAA user on the two devices. The DHCP configuration for the AAA user should be the same, otherwise it might cause that the client and server negotiate successfully, but the traffic is blocked.

Configuring IPSec-XAUTH Address Pool

XAUTH server assigns the IP addresses in the address pool to users. After the client has established a connection to the XAUTH server successfully, the XAUTH server will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and will assign them to the client.

XAUTH server provides fixed IP addresses by creating and implementing IP binding rules that consist of a static IP binding rule and an IP-role binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client. The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When the XAUTH server is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses to the client based on the specific checking order below:

1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, check the other configuration. Note if the binding IP address is in use, the user will be unable to log in.
2. Check if the client is configured with any IP-role binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.

Notes: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To configure the IPSec-XAUTH address pool, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. At the top-right corner, Select **IPSec-XAUTH Address Pool.**.
3. In the XAUTH Address Pool Configuration dialog box, click **New**.

In the Basic Configuration tab, configure the corresponding options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
Netmask	Specifies the netmask of the IP address.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. At most two DNS servers can be configured for one address pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to two WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add the item that binds the specified user to the IP address.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Select a role from the **Role**drop-down list.
Start IP	Type the start IP address into the **Start IP**

Option	Description
	box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add** to add the item that binds the specified role to the IP address range.
Up/Down/Top/Bottom	Move the selected IP-role binding rule . For the user that is bound to multiple roles that are also configured with their corresponding IP-role binding rules, system will query the IP-role binding rules in order, and assign an IP address based on the first matched rule.

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

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.
- Encrypt and forward IPSec data.

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:

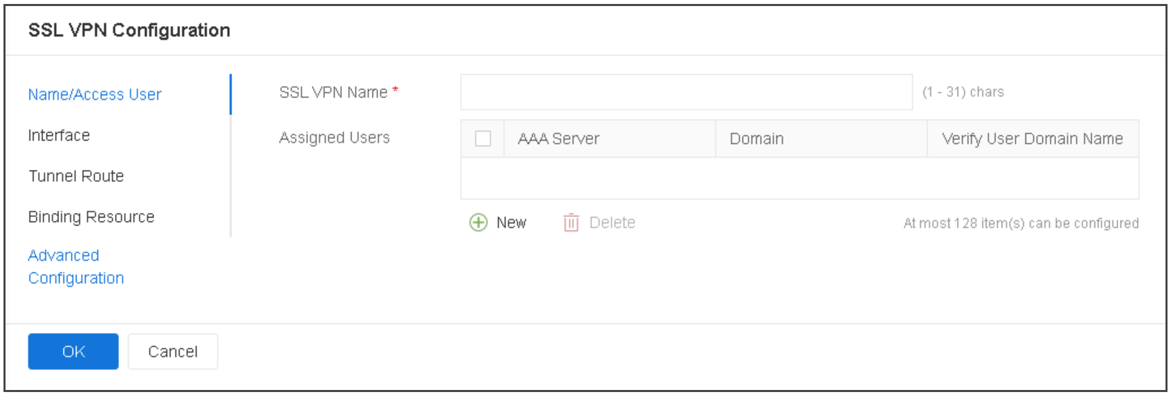
- "SSL VPN Client for Windows" on Page 449
- "SSL VPN Client for Android" on Page 495
- "SSL VPN Client for iOS" on Page 502
- "SSL VPN Client for Mac OS" on Page 507
- "SSL VPN Client for Linux" on Page 512

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**.



SSL VPN Configuration

Name/Access User
Interface
Tunnel Route
Binding Resource
Advanced Configuration

SSL VPN Name * (1 - 31) chars

Assigned Users

□	AAA Server	Domain	Verify User Domain Name

⊕ New   Delete   At most 128 item(s) can be configured

OK   Cancel

In the Name/Access User tab, configure the corresponding options.

Option	Description
SSL VPN Name	Type the name of the SSL VPN instance
Assigned Users	
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.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server.
Verify User Domain Name	After enabling this function, system will verify the user-name and its domain name.
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 Interface1	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.
Egress Interface2	Select the interface from the drop-down list. This interface is needed when the optimal path detection function is enabled.
Service Port	Specifies the SSL VPN service port number.
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 then click **Edit** to edit the selected tunnel interface. • Click **New** in the drop-down list to create a new interface.
Information	Shows the zone, IP address, and netmask of the selected tunnel interface.
Address Pool	
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.

Information	Shows the start IP address, end IP address, and mask of the address pool.

In the Tunnel Route tab, configure the following options.

Tunnel Route	
Specify the destination network segment that you want to access through SCVPN tunnel. 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.	
IP	Type the destination IP address.
Mask	Type the netmask of the destination IP address.
Metric	Type the metric value.
Add	Click **Add** to add this route. You can repeat to add more items.
Delete	Click **Delete** to delete the selected route.
Enable Domain Route	
Specify the destination domain name that you want to access through SCVPN tunnel. After selecting the **Enable Domain Route** check box, 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.	
Domain	Specify 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.
Add	Click **Add** to add the domain name to the list and you can add up to 64 domain names.

Delete	Click **Delete** to delete the selected domain name.
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.

In the Binding Resource tab, configure the binding relationship between user groups and resources.

Binding Resource	
Resource List	Types or selects an existing resource name.
User Group	Specifies a user group name. 1. From the **User Group** drop-down menu, select the AAA servers where user groups reside. Currently, only the local authentication server and the RADIUS server are available. 2. Based on different types of AAA server, you can execute one or more actions: search a user group, expand the user group list, and enter the name of the user group. 3. After selecting user groups, click → to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog to complete the configuration. **Note**: • A user group can be bound with multiple resources, and a resource can also be bound with multiple user

	groups. - Only 32 binding entries can be configured in an SSL VPN instance.
Add	Click **Add** to add binding entries for resources and user groups to the list below. You can repeat to add more items.
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. **Any** indicates one of SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2 or GMSSLv1.0 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 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 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 3DES. **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 SHA-1. **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 Browser Login	If the check box is selected , you're allowed to log in to SSL VPN via the browser WebUI. By default, the function is enabled. When this function is disabled, you can only log in to the SSL VPN via SCVPN client.
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 15 to 1500 minutes. The default value is 30.
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 login time into the **Multiple Login Times** box. The value range is 0 to 99,999,999. The value of 0 indicates no login time limitation.
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 SSL VPN connection.

In the Client tab, configure the corresponding options.

Client Configuration	
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 1 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 1 to 255 characters.
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 1 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+username=$GBUSER&password=$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 1 to 31 bytes. This title will appear as a client menu item.
Delete privacy data after disconnection	Select **Enable** to delete the corresponding privacy data after the client's disconnection.
Digital Certificate Authentication	
Authentication	Select the **Enable** check box to enable this function. 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 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" on Page 630. • 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.

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 Veri-	Click **Two-Step Verification** to enable the func-

fication	tion. Two-Step Verification means that when an SSL VPN user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS Authentication, Token Authentication or Email Authentication after the username and password is entered. The user must enter the random verification code received in order to log into SSL VPN and access intranet resources.
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. • 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" on Page 1241.
Lifetime of SMS Auth Code	Specifies the lifetime of the SMS authentication code. Type the lifetime value into the **Lifetime of SMS Auth Code** box. The range is 1 to 10 minutes.
Sender Name	Specifies a message sender name to display in the message content. The range is 1 to 63. **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 range is 4 to 8 characters. The default value is 8.
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 the "SMS Gateway Name" option, the code of the SMS template must be entered in this field. The range is 1 to 29 characters. This para-

	meter 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" on Page 1237.
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 1 to 63 characters. The default value is "hillstone". In order to prevent the mail from being identified as spam, it's recommended that users to configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The range is 4 to 8 characters. 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 default content is "SCVPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not 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" on Page 443.	
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 text-

	box. 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 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	Specify 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	Select the **Enable Host Binding** check box to enable the 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" on Page 436.

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.
The device	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 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.

4. Click **Done** to save the settings.

To view the SSL VPN online users, take the following steps:

1. Select **Configure > Network > SSL VPN**.

2. Select an SSL VPN instance.

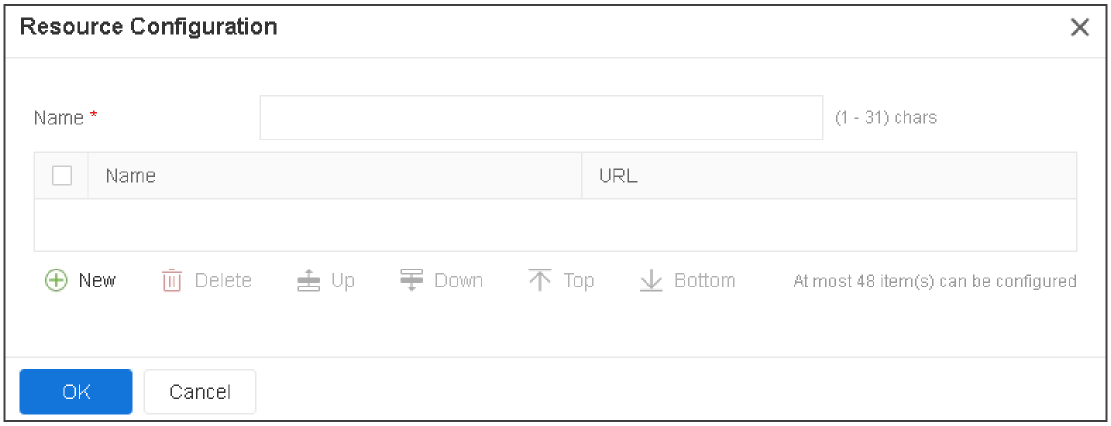
3. View the detailed information of the online users in the table.

Configuring Resource List

Resource list refers to resources configured in system that can be easily accessible by users. Each resource contains multiple resource items. The resource item is presented in the form of a resource item name followed by a URL in your default browser page. After the SSL VPN user is authenticated successfully, the authentication server will send the user group information of the user to the SSL VPN server. Then, according to the binding relationship between the user group and resources in the SSL VPN instance, the server will send a resource list in which the user can access to the client. After that, the client will analyze and make the IE browser in system pop up a page to display the received resource list information, so that the user can access the private network resource directly by clicking the URL link. The resource list page pops up only after the authentication is passed. If a user does not belong to any user group, the browser will not pop up the resource list page unless authentication is passed.

To configure resource list for SSL VPN:

1. Select **Network > VPN > SSL VPN**.
2. Click **Configuration > Resources List** at the top-right corner.
3. Click **New**.



In the Resources Configuration dialog box, configure the corresponding options.

Option	Description

Name	Enters a name for the new resource.
Resource Item	
Name	Enters a name for a new resource item. Names of resource items in different resources can not be the same.
URL	Enters a URL for a new resource item.
Add	Click **Add**to add this binding item to the list below. **Note**: The number of resource items that can be added in a resource ranges from 0 to 48. The total number of resource items that can be added in all resources can not exceed 48.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down/Top/Bottom	You can move the location for items at your own choice to adjust the presentation sequence accordingly.

4. Click **OK**, the new resource will be displayed in the resource list.

   At most 3 resource items can be displayed in the resource list for each resource, and the other items will be displayed as "...". You can click **Edit** or **Delete** button to edit or delete the selected resource.

Notes:

- Less than 48 resources can be configured in a SSL VPN instance.

- The resource list function is only available for Windows SSL VPN clients.

Configuring an SSL VPN Address Pool

The SSL VPN servers allocate the IPs in the SSL VPN address pools to the clients. After the client connects to the server successfully, the server will fetch an IP address along with other related parameters (e.g., DNS server address, and WIN server address) from the SSL VPN address pool and then allocate the IP and parameters to the client.

You can create an IP binding rule to meet the fixed IP requirement. The IP binding rule includes the IP-user binding rule and the IP-role binding rule. The IP-user binding rule binds the client to a fixed IP in the configured address pool. When the client connects to the server successfully, the server will allocate the binding IP to the client. The IP-role binding rule binds the role to an IP range in the configured address pool. When the client connects to the server successfully, the server will select an IP from the IP range and allocate the IP to the client.

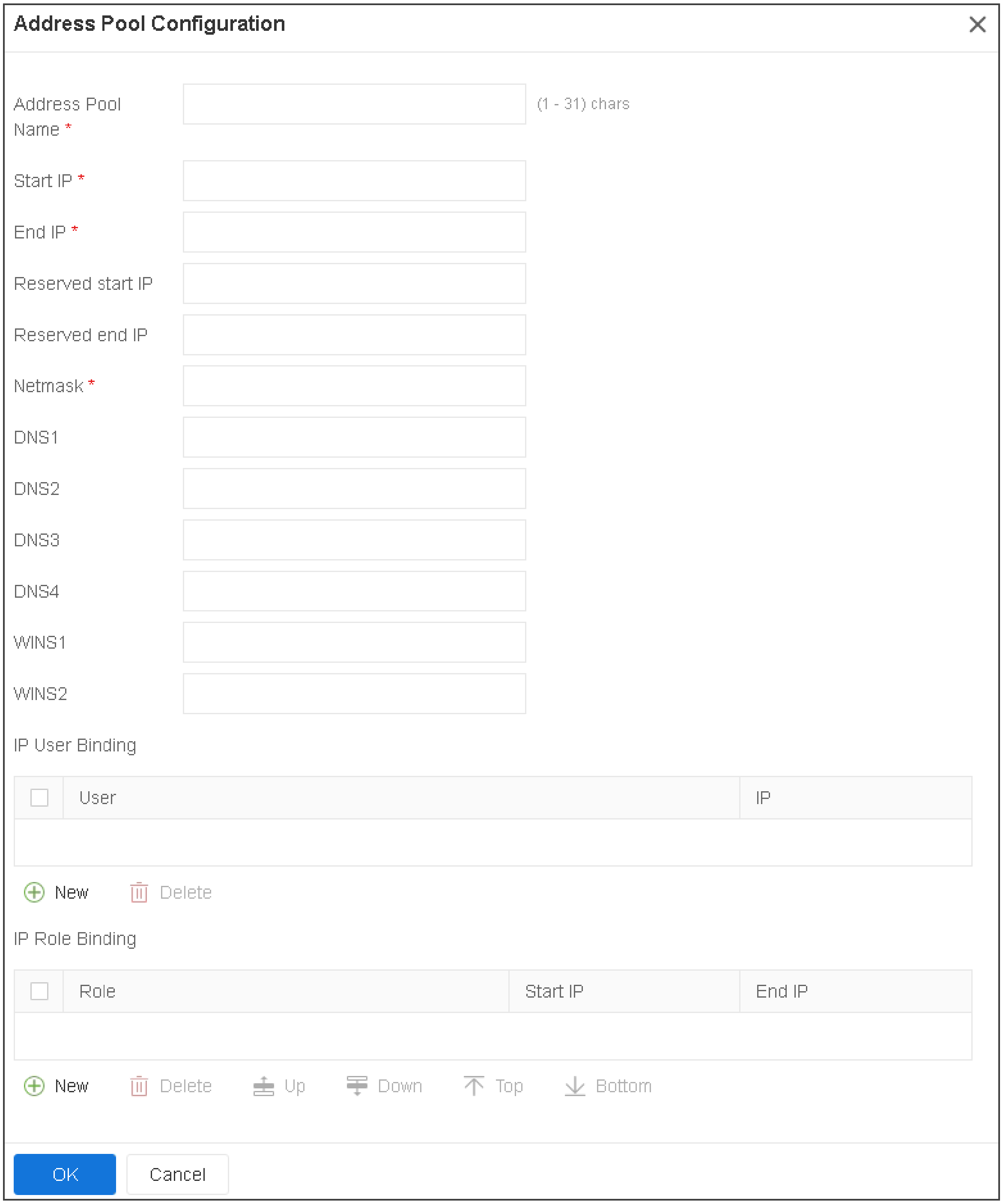
After the client successfully connects to the server, the server will check the binding rules in a certain order to determine which IP to allocate. The order is shown as below:

- Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.
- Check whether the IP-role binding rule is configured for the client. If yes, get an IP from the IP range and allocate to the client; if no, the server will select an IP which is not bound or used from the address pool, then allocate it to the client.

Notes: IP addresses in the IP-user binding rule and the IP address in the IP-role binding rules should not overlap.

To configure an address pool, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. Click **Configuration > Address Pool** at the top-right corner.
3. Click **New**.



In the Basic tab, configure the following options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
Netmask	Specifies the netmask in the dotted decimal format.
DNS1/2/3/4	Specifies the DNS server IP address for the address pool. It is optional. 4 DNS servers can be configured for one address pool at most.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add this IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from

	the list and click **Delete**.

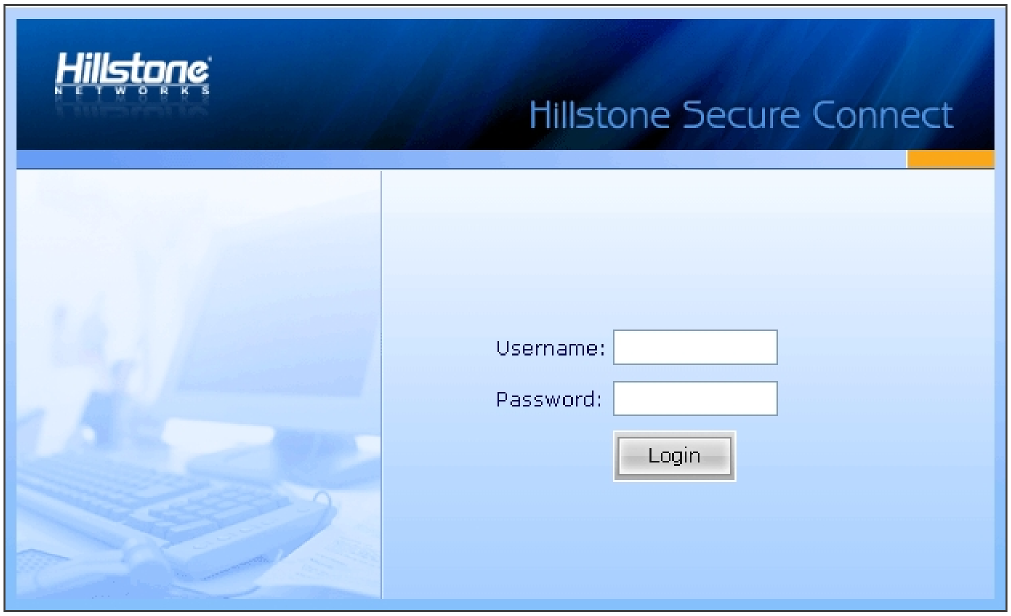
In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the **Role** box.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add**to add this IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down/Top/Bottom	System will query IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

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

Configuring SSL VPN Login Page

You can customize the title and background of the SSL VPN login page. The default title is **Login** and the login page is shown as below:



To customize the SSL VPN login page, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top-right corner, click **Configuration > Login Page Configuration**.
3. Click **Browse** to select the background picture. The selected pictures must be zipped, and the file name must be **Login_box_bg_en.gif** for English pages. The picture size must be 624px*376px.
4. Click **Upload** to upload the background picture to system. After uploading successfully, you will have completed the background picture modification.
5. Enter the title in the **Authentication Page Title** box to customize the title of the login page.
6. Click **OK** to save the settings. Clicking **Cancel** will only affect the authentication page title modification.

If you want to use the default authentication title **Login**, click **Clear Page Title**. Then click **OK**. If you want to restore the default picture, click **Restore Default Background** and select **English** in the pop-up dialog. Then click **OK**.

Host Binding

The host binding function verifies that the hosts are running the SSL VPN clients according to their host IDs and user information. The verification process is:

1. When an SSL VPN user logs in via the SSL VPN client, the client will collect the host information of main board serial number, hard disk serial number, CUP ID, and BIOS serial number.
2. Based on the above information, the client performs the MD5 calculation to generate a 32-digit character, which is named host ID.
3. The client sends the host ID and user/password to the SSL VPN server.
4. The SSL VPN server verifies the host according to the entries in the host unbinding list and host binding list, and deals with the verified host according to the host binding configuration.

The host unbinding list and host binding list are described as follows:

- Host unbinding list: The host unbinding list contains the user-host ID entries for the first-login users.
- Host binding list: The host binding list contains the user-host ID entries for the users who can pass the verification. The entries in the host unbinding list can be moved to the host binding list manually or automatically for the first login. When a user logs in, the SSL VPN server will check whether the host binding list contains the user-host ID entry of the login user. If there is a matched entry in the host binding list, the user will pass the verification and the sever will go on checking the user/password. If there is no matched entry for the login user, the connection will be disconnected.

Configuring Host Binding

Configuring host binding includes host binding/unbinding configurations, super user configurations, shared host configurations, and user-host binding list importing/exporting.

Configuring Host Binding and Unbinding

To add a binding entry to the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Compliance Check-/Binding page.

2. With the Binding and Unbinding tab active, select the entries you want to add to the Host Unbinding List.
3. Click **Add** to add the selected entries to the Host Binding List.

To delete a binding entry from the host binding list, take the following steps:

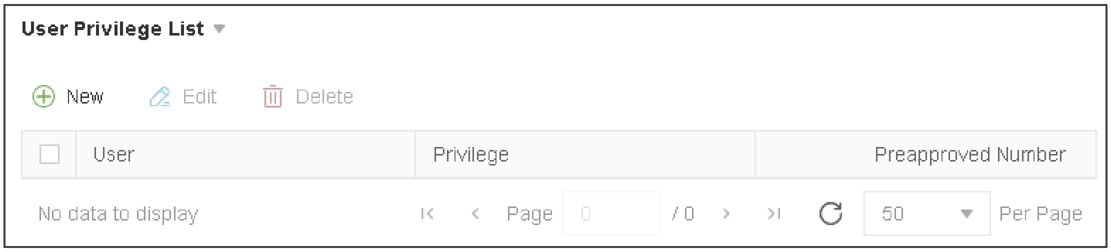
1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Compliance Binding page.
3. With the Binding and Unbinding tab active, select the entries you want to delete from the Host binding List.
4. Click **Unbinding** to remove the selected entries from this list.

Configuring a Super User

The super user won't be controlled by the host checking function, and can log into any host. To configure a super user, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.

3. With the User Privilege List tab active, click **New**.



In the New dialog box, configure the corresponding options.

Option	Description
User	Specifies the name of the user.
Super User	Select the **Enable** check box to make it a super user.
Preapproved Number	If system allows one user to login from multiple hosts, and the option of automatically adding the user-host ID entry into the host binding list at the first login is enabled, then by default system only records the user and first login host ID entry to the host binding list. For example, if the user logs in from other hosts, the user and host ID will be added to the host unbinding list. This pre-approved number specifies the maximum number of user-host ID entries for one user in the host binding list.

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

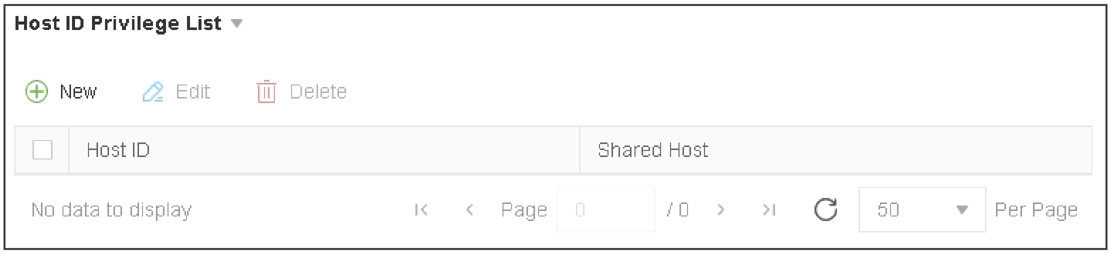
Configuring a Shared Host

Clients that log in from the shared host won't be controlled by the host binding list. To configure a shared host, take the following steps:

1. Select **Network > VPN > SSL VPN**.

2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.

3. With the Host ID Privilege List tab active, click **New**.



Host ID Privilege List ▾

⊕ New Edit Delete

□	Host ID	Shared Host

No data to display |‹ ‹ Page 0 / 0 › ›| ⟳ 50 ▾ Per Page

In the New dialog box, configure the corresponding options.

Option	Description
Host ID	Type the host ID into the Host ID box.
Shared Host	Select the **Enable** check to make it a shared host. By default, this check box is selected.

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

Importing/Exporting Host Binding List

To import the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.

2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.

3. With the Binding and Unbinding tab active, click **Import**.

4. Click **Browse** to find the binding list file and click **Upload**.

To export the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.

2. At the top right corner, click **Host Compliance Binding** to visit the Host Checking/Binding page.

3. With the Binding and Unbinding tab active, click **Export**.

4. Select a path to save the host binding list.

Host Compliance Check

The host compliance check function checks the security status of the hosts running SSL VPN clients, and according to the check result, the SSL VPN server will determine the security level for each host and assign corresponding resource access right based on their security level. It a way to assure the security of SSL VPN connection. The checked factors include the operating system, IE version, and the installation of some specific software.

The factors to be checked by the SSL VPN server are displayed in the list below:

Factor	Description
Operating system	• Operating system, e.g., Windows 2000, Windows 2003, Windows XP, Windows Vista, Windows 7m Windows 8, etc. • Service pack version, e.g., Service Pack 1 • Windows patch, e.g., KB958215, etc.
	• Whether the Windows Security Center and Automatic Updates are enabled. • Whether the installation of AV software is compulsory, and whether the real-time monitor and the auto update of the signature database are enabled. • Whether the installation of anti-spyware is compulsory, and whether the real-time monitor and the online update of the signature database are enabled. • Whether the personal firewall is installed, and whether the real-time protection is enabled.
	Whether the IE version and security level reach the specified requirements.

Factor	Description
Other configurations	Whether the specified processes are running.
	Whether the specified services are installed.
	Whether the specified services are running.
	Whether the specified registry key values exist.
	Whether the specified files exist in the system.

Role Based Access Control and Host Compliance Check Procedure

Role Based Access Control (RBAC) means that the permission of the user is not determined by his user name, but his role. The resources can be accessed by a user after the login is determined by his corresponding role. So role is the bridge connecting the user and permission.

The SSL VPN host checking function supports RBAC. And the concepts of primary role and guest role are introduced in the host checking procedure. The primary role determines which host compliance check profile (contains the host checking contents and the security level) will be applied to the user and what access permission can the user have if he passes the host checking. The guest role determines the access permissions for the users who fail the host checking.

The host compliance check procedure is shown as below

1. The SSL VPN client sends request for connection and passes the authentication.
2. The SSL VPN server sends the host checking profile to the client.
3. The client checks the host security status according to the items in the host checking profile. If it fails the host compliance check, system will be notified of the checking result.
4. The client sends the checking result back to the server.
5. The server disconnects the connection to the failed client or gives the guest role's access permission to the failed client.

The host compliance check function also supports dynamic access permission control. On one side, when the client's security status changes, the server will send a new host checking profile to the client to make him re-check; on the other side, the client can perform security checks periodically. For example, if the AV software is disabled and is detected by the host checking function, the role assigned to the client may change as will the access permissions.

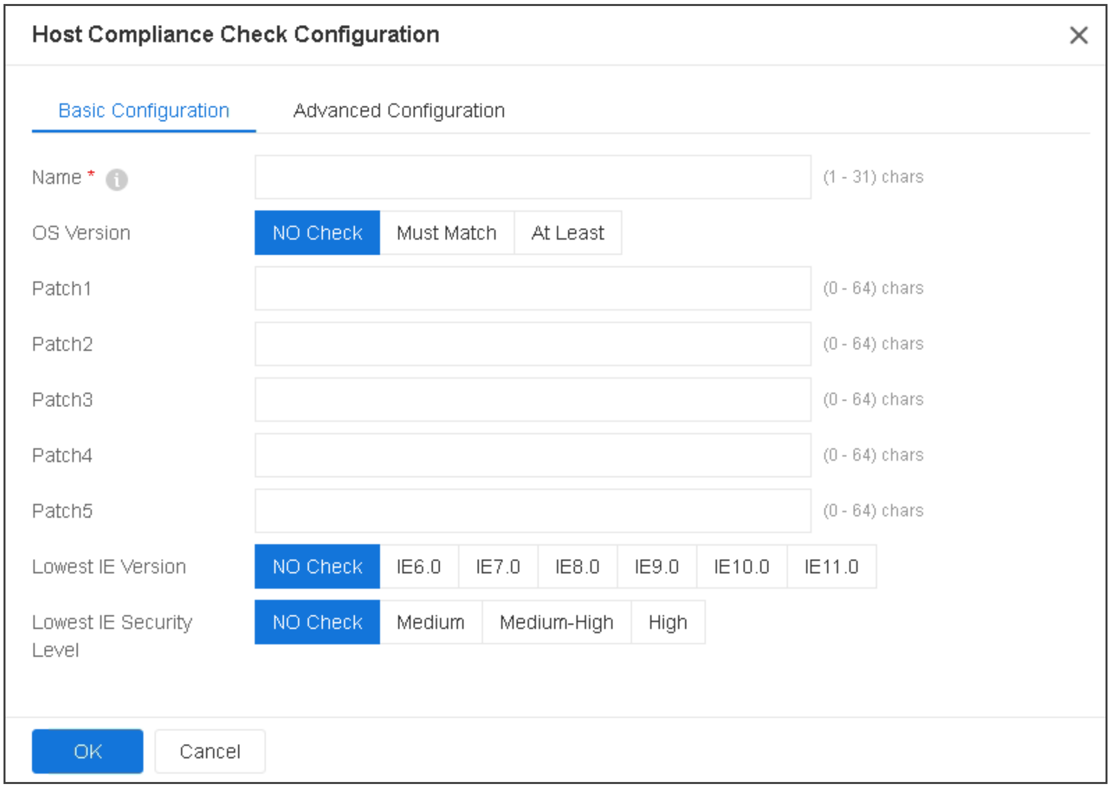
Configuring a Host Compliance Check Profile

To configuring host compliance check profile, take the following steps:

1. Select **Network** > **VPN** > **SSL VPN**.

2. At the top right corner, click **Configuration** ,select **Host Compliance Check** from the drop-down list to visit the Host Compliance Check page.

3. In the Host Compliance Check tab, click **New** to create a new host checking rule.



In the Basic Configuration tab, configure the corresponding options.

Option	Description
Name	Specifies the name of the host checking profile.
OS Version	Specifies whether to check the OS version on the client host. Click one of the following options: • No Check: Do not check the OS version. • Must Match: The OS version running on the client host must be the same as the version specified here. Select the OS version and service pack version from the drop-down lists respectively. • At Least: The OS version running on the client host should not be lower than the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
Patch1/2/3/4/5	Specifies the patch that must be installed on the client host. Type the patch name into the box. Up to 5 patches can be specified.
Lowest IE Version	Specifies the lowest IE version in the Internet zone on the client host. The IE version running on the client host should not be lower than the version specified here.
Lowest IE Security Level	Specifies the lowest IE security level on the client host. The IE security level on the host should not be lower than the level specified here.

In the Advanced Configuration tab, configure the corresponding options.

Option	Description
Security Center	Checks whether the security center is enabled on the client host.
Auto Update	Checks whether the Windows auto update function is enabled.
Anti-Virus Software	Checks the status and configurations of the antivirus software: • Installed: The client host must have the AV software installed. • Monitor: The client host must enable the real-time monitor of the AV software. • Virus Signature DB Update: The client host must enable the signature database online update function.
Anti-Spyware Software	Checks the status and configurations of the antispyware software: • Installed: The client host must have the anti-spyware installed. • Monitor: The client host must enable the real-time monitor of the anti-spyware. • Signature DB Update: The client host must enable the signature database online update function.
Firewall	Checks the status and configurations of the fire-

	wall: - Installed: The client host must have the personal firewall installed. - Monitor: The client host must enable the real-time monitor function of the personal firewall.
Registry Key Value	
Key1/2/3/4/5	Checks whether the key value exists. Up to 5 key values can be configured. The check types are: - No Check: Do not check the key value. - Exist: The client host must have the key value. Type the value into the box. - Do not Exist: The client cannot have the key value. Type the value into the box.
File Path Name	
File1/2/3/4/5	Checks whether the file exists. Up to 5 files can be configured. The check types are: - No Check: Do not check file. - Exist: The client host must have the file. Type the value into the box. - Do not Exist: The client cannot have the file. Type the value into the box.

Name of Running Process	
Process1/2/3/4/5	Checks whether the process is running. Up to 5 processes can be configured. The check types are: • No Check: Do not check the process. • Exist: The client host must have the process run. Type the process name into the box. • Do not Exist: The client cannot have the process run. Type the process name into the box.
Name of Installed Service	
Service1/2/3/4/5	Checks whether the service is installed. Up to 5 services can be configured. The check types are: • No Check: Do not check the service. • Exist: The client host must have the service installed. Type the service name into the box. • Do not Exist: The client host cannot have the service installed. Type the service name into the box.
Name of Running Service	
Service1/2/3/4/5	Checks whether the service is running. Up to 5

	services can be configured. The check types are: • No Check: Do not check the service. • Exist: The client host must have the service run. Type the service name into the box. • Do not Exist: The client host cannot have the service run. Type the service name into the box.

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

SSL VPN Client for Windows

SSL VPN client for Windows is named Hillstone Secure Connect. Hillstone Secure Connect can be run with the following operating systems: Windows 2000/2003/XP/Vista/Windows 7/Windows 8/Windows 2008/Windows 10/Windows 2012. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server after a connection has been established successfully. The functions of the client are:

- Get the interface and the route information of the PC on which the client is running.
- Show the connecting status, statistics, interface information, and route information.
- Show SSL VPN log messages.
- Upgrade the client software.
- Resolve the resource list information received from the server.

This section mainly describes how to download, install, start, uninstall the SSL VPN client, and its GUI and menu. The method for downloading, installing and starting the client may vary from the authentication methods configured on the server. The SSL VPN server supports the following authentication methods:

- Username/Password
- Username/Password + Digital Certificate
- Digital Certificate only

Downloading and Installing Secure Connect

When using the SSL VPN client for the first time, you need to download and install the client software Hillstone Secure Connect. This section describes three methods for downloading and installing the client software based on three available authentication methods. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

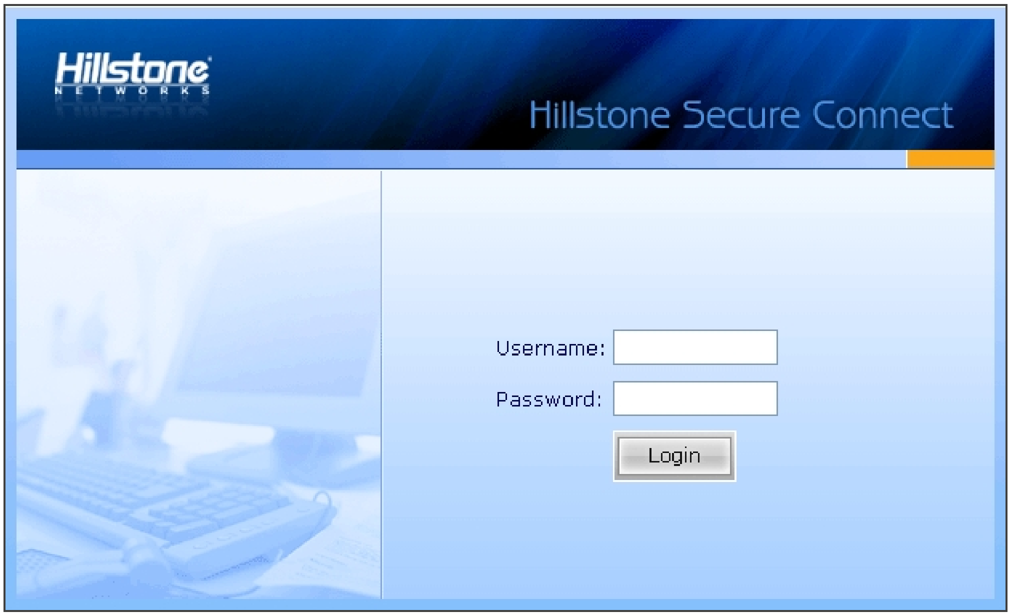
1. Visit the following URL with a web browser: https://IP-Address:Port-Number. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN instance.

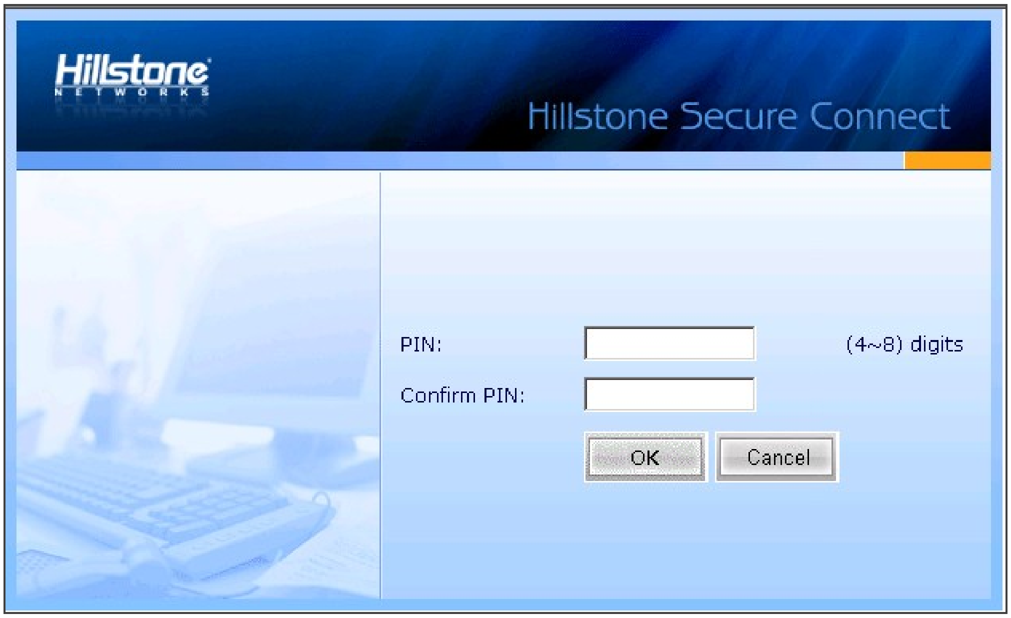
2. In the SSL VPN login page (shown in Figure 1), type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**.

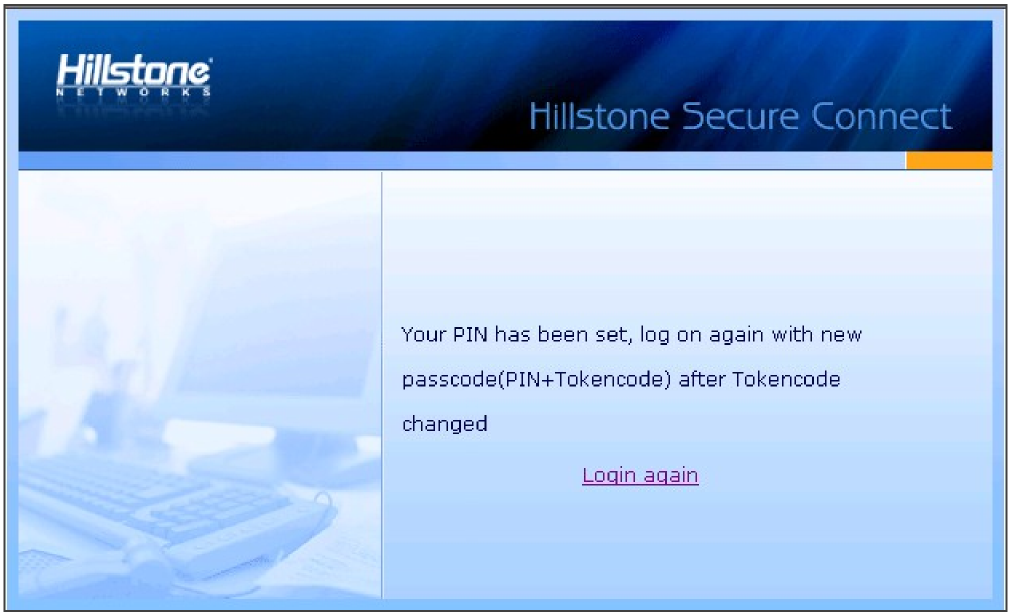
   - If the local authentication server is configured on the device, the username and password should already be configured on the device.

   - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 2), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 3). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.

   - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.


Hillstone NETWORKS
Hillstone Secure Connect
Username:
Password:
Login


Hillstone NETWORKS
Hillstone Secure Connect
PIN:
(4~8) digits
Confirm PIN:
OK
Cancel



Your PIN has been set, log on again with new passcode(PIN+Tokencode) after Tokencode changed

3. If SMS authentication is enabled on the SSL VPN server, the SMS Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

4. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

5. If Email authentication is enabled on the SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

    - 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.

6. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Using Username/Password + Digital Certificate Authentication

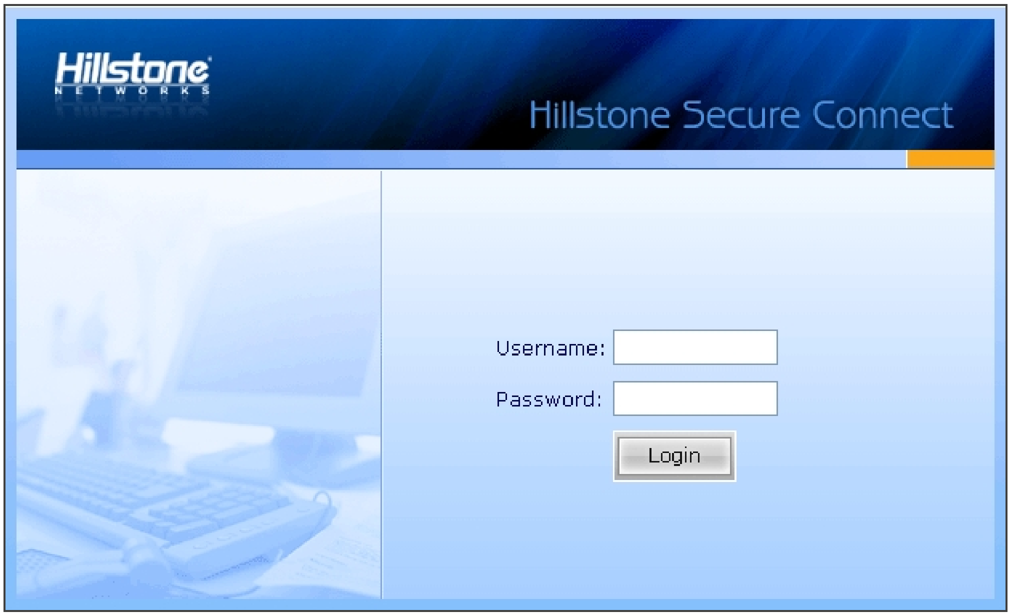
When the Username/Password + Digital Certificate authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

1. Insert the USB Key to the USB port of the PC, or import the file certificate provided by the administrator manually.

2. Visit the following URL with a web browser: https://IP-Address:Port-Number. 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 instance.

3. In the Select Digital Certificate dialog box, select the certificate you want and click **OK**. If USB Key certificate is selected, in the pop-up dialog box, provide the UKey PIN code (1111 by default) and click **OK**.

4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should be configured before in the device.



5. If SMS authentication is enabled on the SSL VPN server, the SMS Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.
   - 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 SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.
   - 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.

8. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Using Digital Certificate Only

When only the Digital Certificate authentication is configured on the server, take the following steps to download and install the SSL VPN client software - Hillstone Secure Connect:

1. Insert the USB Key to the USB port of the PC, or import the file certificate provided by the administrator manually.

2. Visit the following URL with a web browser: https://IP-Address:Port-Number. 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 instance.

3. In the Select Digital Certificate dialog box, select the certificate you want and click **OK**. If USB Key certificate is selected, in the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.

4. After logging in, IE will download the client software automatically, and you can install it by following the prompts; for other web browsers, e.g., Firefox, you should click **Download** to download the client software scvpn.exe first, and then double click it to install.

A virtual network adapter will be installed on your PC together with Secure Connect. It is used to transmit encrypted data between the SSL VPN server and client.

Starting Secure Connect

After installing Secure Connect on your PC, you can start it in two ways:

- Starting via Web

- Starting directly

Starting via Web

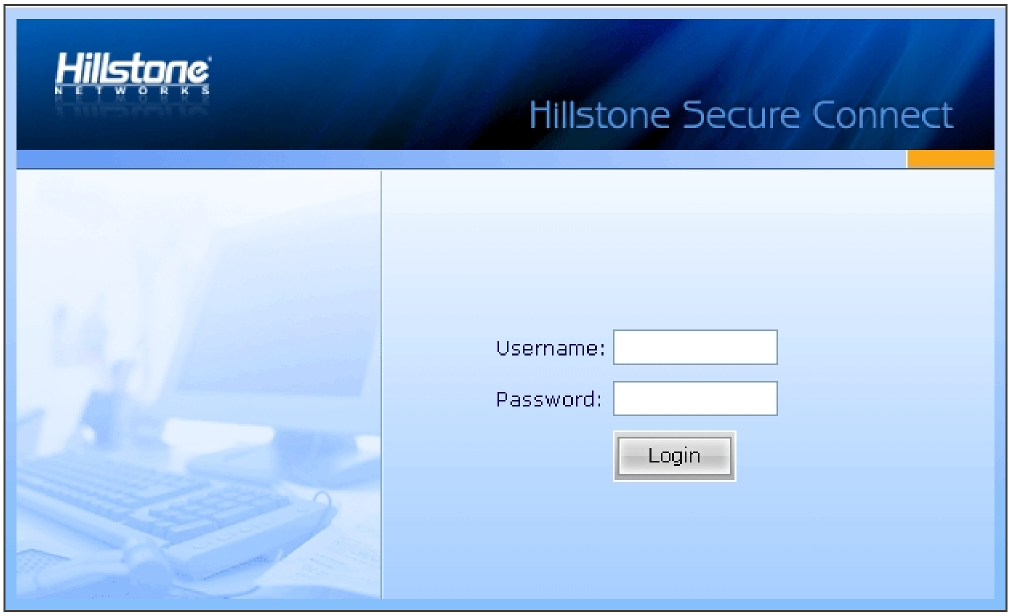
This section describes how to start Secure Connect via Web based on the three authentication methods configured on the server. For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

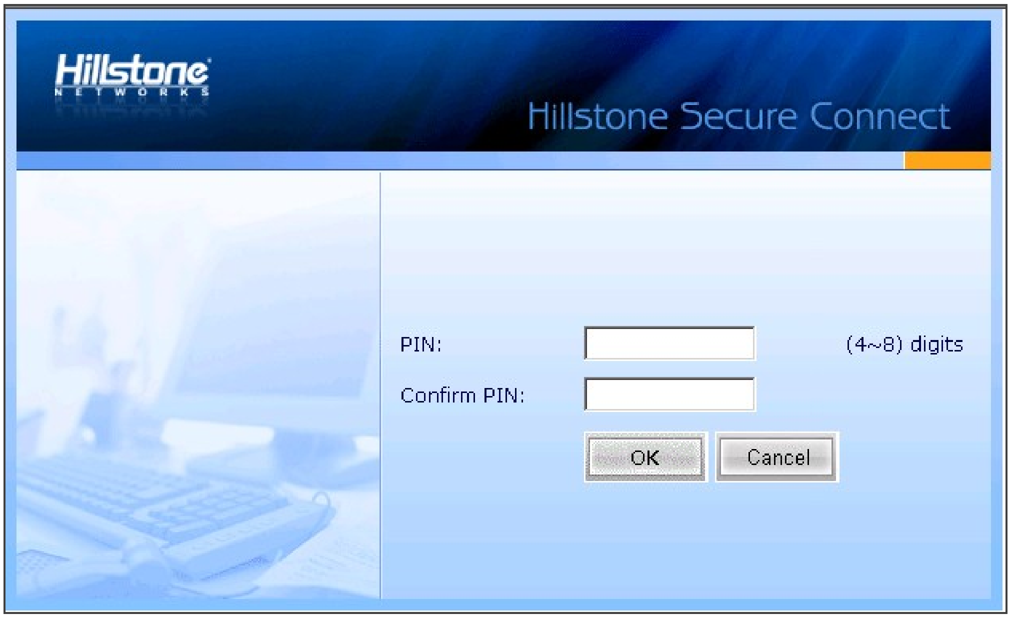
Using Username/Password Authentication

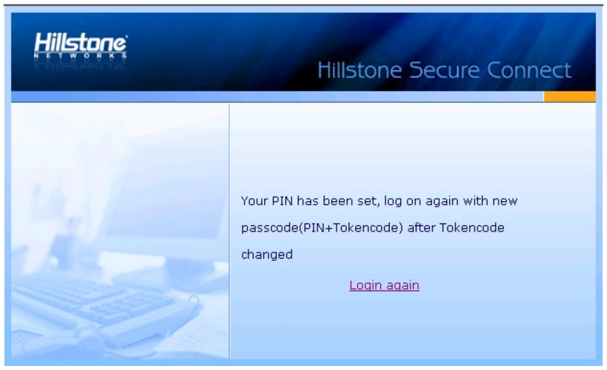
When the Username/Password authentication is configured on the server, take the following steps to start Secure Connect via web:

1. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.
2. In the login page (shown in Figure 4), type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**.
    - If local authentication server is configured on the device, the username and password should be configured before on the device;
    - If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 5), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 6). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.

- If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.







Your PIN has been set, log on again with new passcode(PIN+Tokencode) after Tokencode changed

Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. If SMS authentication is enabled on the SSL VPN server, the SMS Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

    - 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.

4. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

5. If Email authentication is enabled on the SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (H) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using Username/Password + USB Key Certificate Authentication

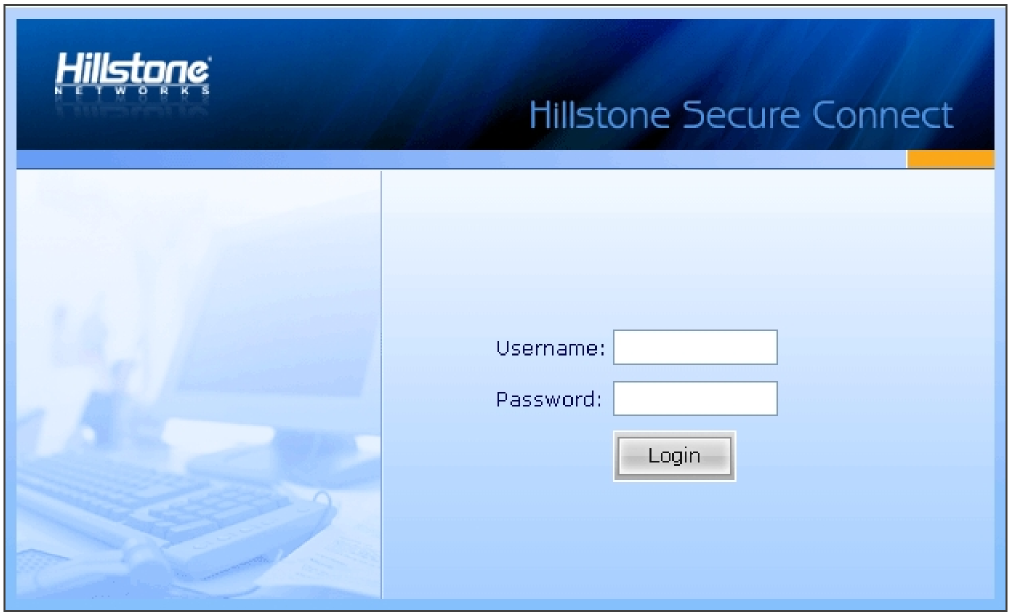
When the Username/Password + Digital Certificate authentication for the USB Key certificate is configured on the server, to start Secure Connect via web, take the following steps:

1. Insert the USB Key to the USB port of the PC.

2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.

3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**. In the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.

4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should already be configured on the device.



5. If the SMS authentication function is enabled, type the SMS authentication code into the box, and then click **Authenticate**. If you have not received the code within one minute, you can re-apply.

   - 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.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

    - 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.

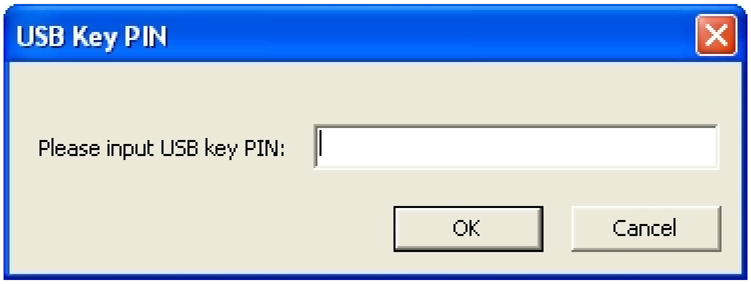
    - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

7. If Email authentication is enabled on the SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

    - 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.

8. In the USB Key PIN dialog box shown below, type the UKey PIN (1111 by default), and click **OK**.



USB Key PIN

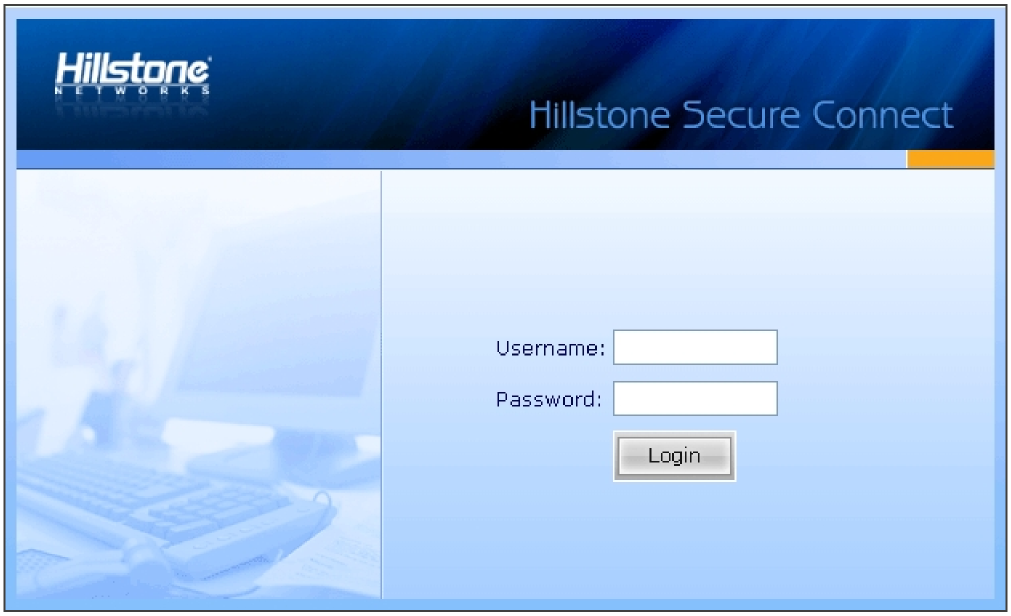
Please input USB key PIN:

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using Username/Password + File Certificate Authentication

When the Username/Password + Digital Certificate authentication for the file certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Import the file certificate provided by the administrator manually.
2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.
3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**.
4. In the SSL VPN login page shown below, type the username and password into the **Username** and **Password** boxes respectively, and then click **Login**. The login user should already be configured on the device.



5. If the SMS authentication function is enabled, type the SMS authentication code into the box, and then click **Authenticate**. If you have not received the code within one minute, you can re-apply.

   - 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.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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 SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (H) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using USB Key Certificate Only Authentication

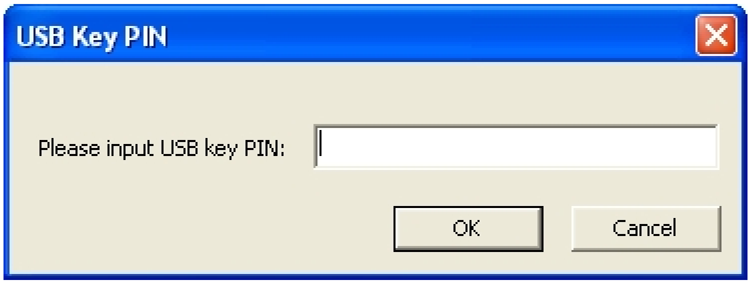
When the Digital Certificate only authentication for the USB Key certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Insert the USB Key to the USB port of the PC.

2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.

3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**. In the Enter Password dialog box, provide the UKey user password (1111 by default) and click **OK**.

4. In the USB Key PIN dialog box shown below, type the UKey PIN (1111 by default), and click **OK**.



After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using File Certificate Only Authentication

When the Digital Certificate only authentication for the file certificate is configured on the server, to start the Secure Connect via web, take the following steps:

1. Import the file certificate provided by the administrator manually.

2. Type the URL https://IP-Address:Port-Number into the address bar of your web browser.

3. In the Select Digital Certificate dialog box, select the digital certificate you want and click **OK**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Starting Directly

This section describes how to start Secure Connect directly based on the three authentication methods configured on the server.

Starting the Software Based on TLS/SSL Protocol

For the Username/Password + Digital Certificate authentication, the digital certificate can either be the USB Key certificate provided by the vendor, or the file certificate provided by the administrator.

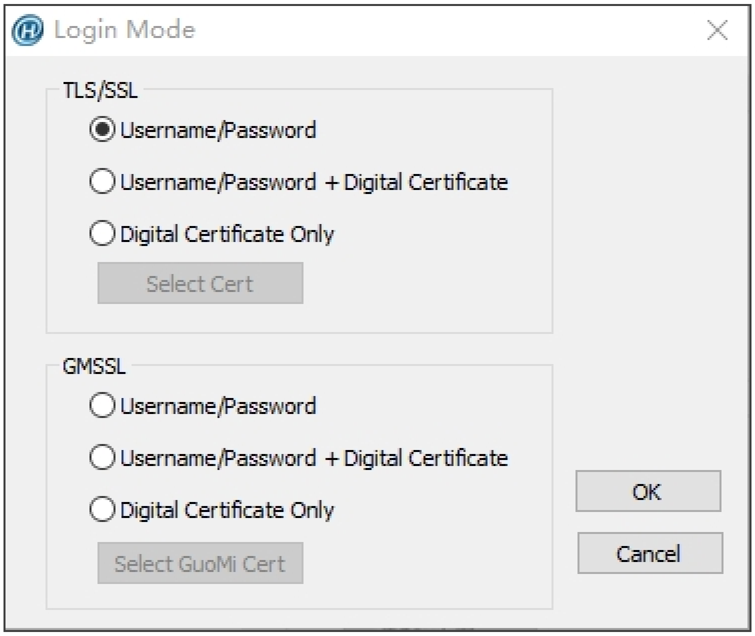
The starting mode based on TLS/SSL protocol are as follows:

- Username/Password
- Username/Password + USB Key Certificate
- Username/Password + File Certificate
- USB Key Certificate Only
- File Certificate Only

Using Username/Password Authentication

When the Username/Password authentication is configured on the server, to start the Secure Connect directly, take the following steps:

1. On your PC, double click the shortcut of Hillstone Secure Connect on your desktop.
2. In the Login dialog box, click **Mode**. In the Login Mode dialog shown below, in **TLS/SSL** section, click **Username/Password**, and then click **OK**.


Login Mode
TLS/SSL
● Username/Password
○ Username/Password + Digital Certificate
○ Digital Certificate Only
Select Cert
GMSSL
○ Username/Password
○ Username/Password + Digital Certificate
○ Digital Certificate Only
Select GuoMi Cert
OK
Cancel

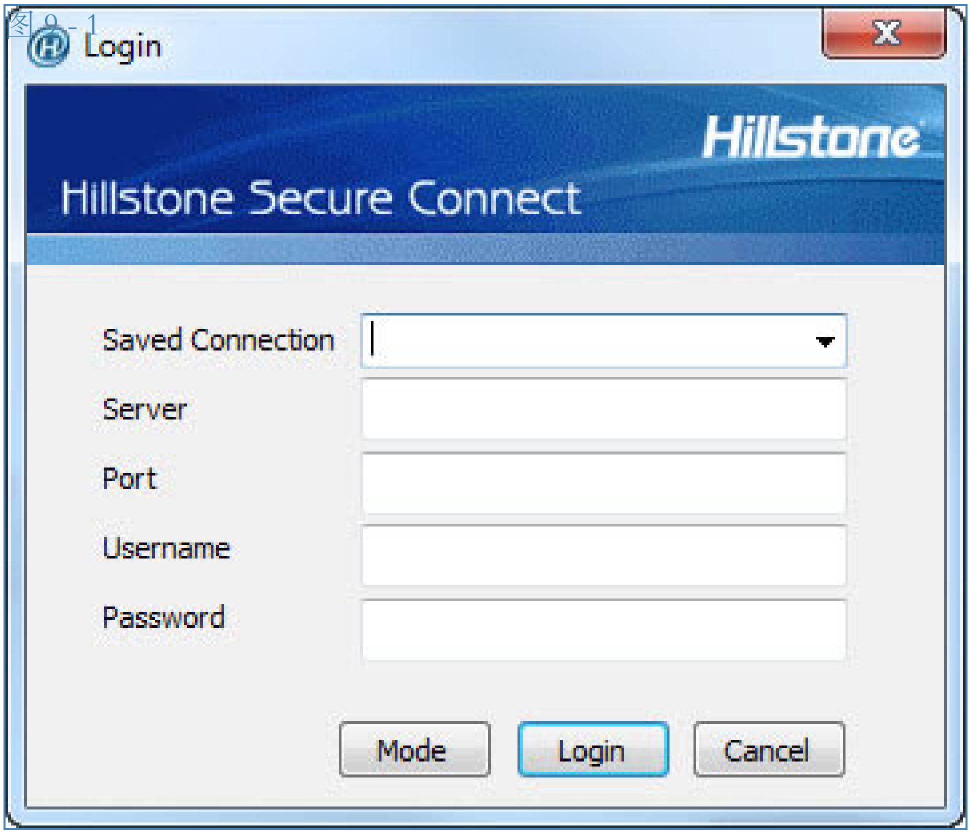
3. In the Login dialog box of the Username/Password authentication mode (shown in Figure 7), configure the options to login.

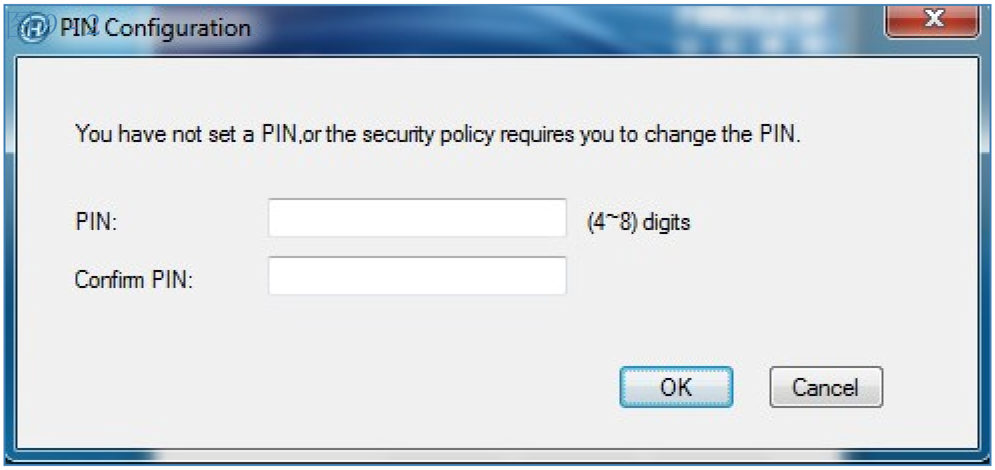
Option	Description
Saved Connection	Provides the connection information you have filled before. Select a connection from the drop-down list.
Server	Enter the IP address of SSL VPN server.
Port	Enter the HTTPS port number of SSL VPN server.
Username	Enter the name of the login user.
Password	Enter the password of the login user.

- If the local authentication server is configured on the device, the username and password should already be configured on the device.

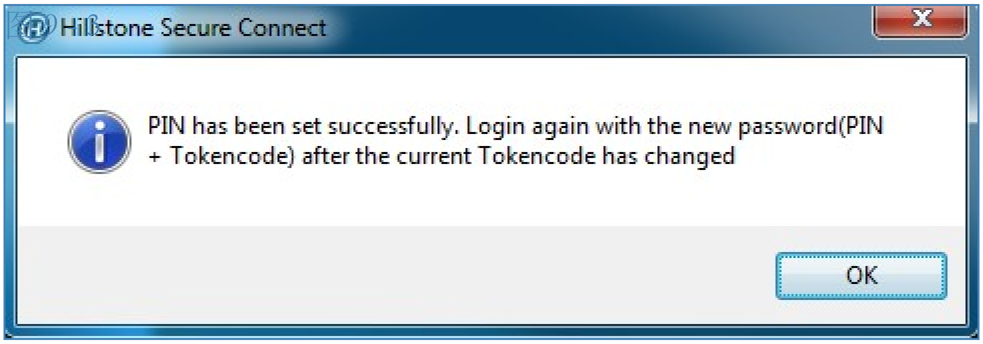
- If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, and the user logs in for the first time, the username should be the username configured on the Radius server, and the password should be the dynamic Token password bound to the user. Click **Login**, and in the PIN Setting page (shown in Figure 8), set a PIN (4 to 8 digits). After the PIN has been set successfully, you will be prompted to login again with the new password (shown in Figure 9). Click **Login again** to return to the login page, type the correct username and new password, and click **Login**. The new password is PIN + dynamic Token password. For example, if the PIN is set to 54321, and the dynamic Token password is 808771, then the new password is 54321808771.

- If "Radius authentication + RSA SecurID Token authentication by RSA Server" is configured on the device, but the user is not logging in for the first time, the username should be the username configured on the Radius server, and the password should be PIN + dynamic Token password.





You have not set a PIN,or the security policy requires you to change the PIN.

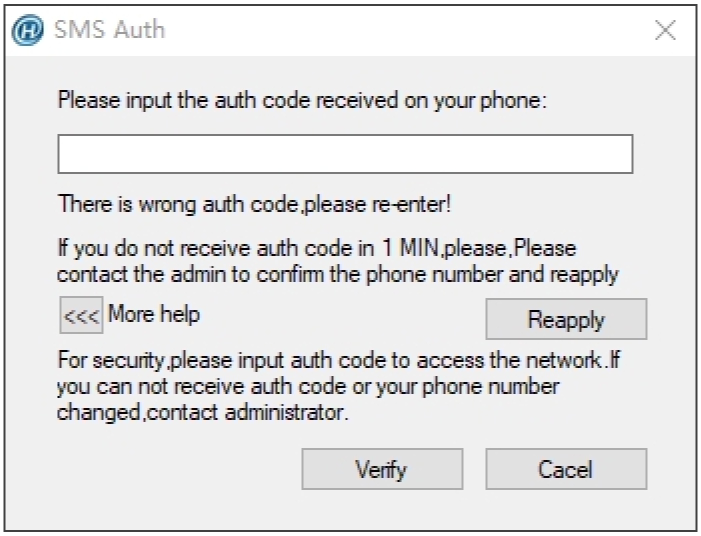


Hillstone Secure Connect

PIN has been set successfully. Login again with the new password(PIN + Tokencode) after the current Tokencode has changed

Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

4. Click **Login**. 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 **Reapply**.



SMS Auth

Please input the auth code received on your phone:

There is wrong auth code,please re-enter!

If you do not receive auth code in 1 MIN,please,Please contact the admin to confirm the phone number and reapply

For security,please input auth code to access the network.If you can not receive auth code or your phone number changed,contact administrator.

5. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - 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.

6. If Email authentication is enabled on the SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

   - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.

   - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. And the encrypted communication between the client and server can be implemented now.

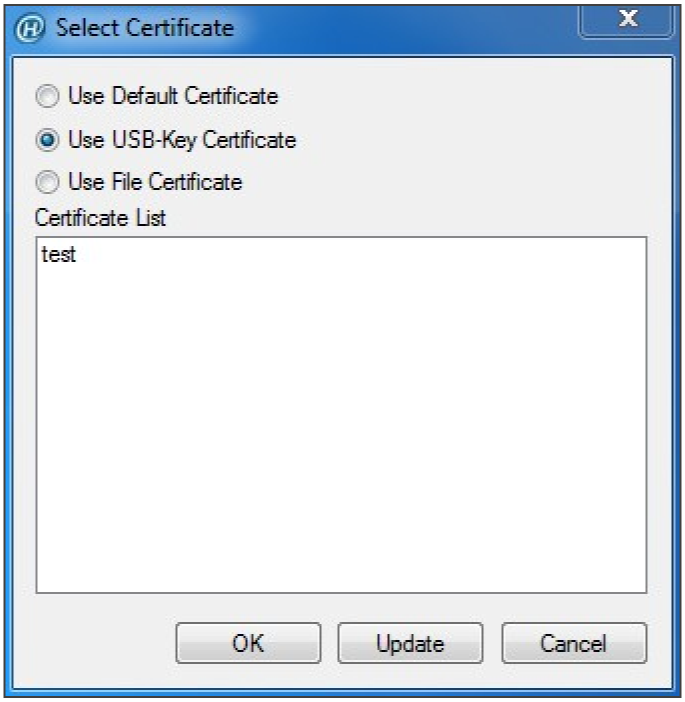
Using Username/Password + USB Key Certificate Authentication

When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, to start Secure Connect directly, take the following steps:

1. Insert the USB Key to the USB port of the PC.

2. In your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **User-name/Password + Digital Certificate** in **TLS/SSL** section, and if necessary, click **Select Cert**. In the Select Certificate dialog box shown below, select a USB Key certificate. If the USB Key certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.

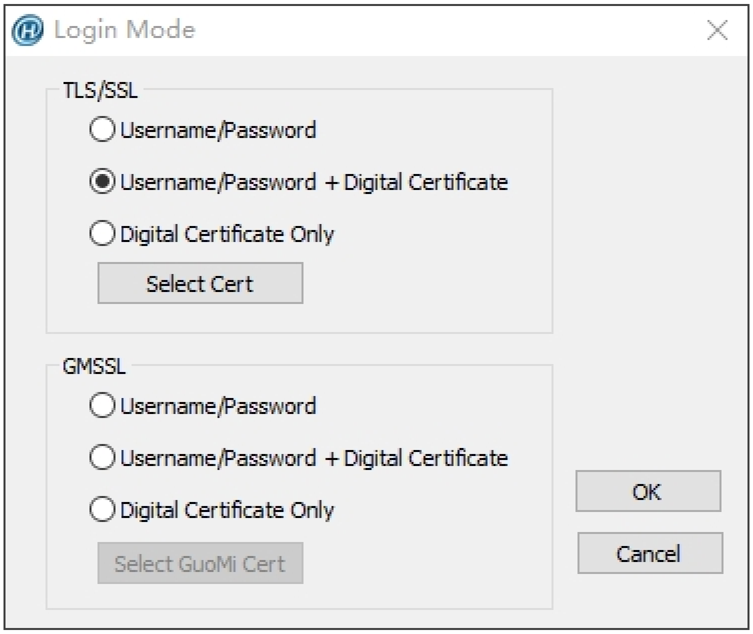


○ Use Default Certificate
● Use USB-Key Certificate
○ Use File Certificate

Certificate List

test

4. In the Login dialog of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



TLS/SSL

○ Username/Password

● Username/Password + Digital Certificate

○ Digital Certificate Only

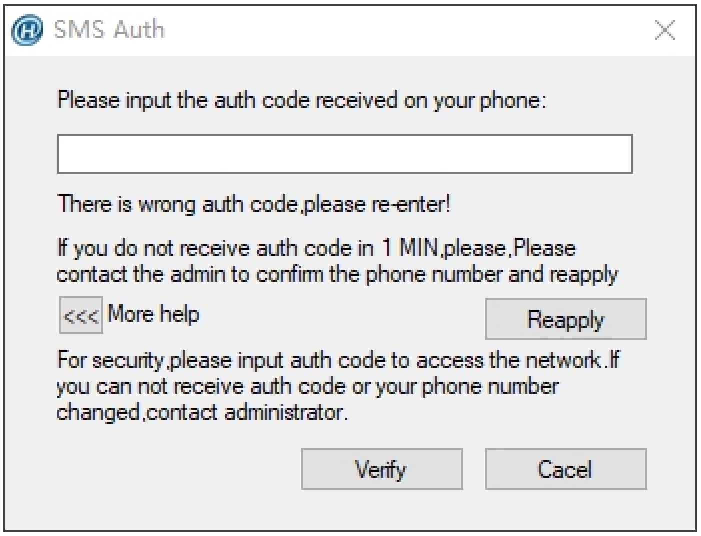
GMSSL

○ Username/Password

○ Username/Password + Digital Certificate

○ Digital Certificate Only

5. Click **Login**. 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 **Reapply**.



Please input the auth code received on your phone:

There is wrong auth code,please re-enter!

If you do not receive auth code in 1 MIN,please,Please contact the admin to confirm the phone number and reapply

For security,please input auth code to access the network.If you can not receive auth code or your phone number changed,contact administrator.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

- 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 SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.
    - 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.

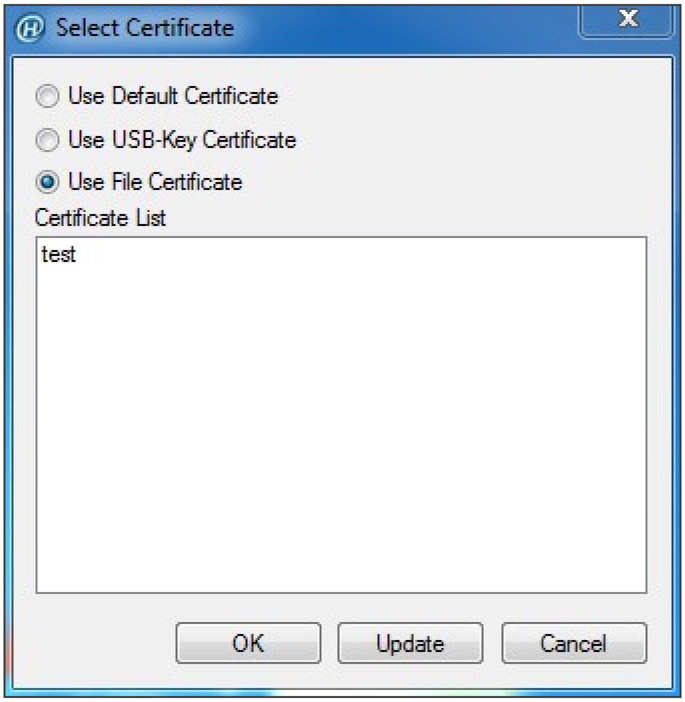
After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using Username/Password + File Certificate Authentication

When the Username/Password + Digital Certificate authentication for the USB Key certificate is configured on the server, to start the Secure Connect directly, take the following steps:

1. Import the file certificate provided by the administrator manually.
2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog box, click **Mode**. In the Login Mode dialog, first click **Username/Password + Digital Certificate**in **TLS/SSL** section, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a file certificate. If the file certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.



Select Certificate

○ Use Default Certificate

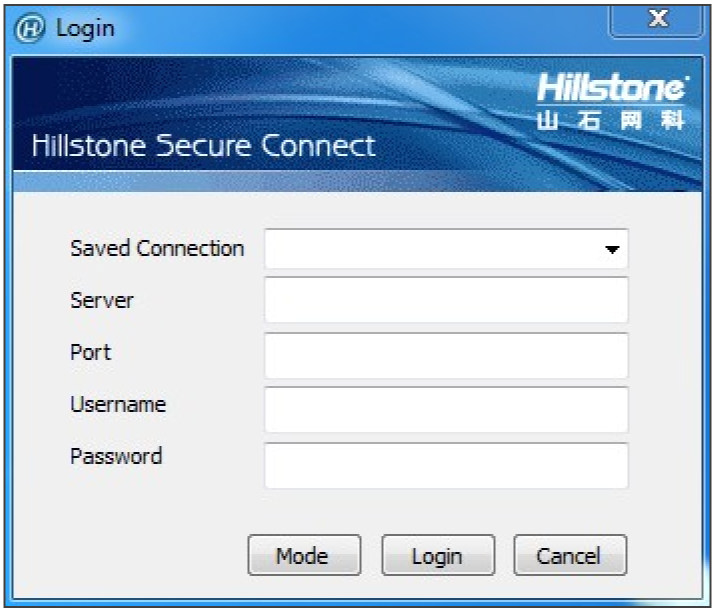
○ Use USB-Key Certificate

● Use File Certificate

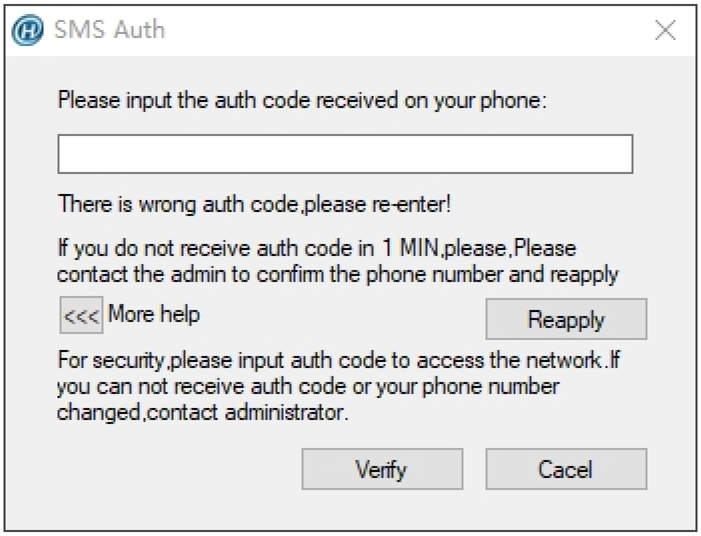
Certificate List

test

4. In the Login dialog box of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



5. Click **Login**. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog box(as shown below) and click **Verify**. If you have not received the authentication code in one minute, you can re-apply by clicking **Reapply**.



Please input the auth code received on your phone:

There is wrong auth code,please re-enter!

If you do not receive auth code in 1 MIN,please,Please contact the admin to confirm the phone number and reapply

For security,please input auth code to access the network.If you can not receive auth code or your phone number changed,contact administrator.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.

- 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 SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Authenticate. If you have not received the authentication code within one minute, you can re-apply.
    - 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.

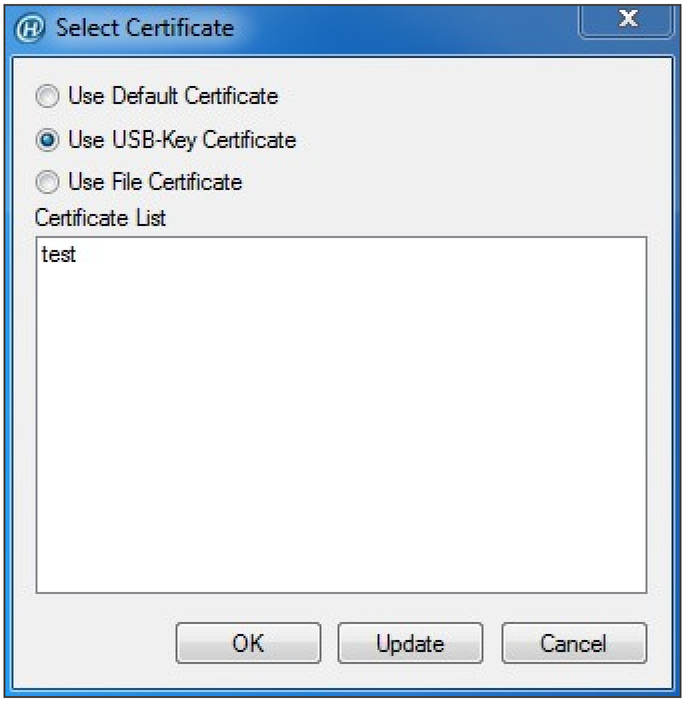
After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (H) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Using USB Key Certificate Only

When the Username/Password + Digital Certificate authentication for the file certificate is configured on the server, to start the Secure Connect directly, take the following steps:

1. Insert the USB Key to the USB port of the PC.
2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **Username/Password + Digital Certificate** in **TLS/SSL** section, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a USB Key certificate. If the USB Key certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.



Select Certificate

○ Use Default Certificate

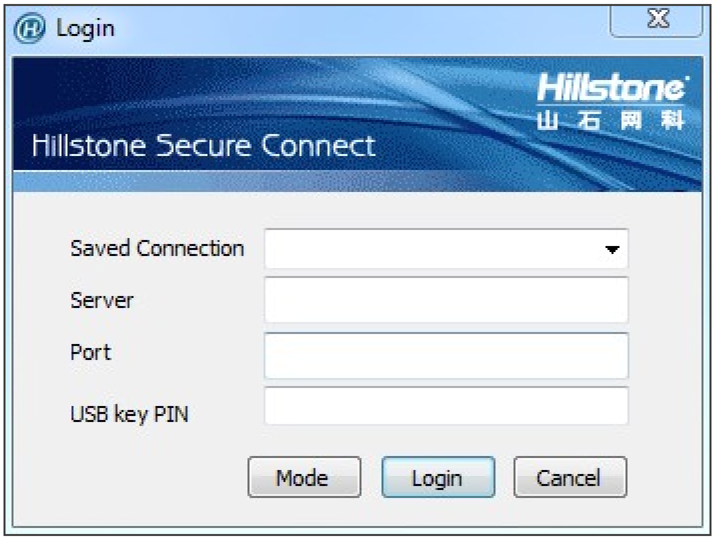
● Use USB-Key Certificate

○ Use File Certificate

Certificate List

test

4. In the Login dialog box of the Username/Password + Digital Certificate authentication mode (as shown below), configure the options to login.



5. Finishing the above configuration, click **Login**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

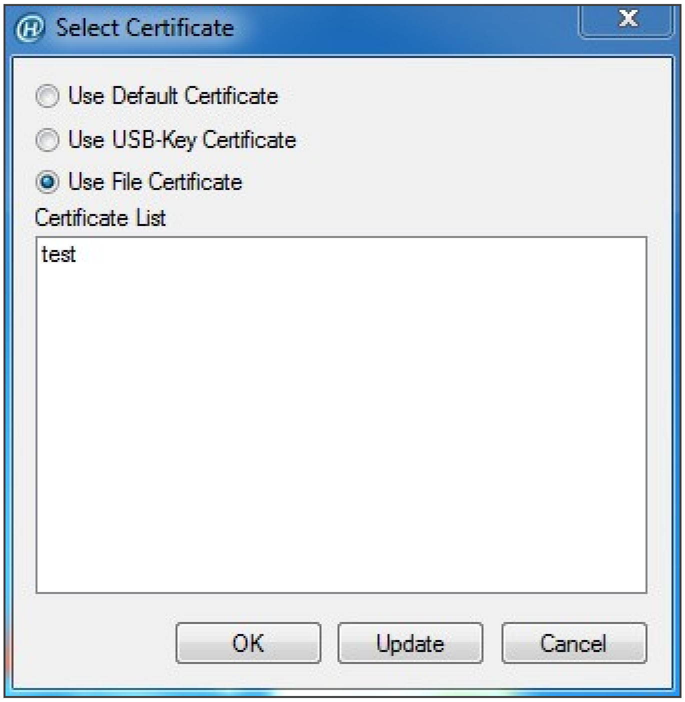
Using File Certificate Only

When the Digital Certificate Only authentication for the USB Key certificate is configured on the server, to start the Secure Connect directly, take the following steps:

1. Import the file certificate provided by the administrator manually.

2. On your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog box, click **Mode**. In the Login Mode dialog box, first click **Username/Password + Digital Certificate** in **TLS/SSL** section, and if necessary, click **Select Certificate**. In the Select Certificate dialog box shown below, select a file certificate. If the file certificate is not listed, click **Update**. The client will send the selected certificate to the server for authentication. Finally click **OK**.



Select Certificate

○ Use Default Certificate

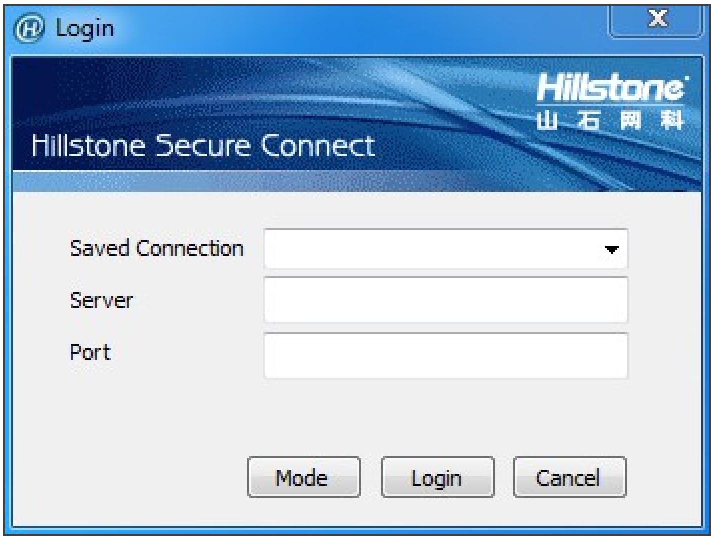
○ Use USB-Key Certificate

● Use File Certificate

Certificate List

test

4. In the Login dialog box of the Digital Certificate Only authentication mode (as shown below), configure the options to login.



Login

Hillstone Secure Connect

Saved Connection:

Server:

Port:

5. Finishing the above configuration, click **Login**.

After the above steps being finished, the client will connect to the server automatically. After the connection has been established successfully, the icon (Ⓗ) will be displayed in the notification area. The encrypted communication between the client and server can be implemented now.

Starting the Software Based on GMSSL Protocol

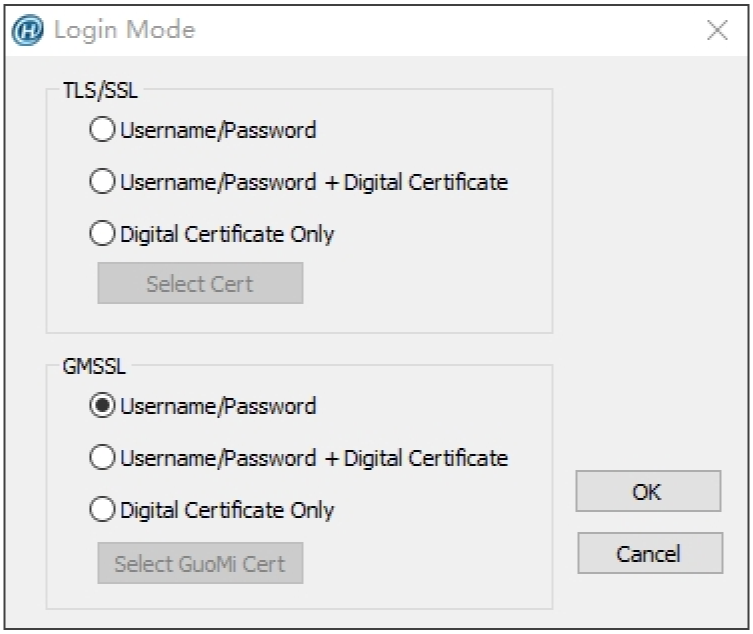
The starting mode based on GMSSL protocol are as follows:

- Username/Password
- Username/Password + Digital Certificate
- Digital Certificate Only

Using Username/Password Authentication

To start the Secure Connect client software, take the following steps:

1. On your PC, double click the shortcut of Hillstone Secure Connect on your desktop.
2. In the Login dialog box, click **Mode**. In the Login Mode dialog shown below, click **Username/Password** in **GMSSL** section,, and then click **OK**.



Login Mode

TLS/SSL

○ Username/Password

○ Username/Password + Digital Certificate

○ Digital Certificate Only

Select Cert

GMSSL

● Username/Password

○ Username/Password + Digital Certificate

○ Digital Certificate Only

Select GuoMi Cert

OK

Cancel

3. In the Login dialog box of the Username/Password authentication mode, configure the options to login.

Option	Description
Saved Connection	Provides the connection information you have filled before. Select a connection from the drop-down list.
Server	Enter the IP address of SSL VPN server.
Port	Enter the HTTPS port number of SSL VPN server.
Username	Enter the name of the login user.
Password	Enter the password of the login user.

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.

Using Username/Password + Digital Certificate Authentication

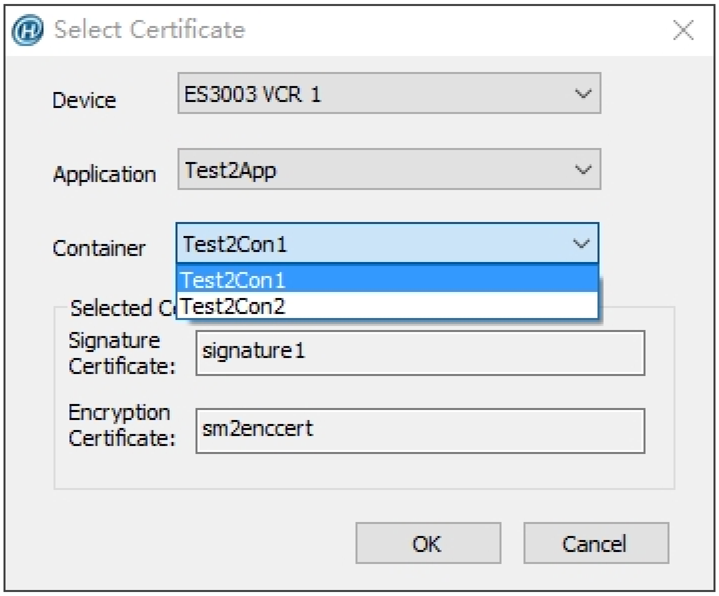
When the Username/Password + Digital Certificate authentication is configured on the server, for the USB Key certificate, to start the Secure Connect software directly, take the following steps:

1. Insert the USB Token to the USB port of the PC.

2. In your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Username/Password + Digital Certificate** in **GMSSL** section, and if necessary, click **Select GuoMi Cert**. In the

Select Certificate dialog as shown below, select a GM certificate. Finally click **OK**.



Select Certificate

Device: ES3003 VCR 1

Application: Test2App

Container: Test2Con1

Test2Con1
Test2Con2

Selected C

Signature Certificate: signature1

Encryption Certificate: sm2enccert

4. In the Select Certificate dialog box, configure the options to login.

Option	Description
Device	Select the current USB Token device name in the drop-down list.
Application	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	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.

Option	Description
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.

5. In the Login dialog of the Username/Password + Digital Certificate authentication mode as shown below, configure the options to login.

Option	Description
Saved Connection	Provides the connection information you have filled before. Select a connection from the drop-down list.
Server	Enter the IP address of SSL VPN server.
Port	Enter the HTTPS port number of SSL VPN server.
Username	Enter the name of the login user.
Password	Enter the password of the login user.
USB Key PIN	Enter the PIN code of the USB Key (1111 by default). One USB Key only corresponds to one password.

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.

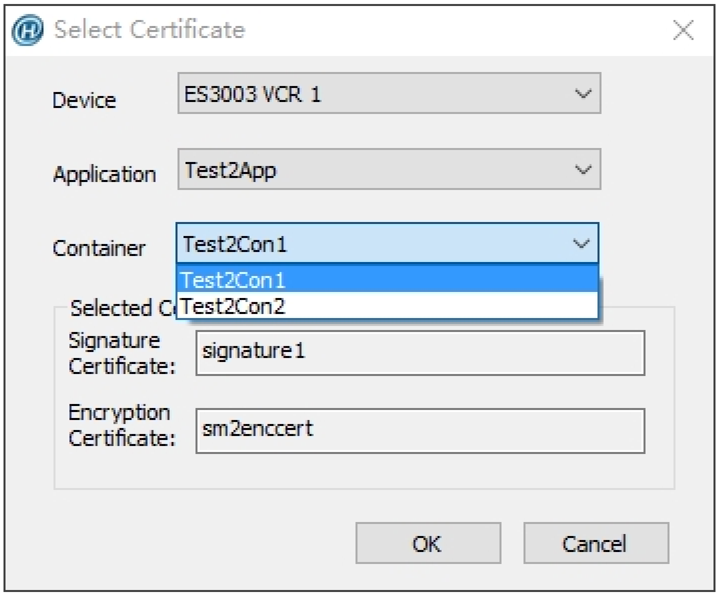
Using Digital Certificate Only Authentication

When the Digital Certificate Only authentication is configured on the server, for the file certificate, to start the Secure Connect software directly, take the following steps:

1. Insert the USB Token to the USB port of the PC.

2. In your PC, double click the shortcut to Hillstone Secure Connect on your desktop.

3. In the Login dialog, click **Mode**. In the Login Mode dialog, first click **Digital Certificate only** in **GMSSL** section, and if necessary, click **Select GuoMi Cert**. In the Select Certificate dialog as shown below, select a GM certificate. Finally click **OK**.



Select Certificate

Device: ES3003 VCR 1

Application: Test2App

Container: Test2Con1

Test2Con1
Test2Con2

Signature Certificate: signature1

Encryption Certificate: sm2enccert

4. In the Select Certificate dialog box, configure the options to login.

Option	Description
Device	Select the current USB Token device name in the drop-down list.
Application	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	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 cor-

Option	Description
	responding 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.

5. In the Login dialog of the Digital Certificate Only authentication mode as shown below, configure the options to login.

Option	Description
Saved Connection	Provides the connection information you have filled before. Select a connection from the drop-down list.
Server	Enter the IP address of SSL VPN server.
Port	Enter the HTTPS port number of SSL VPN server.
USB Key PIN	Enter the PIN code of the USB Key (1111 by default). One USB Key only corresponds to one password.

6. Finish the above configuration, click **Login**.

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.

Viewing Secure Connect GUI

Double click the Secure Connect icon (Ⓗ) in the notification area, and the Network Information dialog box appears. This dialog box shows information about statistics, interfaces, and routes.

General

Descriptions of the options on the General tab:

Address Information	
Server	The IP address of the connected SSL VPN server.
Client	The IP address of the client.
Crypto Suite	
Cipher	The encryption algorithm and authentication algorithm used by SSL VPN.
Version	The SSL version used by SSL VPN.
Connection Status	
Status	The current connecting status between the client and server. The possible statuses are: connecting, connected, disconnecting, and disconnected.
IPCompress	
Algorithm	Shows the compression algorithm used by SSL VPN.
Tunnel Packets	
Sent	The number of sent packets through the SSL VPN tunnel.
Received	The number of received packets through the SSL VPN tunnel.
Tunnel Bytes	

Address Information	
Sent	The number of sent bytes through the SSL VPN tunnel.
Received	The number of received bytes through the SSL VPN tunnel.
Connected Time	
Duration	Shows the time period during which the client is online.
Compress Ratio	
Sent	Shows the length ratio of sent data after compression.
Received	Shows the length ratio of received data after compression.

Interface

Descriptions of the options on the Interface tab:

Option	Description
Adapter Name	The name of the adapter used to send SSL VPN encrypted data.
Adapter Type	The type of the adapter used to send SSL VPN encrypted data.
Adapter Status	The status of the adapter used to send SSL VPN encrypted data.
Physical Address	The MAC address of the interface used to send SSL VPN encrypted data.
IP Address Type	The type of the interface address used to send SSL VPN encrypted data.
Network Address	The IP address (allocated by SSL VPN server) of the interface used to send SSL VPN encrypted data.
Subnet Mask	The subnet mask of the interface used to send SSL VPN

Option	Description
	encrypted data.
Default Gateway	The gateway address of the interface used to send SSL VPN encrypted data.
DNS Server Address	The DNS server addresses used by the client.
WINS Address	The WINS server addresses used by the client.

Route

Description of the option on the Route tab:

Option	Description
Local LAN Routes	The routes used by the virtual network adapter.

Viewing Secure Connect Menu

Right-click the Secure Connect icon (H) in the notification area and the menu appears.

Descriptions of the menu items are as follows:

Option	Description
Network Information	Displays the related information in the Network Information dialog box.
Log	Shows Secure Connect log messages in the Log dialog box. This dialog box shows the main log messages. To view the detailed log messages, click **Detail**. Click **Clear** to remove the messages in the dialog box. Click **OK** to close the Log dialog box.

Option	Description
Debug	Configures Secure Connect's debug function in the Debug dialog box.
About	Shows Secure Connect related information in the About dialog box.
Connect	When Secure Connect is disconnected, click this menu item to connect.
Disconnect	When Secure Connect is connected, click this menu item to disconnect.
Option	Configures Secure Connect options, including login information, auto start, auto login, and so on. For more information, see "Configuring Secure Connect" on Page 491.
Exit	Click **Exit** to exit the client. If the client is connected to the server, the connection will be disconnected.

Configuring Secure Connect

You can configure Secure Connect in the Secure Connect Options dialog box(click **Option** from the client menu). The configurations include:

- Configuring General Options
- Configuring a Login Entry

Configuring General Options

In the Secure Connect Options dialog box, select **General** from the navigation pane and the general options will be displayed.

Descriptions of the options:

Option	Description
Auto Start	Select this check box to autorun the SSL VPN client when the PC is started.
Auto Login	Select this check box to allow the specified user to login automatically when the PC is started. Select the auto login user from the Default Connection drop-down list.
Auto Reconnect	Select this check box to allow the client to reconnect to the SSL VPN server automatically after an unexpected disconnection.
Select Cert	Click the button to select a USB Key certificate in the Select Certificate dialog box. This option is available when the USB KEY authentication is enabled.

Configuring a Login Entry

Login entry contains the login information for clients. The configured login entries will be displayed in the Saved Connection drop-down list in the Login dialog box. You can login by simply choosing the preferred connection instead of filling up the options in the Login dialog box.

To add a login entry, take the following steps:

1. In the Secure Connect Options dialog box, select **Saved Connection** from the navigation pane and the login options will be displayed.

In the dialog box, configure the corresponding options.

Option	Description
Connection Name	Specifies the name for the connection to identify it. System will assign a name to the connection based on its server, port, and user automatically if this option is kept blank
Server	Specifies the IP address of the SSL VPN server.
Port	Specifies the HTTPS port number of the SSL VPN server.
Username	Specifies the login user.
Login Mode	Specifies the login mode. It can be one of the following options: • Password (the username/password authentication method). If **Password** is selected, select **Remember Password** to make system remember the password and type the password into the **Password** box. • Password + UKey (the USB KEY authentication method). If **Password + UKey** is selected, select **Remember PIN** to make system remember the PIN number and type PIN number into the **UKey PIN** box.
Proximity Auto Detection	Select the option to enable the optimal path detection function. For more information about optimal path detection, see "Configuring an SSL VPN" on Page 410.

2. Click **Apply**.

SSL VPN Client for Android

The SSL VPN client for Android is Hillstone Secure Connect. It can run on Android 4.0 and above. The functions of Hillstone Secure Connect contains the following items:

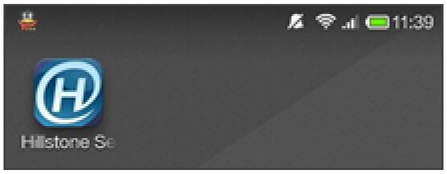
- Obtain the interface information of the Android OS.
- Display the connection status with the device, traffic statistics, interface information, and routing information.
- Display the log information of the application.

Downloading and Installing the Client

To download and install the client, take the following steps:

1. Visit https://www.hillstonenet.com/our-products/next-gen-firewalls-e-series/ to download the installation file of the client.
2. Use your mobile phone to scan the QR code of the client for Android at the right sidebar, and the URL of the client displays.
3. Open the URL and download the Hillstone-Secure-Connect-Versione_Number.apk file.
4. After downloading successfully, find this file in your mobile phone.
5. Click it and the installation starts.
6. Read the permission requirements.
7. Click **Install**.

After the client being installed successfully, the icon of Hillstone Secure Connect appears in the desktop as shown below:



Starting and Logging into the Client

To start and log into the client, take the following steps:

1. Click the icon of Hillstone Secure Connect. The login page appears.

2. **Provide the following information and then click Login.**

   - Please Choose: Select a login entry. A login entry stores the login information and it facilities your next login. For more information on login entry, see the Configuration Management section below.
   - Server: Enters the IP address or the server name of the device that acts as the VPN server.
   - Port: Enters the HTTPs port number of the device.
   - Username: Enters the username for logging into the VPN.
   - Password: Enters the corresponding password.

3. If the SSL VPN server enables the SMS authentication, the SMS authentication page will appear. In this page, enter the received authentication code and then submit it. If you do not receive the authentication code, you can request it after one minute.

4. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Submit. If you have not received the authentication code within one minute, you can re-apply.

5. If Email authentication is enabled on the SSL VPN server, the Email Authentication dialog will appear. Type the authentication code and click Submit. If you have not received the authentication code within one minute, you can re-apply.

After the client connecting to the SSL VPN server, the key icon (🔑) will appear at the notification area of your Android system.

GUI

After the client connects to the SSL VPN server, you can view the following pages: Connection Status page, Configuration Management page, Connection Log page, System Configuration page, and About Us page.

Connection Status

Click **Status** at the bottom of the page to enter into the **Connection Status** page and it displays the statistics and routing information:

- The Connection Time: Time period during which the client is online.
- Received Bytes: Shows the received bytes through the SSL VPN tunnel.
- Sent Bytes: Shows the sent bytes through the SSL VPN tunnel.
- Server: Shows the IP address or the server name of the device that client connects to.
- Port: Shows the HTTPs port number of the device.
- Account: Shows the username that logs into the VPN instance.
- Private Server Address: Shows the interface’ s IP address of the device that the client connects to.
- Client Private Address: Shows the IP address of the interface. This interface transmits the encrypted traffic and this IP address is assigned by the SSL VPN server.

- Address Mask: Shows the netmask of the IP address of the interface. This interface transmits the encrypted traffic.
- DNS Address: Shows the DNS Address used by the client.
- Routing Information: Shows the routing information for transmitting encrypted data.
- Disconnection Connection: Click this button to disconnect the current connection with the server.

Configuration Management

Click **VPN** at the bottom of the page to enter into the **Configuration Management** page. In this page, you can perform the following operations:

- Add/Edit/Delete a login entry
- Modify the login password
- Disconnect the connection with SSL VPN server
- Connect to the SSL VPN server

Adding a Login Entry

To facilitate the login process, you can add a login entry that stores the login information. The added login entry will display in the drop-down list of **Please Choose** in the login page. You can select a login entry and the login information will be filled in automatically.

To add a login entry, take the following steps:

1. In the Configuration Management page, click the ➕ icon at the top-right corner.
2. **In the pop-up window, enter the following information:**
   a. Connection Name: Enter a name as an identifier for this login entry

b. Server: Enter the IP address or the server name of the device that acts as the VPN server.

c. Port: Enter the HTTPs port number of the device.

d. Username: Enter the username for logging into the VPN.

3. Click **Confirm** to save this login entry.

Editing a Login Entry

To edit a login entry, take the following steps:

1. In the login entry list, click the one that you want to edit and several buttons will appear.
2. Click **Edit** to make the Edit Configuration dialog box appear.
3. In the dialog box, edit the login entry.
4. Click **Confirm** to save the modifications.

Deleting a Login Entry

To delete a login entry, take the following steps:

1. In the login entry list, click the one that you want to delete and several buttons will appear.
2. Click **Delete**.
3. Click **Yes** in the pop-up dialog box to delete this login entry.

Modifying the Login Password

To modify the login password, take the following steps:

1. In the login entry list, click the one that you want to modify the password and several buttons will appear.
2. Click **Modify Password**.
3. Enter the current password and new password in the pop-up dialog box.
4. Click **Confirm** to save the settings.

Disconnecting the Connection or Logging into the Client

To disconnect the connection or log into the client, take the following steps:

1. In the login entry list, click a login entry and several buttons will appear.
2. If the connection status to this server is disconnected, you can click **Login** to log into the client; if the connection status is connected, you can click **Disconnect Connection** to disconnect the connection.
3. In the pop-up dialog box, confirm your operation.

Connection Log

Click **Log** at the bottom of the page to enter into the **Configuration Log** page. In this page, you can view the logs.

System Configuration

Click **Config** at the bottom of the page to enter into the **System Configuration** page. In this page, you can configure the following options:

- Auto Reconnect: After turning on this switch, the client wil automatically reconnect to the server if the connection is disconnected unexpectedly.
- Show Notify: After turning on this switch, the client icon will display in the notification area.

- Allow To Sleep: After turning on this switch, the client can stay connected while the Android system is in the sleep status. With this switch turned off, the client might disconnect the connection and cannot stay connected for a very long time while the Android system is in the sleep status.
- Auto Login: After turning on this switch, the client will automatically connect to the server when it starts. The server is the one that the client connects to the last time.
- Remember The Password: After turning on this switch, the client wil remember the password and automatically fill in the login entry.
- Exit: Click **Exit** to exit this application.

About Us

Click **About** at the bottom of the page to enter the About US page. This page displays the version information, contact information, copyright information, etc.

SSL VPN Client for iOS

The SSL VPN client for iOS is called Hillstone Access Connectand it supports iOS 10.0 and higher versions. HillstoneAccess Connectmainly has the following functions:

- Simplify the VPN creation process between the Apple device and the Hillstone device
- Display the VPN connection status between the Apple device and the Hillstone device
- Display the log information

To use the SSL VPN client for iOS, download and install the **Hillstone Access Connect**app from the App Store.

Deploying VPN Configurations

For the first-time logon, you need to deploy the VPN configurations, as shown below:

1. Click the HSAccess icon located at the desktop of iOS. The login page of HSAccess appears.
2. **In the login page, specify the following information and then click Login.**
    - Connection: Enter a name for this newly created connection instance.
    - Server: Enter the IP address or the server name of the device that acts as the VPN server.
    - Port: Enter the HTTPs port number of the device.
    - Username: Enter the username for logging into the VPN.
    - Password: Enter the corresponding password.

3. If the SSL VPN server enables the SMS authentication, the SMS authentication page will appear. Enter the received authentication code and then confirm it. If you do not receive the authentication code, you can request it after one minute.

4. After logging the VPN server successfully, the deployment process starts automatically.

5. In the **Would Like to Add VPN Configurations** page, click **Allow**.

6. Enter your passcode. The passcode is the one for unlocking your iOS screen. With the correct passcode entered, iOS starts to install the profile.

Connecting to VPN

After the VPN configuration deployment is finished, take the following steps to connect to VPN:

1. Start HSAccess .

2. In the login page, enter the required information. The value of these parameters should be the ones that you have specified in the above section of Deploying VPN Configurations. If one of the parameter changes, you need to re-deploy the VPN configuration.

3. Click **Login**. HSAccess starts to connects to the Hillstone device.

4. Start **Settings** of iOS and navigate to **VPN**.

5. In the **VPN** page, select the configuration that has the same name as the one you configured in the section of Deploying VPN Configuration.

6. Click the **VPN** switch. iOS starts the VPN connection.

7. In this **VPN** page, when the **Status** value is **Connected**, it indicates the VPN between the iOS device and the Hillstone device has been established.

Introduction to GUI

After logging into HBC, you can view the following pages: Connection Status, Connect, Log, and About.

Connection Status

Click **Status** at the bottom of the page to enter into the **Connection Status** page and it displays the statistics and routing information:

- The Connection Time: Time period during which the client is online.
- In Bytes: Shows the received bytes through the SSL VPN tunnel.
- Out Bytes: Shows the sent bytes through the SSL VPN tunnel.
- Server: Shows the IP address or the server name of the device that client connects to.
- Port: Shows the HTTPs port number of the device.
- Username: Shows the user name of the device.
- Server IP: Shows the interface’s IP address of the device that the client connects to.
- Assigned IP: Shows the IP address of the interface. This interface transmits the encrypted traffic and this IP address is assigned by the SSL VPN server.
- Mask: Shows the netmask of the IP address of the interface. This interface transmits the encrypted traffic.
- DNS Address: Shows the DNS Address used by the client.
- Route Info: Shows the routing information for transmitting encrypted data.

Configuration Management

Click VPN at the bottom of the page to enter into the Configuration Management page. In this page, you can perform the following operations:

- Add a login entry
- Detele a login entry
- Disconnect the connection with SSL VPN server
- Enable/ Disable the auto reconnection

Adding a Login Entry

To facilities the login process, you can add a login entry that stores the login information. The added login entry will display in the drop-down list of Select in the login page. You can select a login entry and the login information will be filled in automatically.

To add a login entry, take the following steps:

1. In the **Configuration Management** page, click the **+** icon at the top-right corner.
2. In the pop-up window, enter the following information:
    - Name: Enters a name as an identifier for this login entry
    - Server: Enters the IP address or the server name of the device that acts as the VPN server.
    - Port: Enters the HTTPs port number of the device.
    - Username: Enters the username for logging into the VPN.
    - Allow Sleep: After turning on this switch, the client can keep connected while the iOS is in the sleep status. With this switch turned off, the client might disconnect the connection and cannot keep connected for a long time while the iOS is in the sleep status.
3. Click **Confirm** to save this login entry.

Deleting a Login Entry

To delete a login entry, take the following steps:

1. In the login entry list, click the one that you want to delete and several buttons display.
2. Click **Delete**.
3. Click **Yes** in the pop-up dialog to delete this login entry.

Disconnecting the Connection or Logging into the Client

To disconnect the connection or log into the client, take the following steps:

1. In the login entry list, click a login entry.
2. In the pop-up dialog, Click Logout / Login to disconnect the connection or log into the client.

Enabling/ Disabling the Auto Reconnection

After turning on this switch, the client will automatically reconnect to the server if the connection is disconnected unexpectedly.

To enable/ disable the auto reconnection, take the following steps:

1. Enter the Configuration Management page.
2. Turn on or turn off the Auto Reconnect switch.

Connection Log

Click **Log** at the bottom of the page to enter into the **Connection Log** page and it displays the connection log messages.

About US

Click **About** at the bottom of the page to enter the **About Hillstone** page and it displays the information of version, copyright, etc.

SSL VPN Client for Mac OS

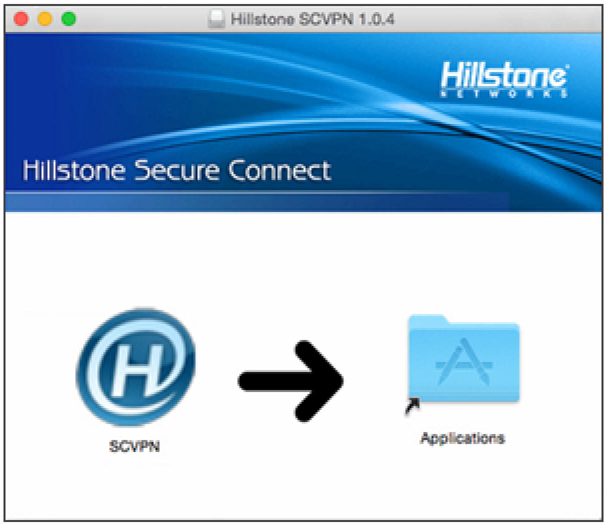
The SSL VPN client for Mac OS is Hillstone Secure Connect. It can run on Mac OS X 10.6.8 and above. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server after a connection has been established successfully. The functions of the client are:

- Establish the SSL VPN connection with the SSL VPN server.
- Show the connection status, traffic statistics, and route information.
- Show log messages.

Downloading and Installing Client

Visit https://www.hillstonenet.com/products/next-gen-firewalls-e-series/ to download the installation file of the client.

After downloading the installation file, double-click it. In the pop-up, drag SCVPN to Applications to perform the installation.



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 Client and Establishing Connection

To start the client and establish the connection with the server side, take the following steps:

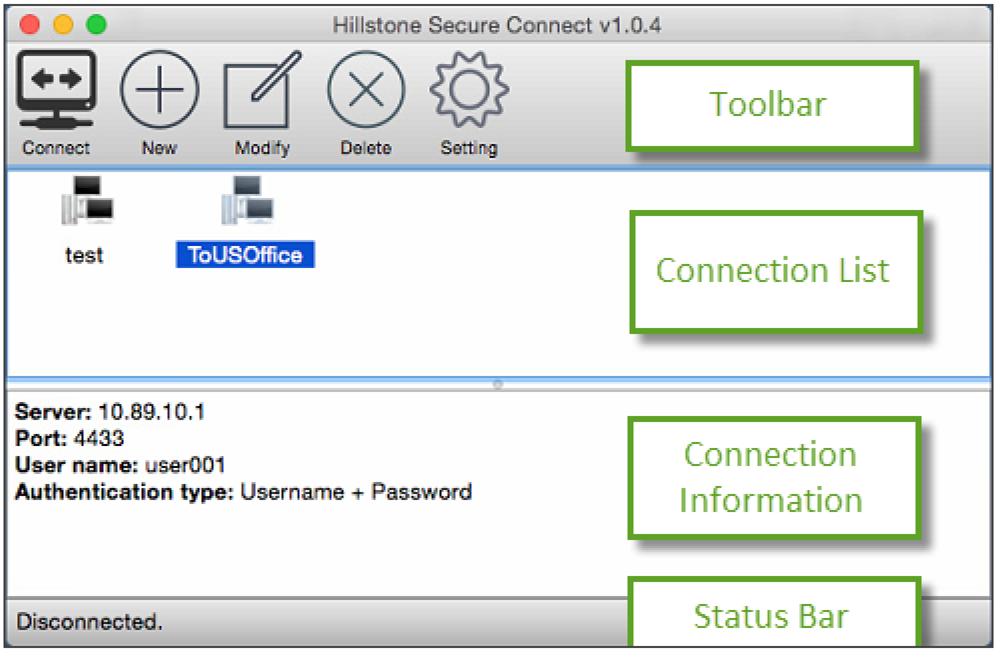
1. In Mac OS, select **Launchpad > SCVPN**. The client starts.
2. Click **New**. The **Create connection profile** window appears.
3. Provide the following information and then click **OK**.
    - **Name**: Specify a name for this VPN connection.
    - **Description**: Specify the description for this VPN connection.
    - **Server**: Enter the IP address or the server name of the device that acts as the VPN server.
    - **Port**: Enter the HTTPs port number of the device.
    - **User name**: Enter the login name.
    - **Password**: Enter the corresponding password.
    - **Remember password** : Select this check box to remember the password.
    - **GMSSL**: Select this check box to use the GM SSL protocol.
4. Select the connection name in the connection list.
5. In the toolbar, click **Connect**. If you do not select **Remember password** in step 3, enter the password in the pop-up and then click **OK**.

6. If token authentication is enabled on the SSL VPN server, the token Authentication dialog will appear. Type the authentication code and click Submit. If you have not received the authentication code within one minute, you can re-apply.

After the client connects to the SSL VPN server, the status bar displays **Connection established**. Meanwhile, the notification area of Mac displays 🔌 . The encrypted data can be transmitted between the SSL VPN client and SSL VPN server now.

GUI

The GUI of the client includes four areas: toolbar, connection list, connection information, and status bar.



Server: 10.89.10.1
Port: 4433
User name: user001
Authentication type: Username + Password

Disconnected.

Toolbar

In the toolbar, you can perform the following actions:

- Connect: Select a connection from the connection list and then click Connect. The client starts to establish the connection with server side.

- New: Create a new connection. For details, see Starting Client and Establishing Connection.
- Modify: Select a connection from the connection list and then click **Modify**. For details of modifying the parameters, see Starting Client and Establishing Connection.
- Delete: Select a connection from the connection list and then click **Delete** to delete this connection.
- Settings: Set to minimize the client when the connection is established and select whether to check the update of the client when it starts.
- Cancel: Click this button to cancel the connection. When the client is connecting to the server side, this button will display.
- Disconnect: Disconnect the current connection. After the connection is established, this button will display.
- Info: View the channel information and the route information of the current connection. After the connection is established, this button displays.

Connection List

Displays all created connections.

Connection Information

When selecting a connection in the connection list, the connection information area displays the corresponding information of this connection.

After establishing the connection, the connection information area displays the connection duration, server IP address, the IP assigned to the client, the number of packets sent/received through the SSL VPN tunnel, and the bytes sent/received through the SSL VPN tunnel.

Status Bar

Displays the connection status.

Menu

The **SCVPN** item in the menu includes the following options:

- About SCVPN: Displays the information of this client.
- Quit SCVPN: Quit the client.

The **Logging** item in the menu includes the following options:

- View: View the logs.
- Level: Select the log level. When selecting the lower level in the menu, the displayed logs will include the logs of upper level. However, when selecting the upper level in the menu, the displayed logs will not include the logs of lower level.

SSL VPN Client for Linux

The SSL VPN client for Linux is Hillstone Secure Connect. It can run on the following operation system.

- 64-bit desktop version of Ubuntu12.04 (GNOME desktop);
- 64-bit desktop version of Ubuntu14.04(GNOME desktop);
- 64-bit desktop version of Ubuntu Kylin16.04(default desktop);
- 64-bit desktop version of CentOS6.5(GNOME desktop);

The encrypted data can be transmitted between the SSL VPN client and SSL VPN server 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 connection status, traffic statistics, and route information.
- Show log messages.

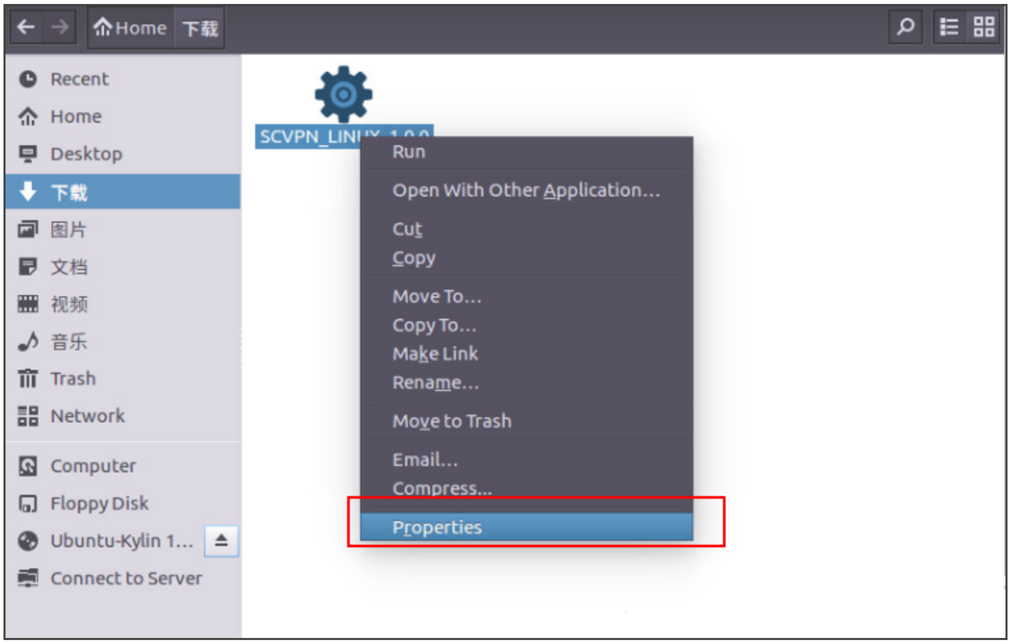
Take 64-bit Ubuntu Kylin16.04 desktop as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other three Linux systems can refer to 64-bit Ubuntu Kylin16.04 desktop.

Downloading and Installing Client

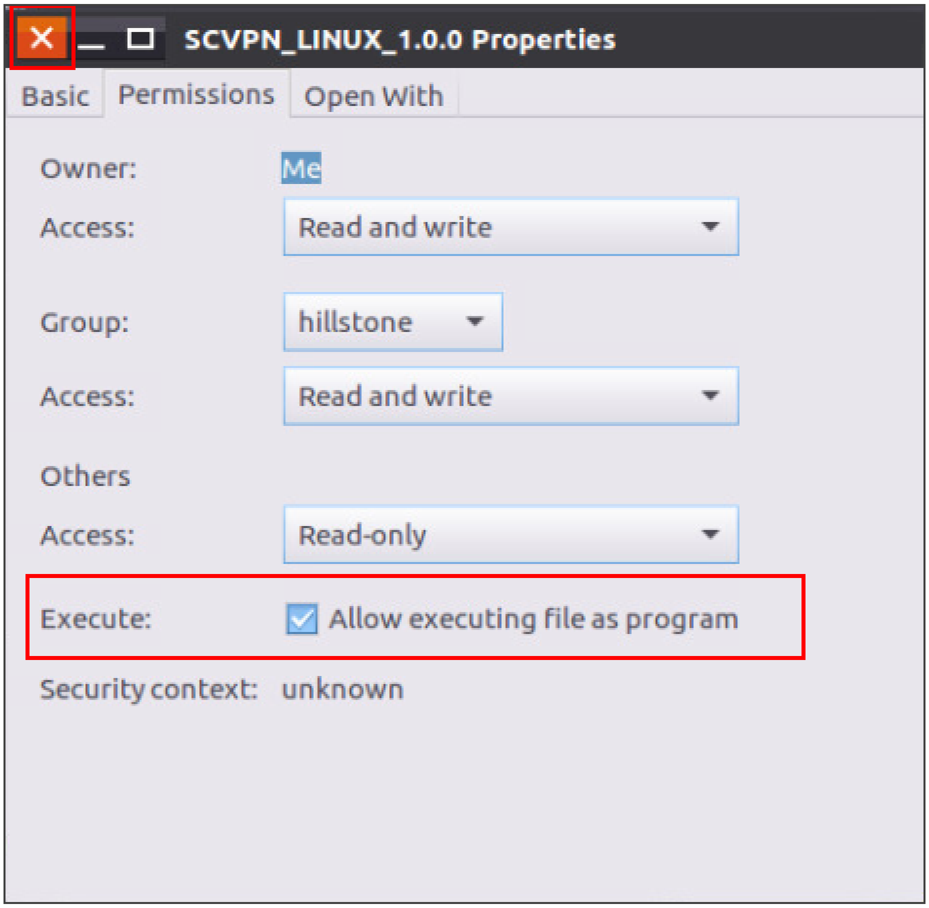
Downloading and installing Hillstone Secure Connect, take the following steps:

1. Visit https://www.hillstonenet.com/products/next-gen-firewalls-e-series/ to download the installation file of the client.

2. After downloading the installation file, right-click the client icon and select **Properties** to go to the properties page.



3. In the properties page, click **Permissions** tab and check **Allow executing files as program**, then close it.



SCVPN_LINUX_1.0.0 Properties

Owner: Me

Access: Read and write

Group: hillstone

Access: Read and write

Others

Access: Read-only

Execute: ☑ Allow executing file as program

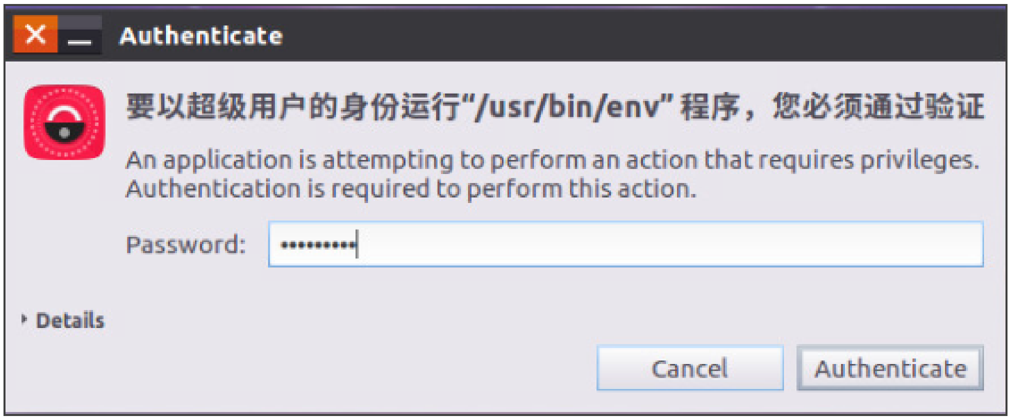
Security context: unknown

4. Double-click the client icon and follow the setup wizard to complete the installation.

Starting Client and Establishing Connection

To start the client and establish the connection with the server side, take the following steps:

1. Double-click the SCVPN icon on the desktop of the Linux system, and system enters the super user authentication page. Then enter the password of super user , and click **Authenticate** to enter the main interface of the client.

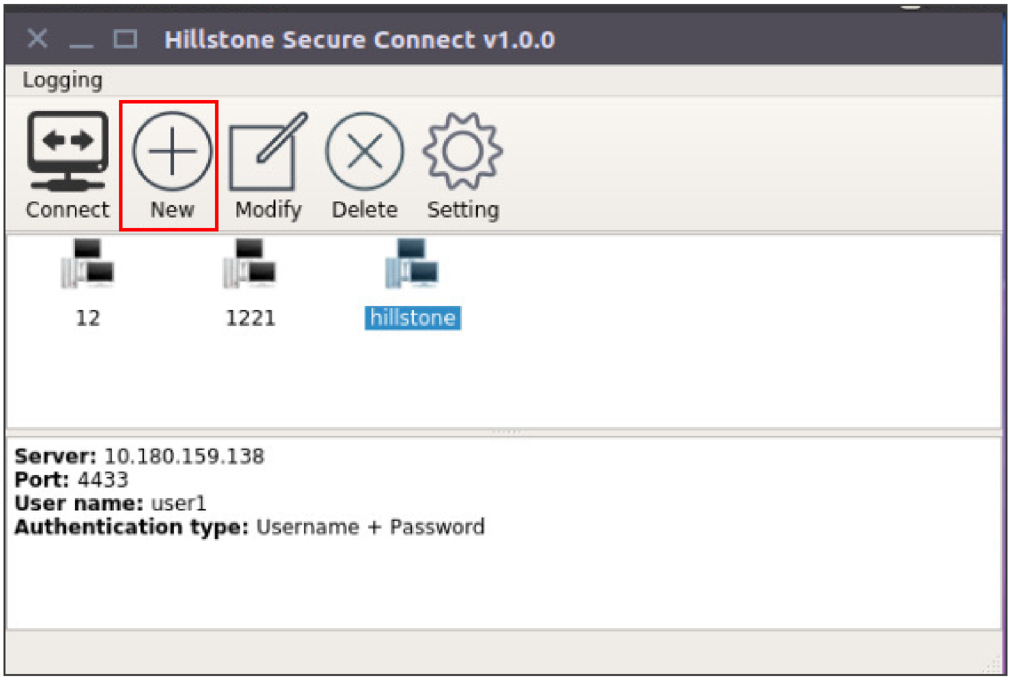

Authenticate

要以超级用户的身份运行"/usr/bin/env"程序，您必须通过验证

An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.

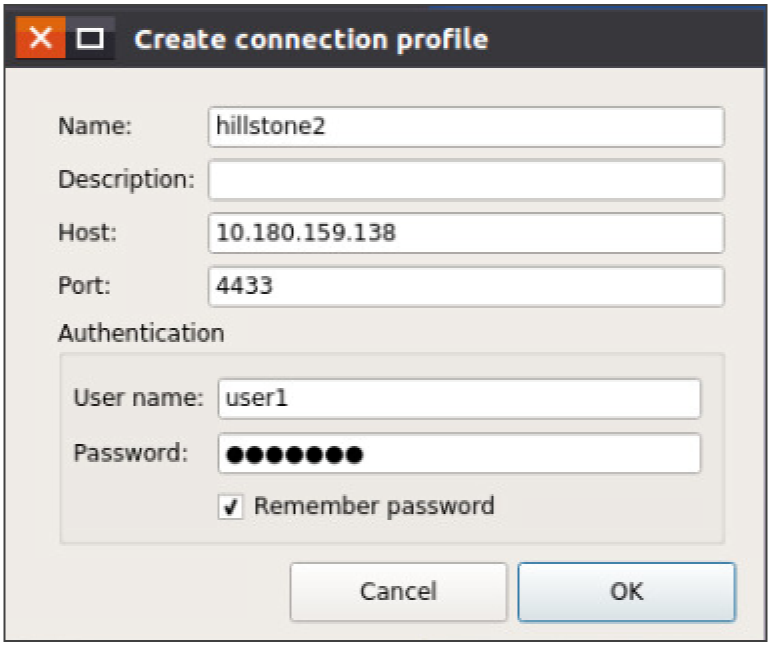
Password: ••••••••••

2. In the client main interface, click **New**. The **Create connection profile** dialog box appears.



Server: 10.180.159.138
Port: 4433
User name: user1
Authentication type: Username + Password

3. Provide the following information and then click OK.


Create connection profile

Name: hillstone2

Description:

Host: 10.180.159.138

Port: 4433

Authentication

User name: user1

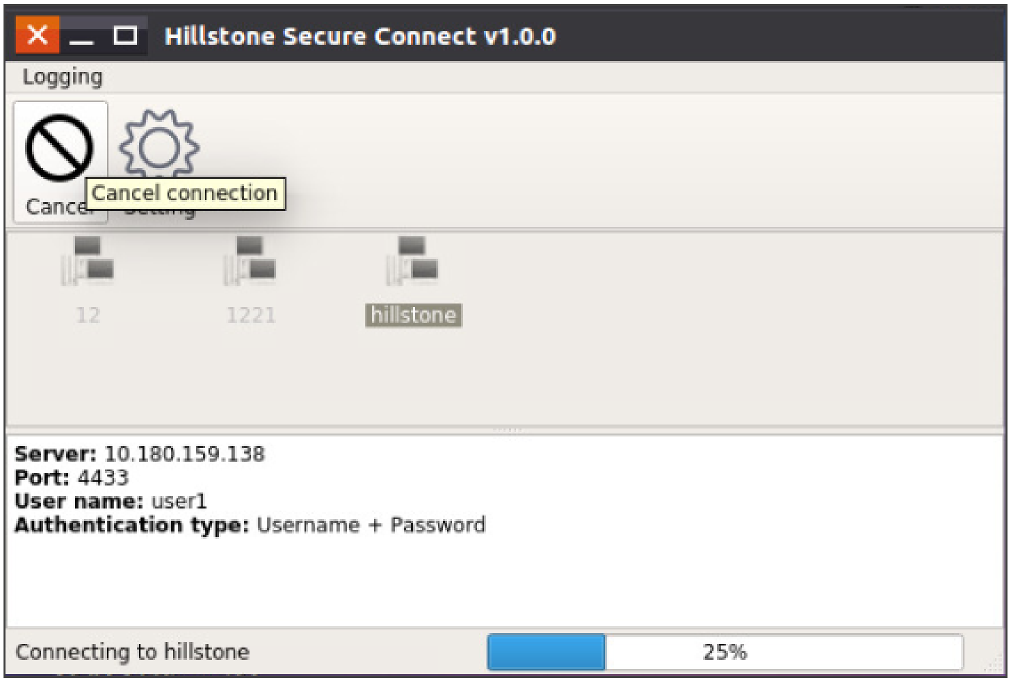
Password: ●●●●●●●

☑ Remember password

- **Name**: Specify a name for this VPN connection.
- **Description**: Specify the description for this VPN connection.
- **Server**: Enter the IP address or the server name of the device that acts as the VPN server.
- **Port**: Enter the HTTPs port number of the device.
- **User name**: Enter the login name. For detailed information, refer to "User" on Page 619.
- **Password**: Enter the corresponding password.
- **Remember password** : Select this check box to remember the password.

4. Select the connection name in the connection list. In the toolbar, click **Connect**. If you do not select **Remember password** in step 3, enter the password in the pop-up and then click

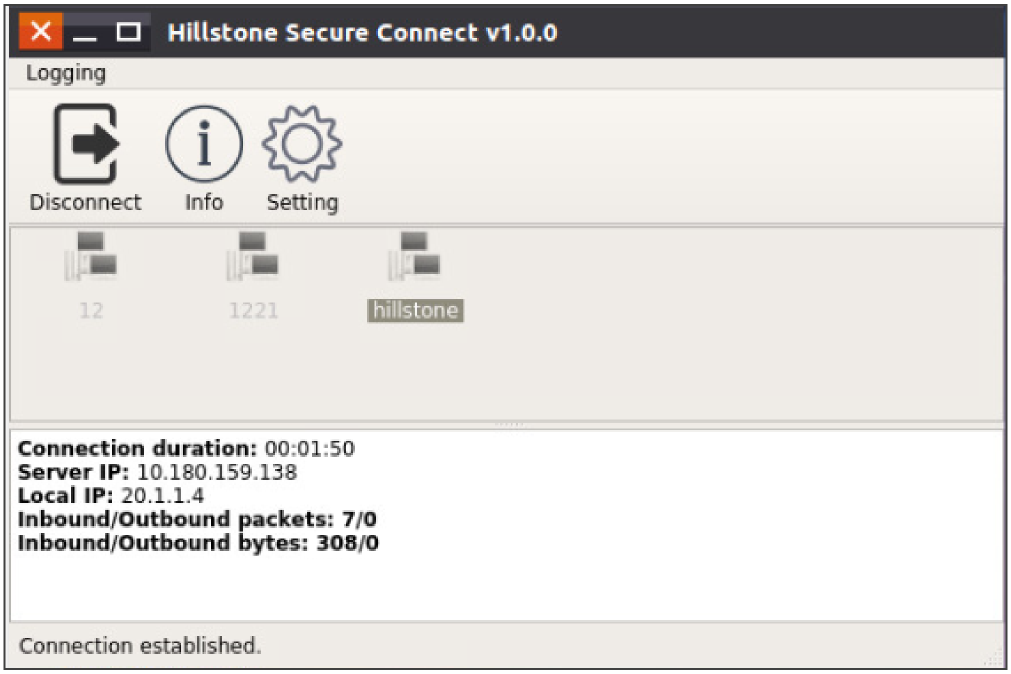
OK.



Server: 10.180.159.138
Port: 4433
User name: user1
Authentication type: Username + Password

Connecting to hillstone 25%

5. After the client connecting to the SSL VPN server, the status bar displays **Connection established**. The encrypted data can be transmitted between the SSL VPN client and SSL VPN server now.



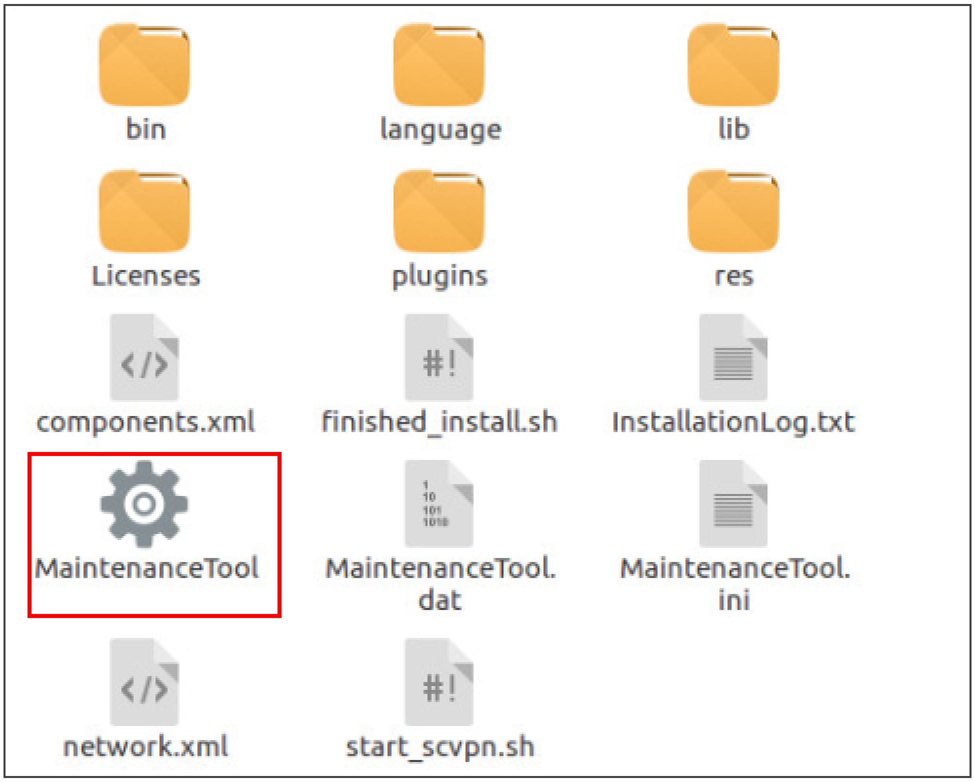
Connection duration: 00:01:50
Server IP: 10.180.159.138
Local IP: 20.1.1.4
Inbound/Outbound packets: 7/0
Inbound/Outbound bytes: 308/0

Connection established.

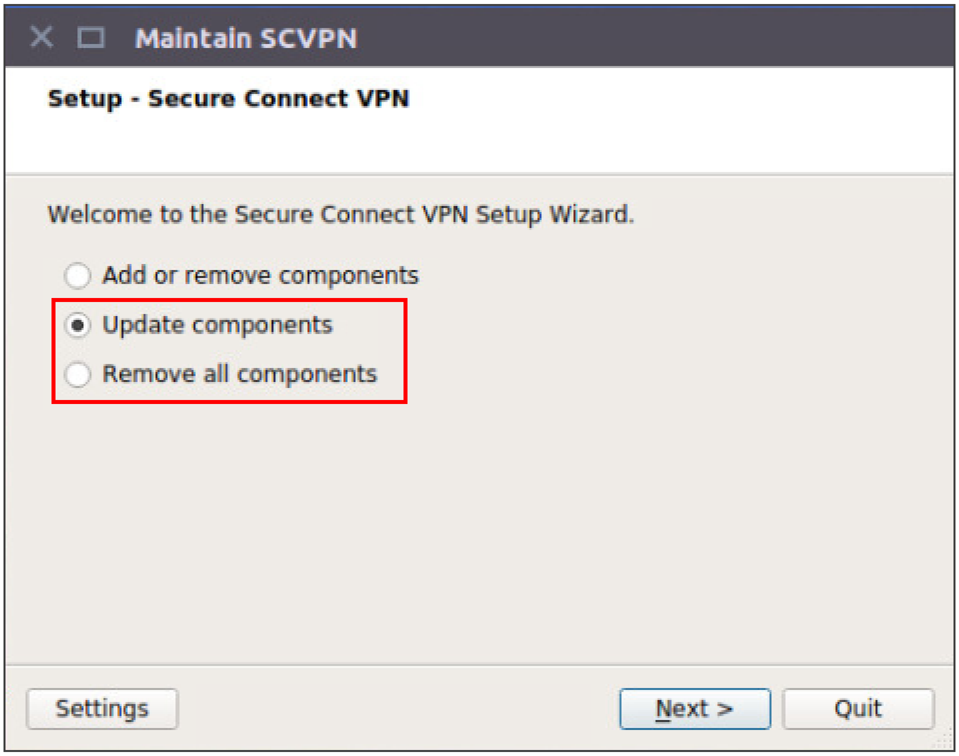
Upgrading and Uninstalling Client

To update and uninstall the SSL VPN Client, take the following steps:

1. Double-click the MaintenanceTool icon to enter the **Maintain SCVPN** page.



2. In the **Maintain SCVPN** page, select **Update components** or **Remove all components** to upgrade or uninstall the client, then click **Next**.



Welcome to the Secure Connect VPN Setup Wizard.

○ Add or remove components

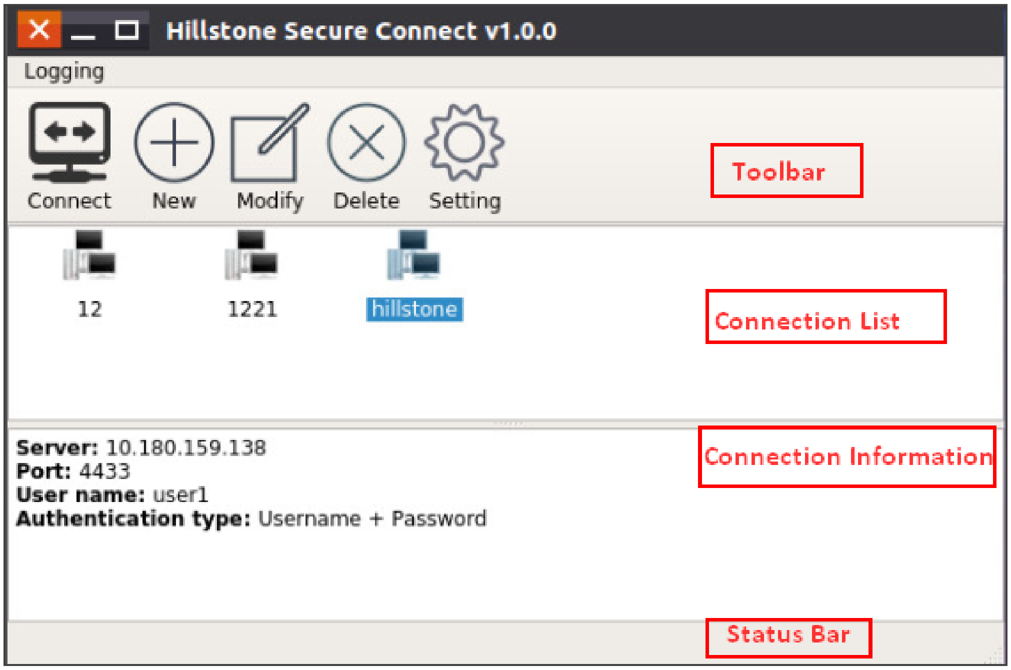
● Update components

○ Remove all components

3. Follow the setup wizard to complete the upgrade or uninstall of client.

GUI

The GUI of the client includes four areas: toolbar, connection list, connection information, and status bar.



Server: 10.180.159.138
Port: 4433
User name: user1
Authentication type: Username + Password

Toolbar

In the toolbar, you can perform the following actions:

- Connect: Select a connection from the connection list and then click **Connect**. The client starts to establish the connection with server side.
- New: Create a new connection. For details, see Starting Client and Establishing Connection.
- Modify: Select a connection from the connection list and then click **Modify**. For details about modifying the parameters, see Starting Client and Establishing Connection.
- Delete: Select a connection from the connection list and then click **Delete** to delete this connection.
- Settings: Set to minimize the client when the connection is established
- Cancel: Click this button to cancel the connection. When the client is connecting to the server side, this button is displayed. For more information, see Starting Client and Establishing Connection.

- Disconnect: Disconnect the current connection. After the connection is established, this button is displayed. For more information, see Starting Client and Establishing Connection.

- Info: View the channel information and the route information of the current connection. After the connection is established, this button is displayed. For more information, see Starting Client and Establishing Connection.

Connection List

Displays all created SSL VPN connections, and uses different icons to distinguish between the connected and the unconnected.

Connection Information

When selecting a connection in the connection list, the connection information area displays the corresponding information of this connection.

- When the client doesn't connect or has connected to the server, the connection information area displays the server IP address, the port number, the user name and the authentication type.

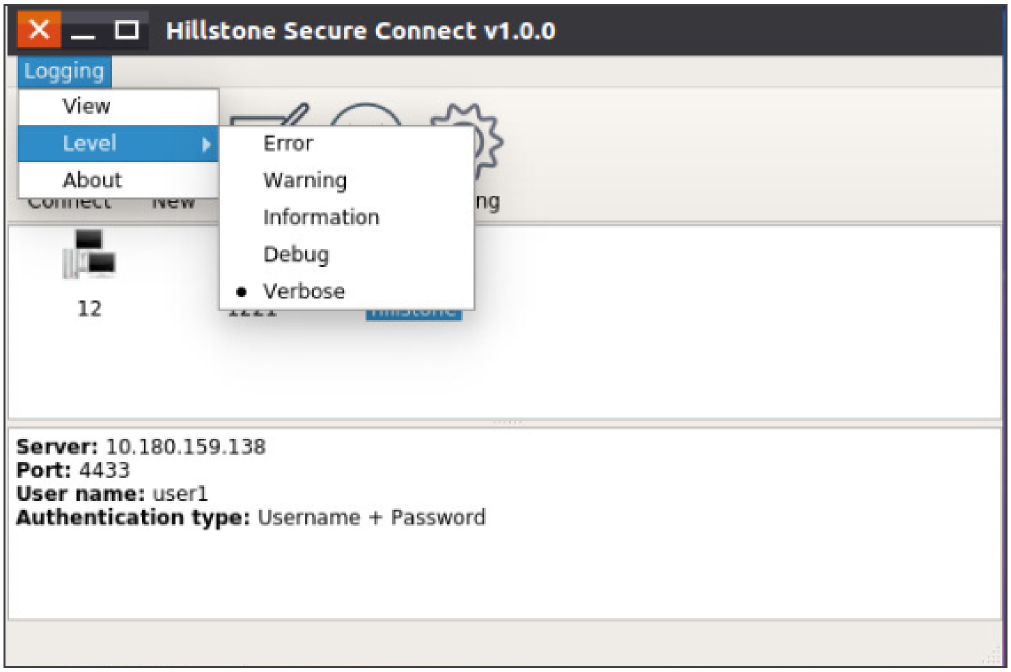
- After establishing the connection, the connection information area displays the connection duration, server IP address, the IP assigned to the client, the number of packets sent/received through the SSL VPN tunnel, and the bytes sent/received through the SSL VPN tunnel.

Status Bar

Displays the connection status and the connection progress when connecting to the server. For more information, see Starting Client and Establishing Connection.

Menu

Click the **logging** menu in the top-left corner of the client interface .



Server: 10.180.159.138
Port: 4433
User name: user1
Authentication type: Username + Password

- View: View the logs.
- Level: Select the log level. When selecting a level in the menu, system will display the logs of upper levels and will not display the logs of lower levels.
  - About: Display the version information, copyright information and other relevant information.

L2TP VPN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

L2TP (Layer Two Tunneling Protocol) is a VPDN technique that allows dial-up users to launch VPN connection from L2TP clients or L2TP access concentrators (LAC), and connect to a L2TP network server (LNS) via PPP. After the connection has been established successfully, LNS will assign IP addresses to legal users and permit them to access the private network.

The device acts as a LNS in the L2TP tunnel network. The device accepts connections from L2TP clients or LACs, implements authentication and authorization, and assigns IP addresses, DNS server addresses and WINS server addresses to legal users.

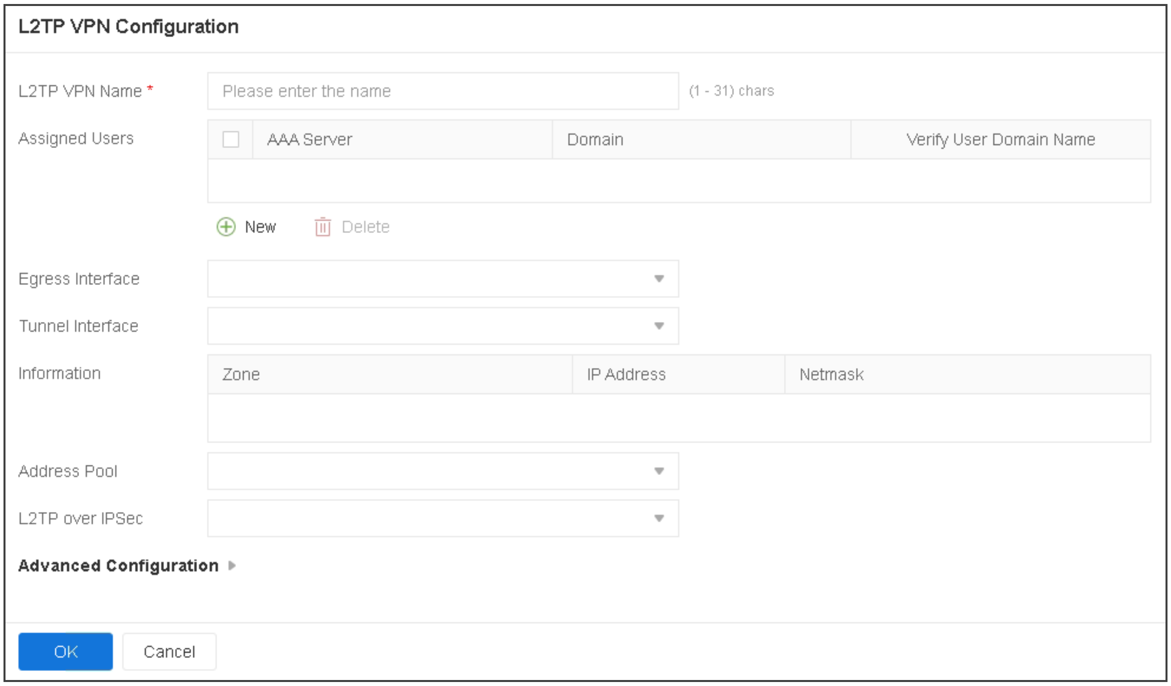
L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPsec, and encrypt data by IPSec, thus assuring the security during the data transmitted through the L2TP tunnel.

Configuring an L2TP VPN

To create an L2TP VPN instance, take the following steps:

1. Select **Network > VPN > L2TP VPN**.

2. In the L2TP VPN page, click **New**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
L2TP VPN Name	Type the name of the L2TP VPN instance
Assigned Users	
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.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server.
Verify User Domain Name	After this function is enable, system will verify the user-name and its domain name.
Add	Click **Add** to add the assigned users. You can repeat to add more items.

In the Interface/Address Pool/IPSec Tunnel tab, configure the corresponding options.

Access Interface	
Egress Interface	Select the interface from the drop-down list as the L2TP VPN server interface. This interface is used to listen to the request from L2TP clients.
Tunnel Interface	
Tunnel Interface	Specifies the tunnel interface used to bind to the L2TP VPN tunnel. Tunnel interface transmits traffic to/from L2TP VPN tunnel. • Select a tunnel interface from the drop-down list, and then click **Edit** to edit the selected tunnel interface. • Click **New** in the drop-down list to create a new interface.
Information	Shows the zone, IP address, and netmask of the selected tunnel interface.
Address Pool	
Address Pool	Specifies the L2TP 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. For more information about creating/editing address pools, see "Configuring an L2TP VPN Address Pool" on Page 528.

Information	Shows the start IP address, end IP address, and mask of the address pool.
L2TP over IPSec	
L2TP over IPSec	Select a referenced IPSec tunnel from the drop-down list. L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPSec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the L2TP tunnel..

3. If necessary, click **Advanced Configuration** to configure the advanced functions.

In the Parameters tab, configure the corresponding options.

Security	
Tunnel Authentication	Click **Enable** to enable tunnel authentication to assure the security of the connection. The tunnel authentication can be launched by either LNS or LAC. The tunnel cannot be established unless the both ends are authenticated, i.e., the secret strings of the two ends are consistent.
AVP Hidden	Click **Enable** to enable AVP hidden. L2TP uses AVP (attribute value pair) to transfer and negotiate several L2TP parameters and attributes. By default AVP is transferred in plain text. For data security consideration, you can encrypt the data by the secret string to hide the AVP during the transmission.
Secret	Specifies the secret string that is used for LNS tunnel authentication.
Peer	Specifies the host name of LAC. If multiple LACs are connected to LNS, you can specify different secret

	strings for different LACs by this parameter.
Add	Click **Add** to add the configured secret and peer name pair to the list.
Client Connection	
Accept Client IP	Click **Enable** to allow the accepting of IP address specified by the client. By default the client IP is selected from the address pool, and allocated by LNS automatically. If this function is enabled, you can specify an IP address. However, this IP address must belong to the specified address pool, and be consistent with the username and role. If the specified IP is already in use, system will not allow the user to log on.
Multiple Login	Click **Enable** to allow a user to log on and be authenticated on different hosts simultaneously.
Hello Interval	Specifies the interval at which Hello packets are sent. LNS sends Hello packets to the L2TP client or LAC regularly, and will drop the connection to the tunnel if no response is returned after the specified period.
LNS Name	Specifies the local name of LNS.
Tunnel Windows	Specifies the window size for the data transmitted through the tunnel.
Control Packet Transmit Retry	Specifies the retry times of control packets. If no response is received from the peer after the specified retry times, system will determine the tunnel connection is disconnected.
PPP Configuration	
LCP Interval Transmit	Specifies parameters for LCP Echo packets used for PPP negotiation. The options are:

Retries	• Interval: Specifies the interval at which LCP Echo packets are sent. • Transmit Retry: Specifies the retry times for sending LCP Echo packets. If LNS has not received any response after the specified retry times, it will determine the connection is disconnected.
PPP Authentication	Specifies a PPP authentication protocol. The options are: • PAP: Uses PAP for PPP authentication. • CHAP: Uses CHAP for PPP authentication. This is the default option. • Any: Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

4. Click **Done** to save the settings.

Configuring an L2TP VPN Address Pool

LNS assigns the IP addresses in the address pool to users. After the client has established a connection to LNS successfully, LNS will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and assign them to the client.

L2TP provides fixed IP addresses by creating and implementing IP binding rules.

- The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client.

- The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When LNS is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses for the client based on the specific checking order below:

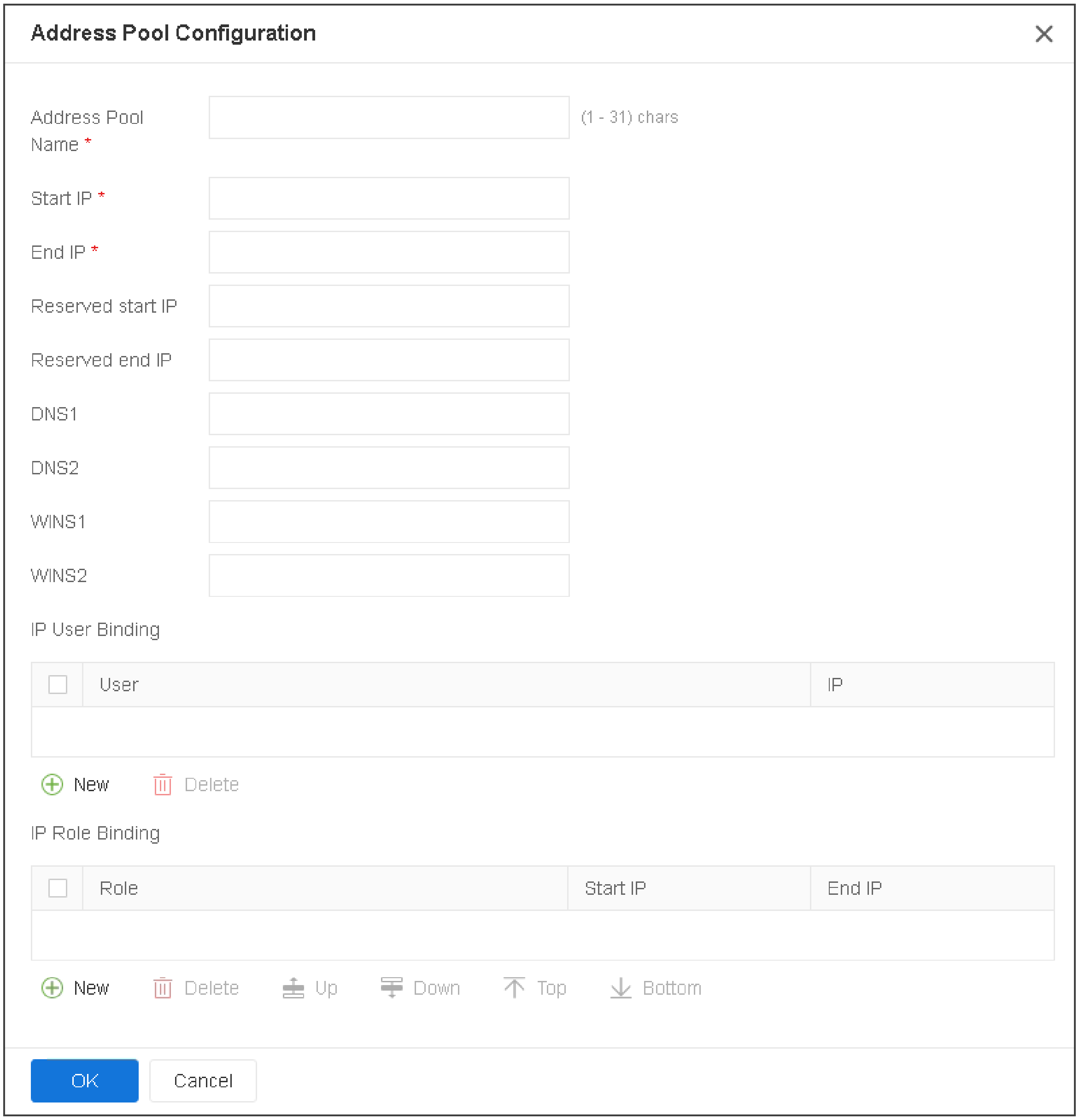
Notes: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To create an address pool, take the following steps:

1. Select **Network > VPN > L2TP VPN**.

2. At the top-right corner, click **Address Pool**.

3. In the pop-up window, click **New**.



Address Pool Configuration

Address Pool Name *		(1 - 31) chars
Start IP *		
End IP *		
Reserved start IP		
Reserved end IP		
DNS1		
DNS2		
WINS1		
WINS2		

IP User Binding

□	User	IP

IP Role Binding

□	Role	Start IP	End IP

In the Basic Configuration tab, configure the corresponding options.

Option	Description
Address Pool	Specifies the name of the address pool.

Option	Description
Name	
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. Up to 2 DNS servers can be configured for one address pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add this IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the **Role** box.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add**to add this IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down/Top/Bottom	System will query for IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

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

Viewing L2TP VPN Online Users

To view the L2TP VPN online users, take the following steps:

1. Select **Network > VPN > L2TP VPN**.

2. Select an L2TP VPN instance.

3. View the detailed information of the online users in the table.

Option	Description
Name	Displays the name of L2TP VPN.
Login Time	Displays the login time of the L2TP VPN online user.
Public IP	Displays the public IP of the L2TP VPN online user.

Option	Description
Private IP	Displays the private IP of the L2TP VPN online user.
Operation	Displays the executable operation of the L2TP VPN online user.

VXLAN

Virtual extensible local area network (VXLAN) is a tunnel encapsulation technology for large layer 2 network expansion overe NOV3 that uses MAC-in-UDP encapsulation. VXLAN uses a 24-bit network segment ID, called VXLAN network identifier (VNI), to identify users. This VNI is similar to a VLAN ID and supports a maximum of 16M [(2^24 - 1)/1024^2] VXLAN segments. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks to ensure uninterrupted services during VM migration, the IP address of the VM must remain unchanged.

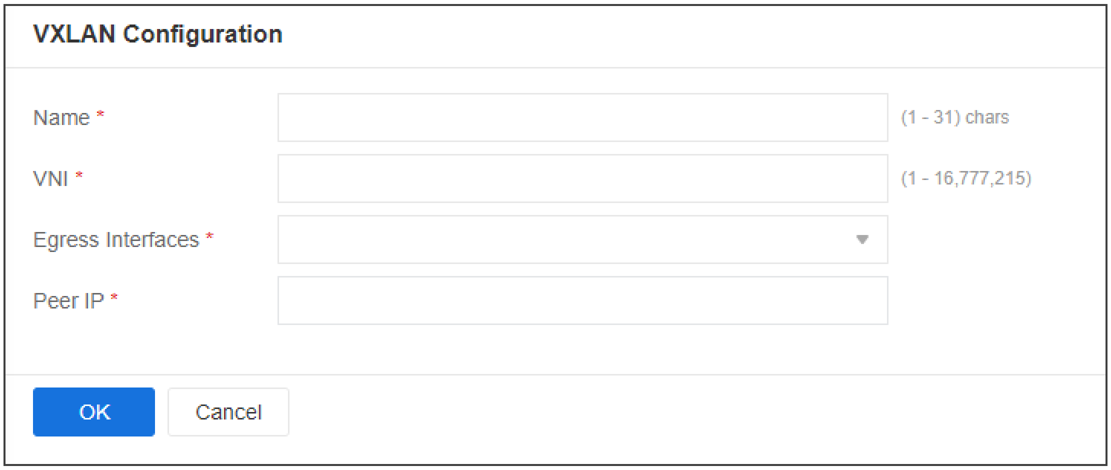
VXLAN uses VTEP (VXLAN Tunnel Endpoint) equipment to encapsulate and decapsulate VXLAN packets, including ARP request packets and normal VXLAN data packets. VETP encapsulates the original Ethernet frame through VXLAN and sends it to the peer VTEP device. The peer VETP device decapsulates the VXLAN packet after receiving it, and then forwards it according to the original MAC. The VTEP can be a physical switch, a physical server, or other VXLAN-enabled Hardware equipment or software.

Creating VXLAN Static Tunnel

To creating VXLAN static tunnel, take the following steps:

1. Click **Network** > **VPN** > **VXLAN**.

2. Click **New**



VXLAN Configuration

Name * (1 - 31) chars

VNI * (1 - 16,777,215)

Egress Interfaces *

Peer IP *

Configure the following options.

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.
Peer IP	Specified the destination VETP IP address.

3. Click **OK**.

Chapter 9 Object

This chapter describes the concept and configuration of objects that will be referenced by other modules in system, including:

- "Address" on Page 537: Contains address information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, session limit rules, etc.
- "Host Book" on Page 541: A collection of one domain name or several domain names.
- "Service Book" on Page 544: Contains service information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- "Application Book" on Page 553: Contains application information, and it can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- "SLB Server Pool " on Page 581: Describes SLB server configurations.
- "Schedule" on Page 586: Specifies a time range or period. The functions (such as policy rules, QoS rules, host blacklist, connections between the PPPoE interface and Internet) that use the schedule will take effect in the time range or period specified by the schedule.
- "AAA Server" on Page 589: Describes how to configure an AAA server.
- "User" on Page 619: Contains information about the functions and services provided by a Hillstone device, and users authenticated and managed by the device.
- "Role" on Page 630: Contains role information that associates users to privileges. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.
- "Track Object" on Page 654: Tracks if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

- " URL Filtering" on Page 659: URL filter controls the access to some certain websites and records log messages for the access actions.

- "NetFlow" on Page 742 : Collect the user's incoming traffic information according to the NetFlow profile, and send it to the server with NetFlow data analysis tool.

- "End Point Protection" on Page 747: Obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.

- "IoT Policy" on Page 758: Identify the network video monitoring devices, like IPC (IP Camera) and NVR (Network Video Recorder) via the flowing traffic, then monitor the identified devices and block illegal behaviors according to the configurations.

Address

IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, system uses an address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only the name is referenced during configuration. The address book is the database in system that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

System provides a global address book. You need to specify an address entry for the global address book. When specifying the address entry, you can replace the IP range with a DNS name. Interfaces of the configured IPs will be used as address entries and added to the address book automatically. You can use them for NAT conveniently. Furthermore, an address entry also has the following features:

- All address books contain two default address entries named **Any** and **private_network**. The IP address of **Any** is 0.0.0.0/0, which is any IP address. **Any** can neither be edited nor deleted. The IP addresses of **private_network** are 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, that all private network address. The **private_network** can be edited and deleted.
- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, StoneOS will update other modules that reference the address entry automatically.

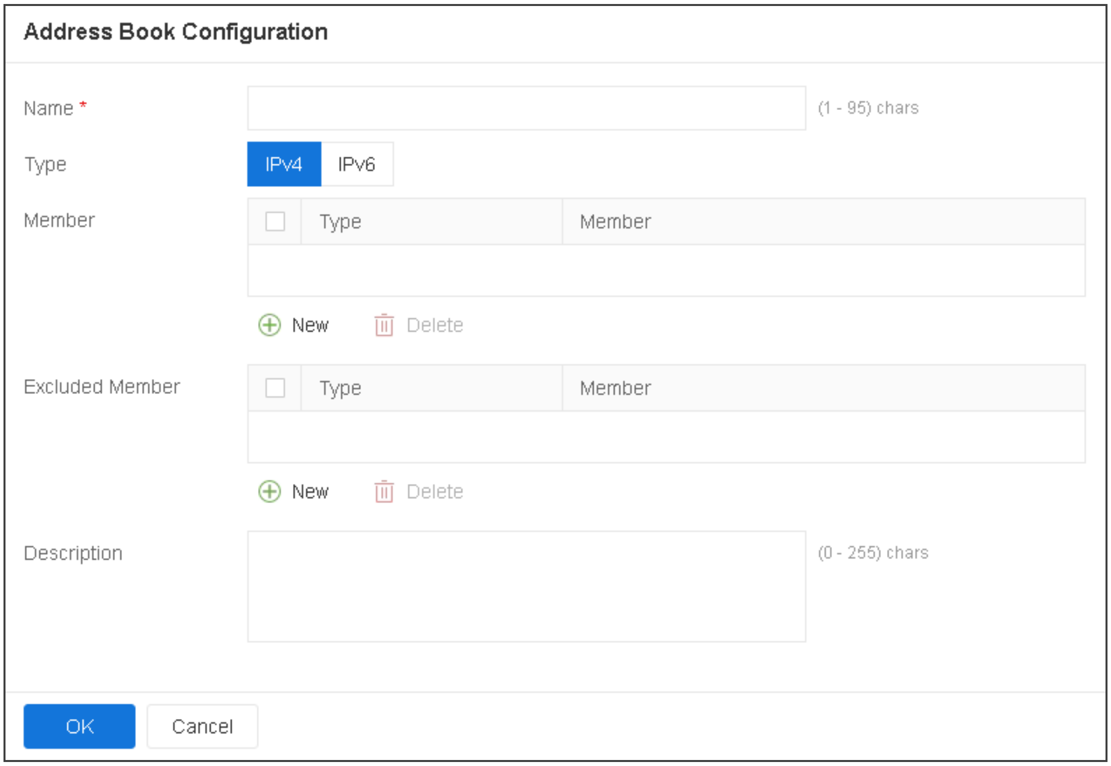
Address book supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry.

Creating an Address Book

To create an address book, take the following steps:

1. Click **Object>Address Book**.

2. Click **New**.



In Address Book Configuration dialog box, enter the address entry configuration.

Basic	
Name	Type the address entry name into the Name box.
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type.
Member	
Member	Click New to add an address entry member . • When you select IPv4 type, configure IP/Netmask, IP Range, Hostname, Address Book, or Coun-

Basic	
	try/Region as needed. • When you select IPv6 type, configure IPv6/prefix, IPv6 Range, Hostname or Address Book as needed. Tips: • Only the security policy and the policy-based route support the address entry with the Country/Region member added. • The address entry with the Country/Region member added does not support the **Excluded Member** settings.
New	Click New to add the configured member to the list below. If it is needed, repeat the above steps to add more members.
Delete	Delete the selected address entry from the list.
Excluded Member	
Member	Specify the excluded member. Click New to add an address entry member , and configure IP/netmask, IP range, Host name or Address entry as needed. **Note**: Excluded members' address range need to be in the address range of the members, otherwise the configuration cannot be completed.
New	Click New to add the configured excluded member to the list below. If needed, repeat the above steps to add more

Basic	
	excluded members.
Delete	Delete the selected excluded member entry from the list.

3. Click OK.

Viewing Details

To view the details of an address entry, take the following steps, including the name, member, description and reference:

1. Click **Object>Address Book**.
2. In the Address Book dialog box, select "+" before an address entry from the member list, and view the details under the entry.

Host Book

You can specify a name to be a collection of one domain name or several domain names, and reference this host book when configuring. Host book is the database to store the relationships of domain integrations and the specified names in system.

The entry of the relationship of domain integrations and the specified name is called host entry.

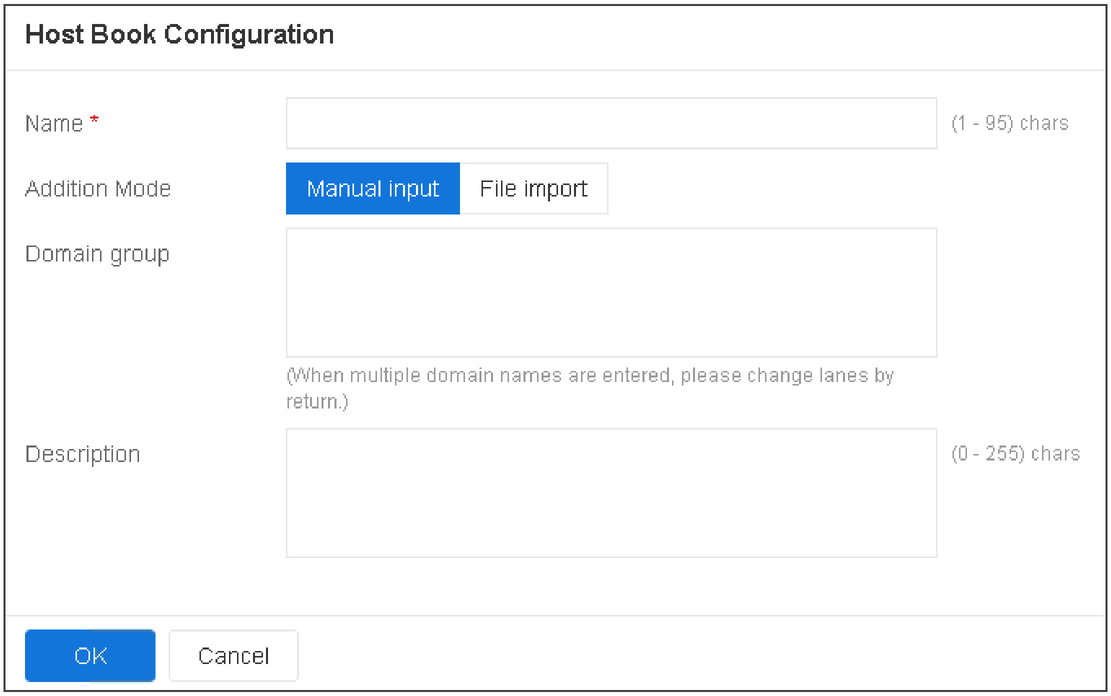
Notes:

- The maximum number of host entries is one fourth of the maximum number of address entries.

Creating a Host Book

To create a host book, take the following steps:

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



(When multiple domain names are entered, please change lanes by return.)

Configure the following options.

Option	Description
Name	Type a name for the host book.
Description	Type the description of host book entry.
Addition Mode	Specify the mode for adding domain members. • Manual input: Add the domain member to the host book via inputting IP address or domain manually. • File import: Add a batch of domain members to the host book via importing the file.
Domain	When the "Manual input" is selected, enter the IP address

Option	Description
Group	or domain names of the domain member. **Note**: Press **Enter** to separate several domain members.
File Name	When the "File import" is selected, click **Browser** to upload a domain name file in the local. **Note:** Only the UTF-8 encoding file (*.txt or *.csv) can be imported currently.

3. Click **OK**.

Editing a Host Book

To edit a host book, take the following steps:

1. Select **Object** > **Host Book**, and enter the **Host Book** page.

2. In the host book list, select a host book entry to edit and click **Edit**.

3. In the **Host Book Configuration** dialog, edit the selected host book entry as needed.

Notes: When you edit a host book entry, if you add more domain members via importing a file, the domain in the file will cover all the domain members in the selected entry.

Deleting a Host Book

To delete a host book, take the following steps:

1. Select **Object** > **Host Book**, and enter the **Host Book** page.

2. In the host book list, select a host book entry to delete and click **Delete**.

Service Book

Service is an information stream designed with protocol standards. Service has some specific distinguishing features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple StoneOS modules including policy rules, NAT rules, QoS rules, etc.

System ships with multiple predefined services/service groups. Besides, you can also customize user-defined services/service groups as needed. All these service/service groups are stored in and managed by StoneOS service book.

Predefined Service/Service Group

System ships with multiple predefined services, and identifies the corresponding application types based on the service ports. The supported predefined services may vary from different Hillstone device models. Predefined service groups contain related predefined services to facilitate user configuration.

User-defined Service

Except for the above predefined services, you can also create your own user-defined services easily. The parameters that will be specified for the user-defined service entries include:

- Name
- Protocol type
- The source and destination port for TCP or UDP service, and the type and code value for ICMP service.

User-defined Service Group

You can organize some services together to form a service group, and apply the service group to StoneOS policies directly to facilitate management. The service group has the following features:

- Each service of the service book can be used by one or more service groups.
- A service group can contain both predefined services and user-defined services.
- A service group can contain another service group. The service group of StoneOS supports up to 8 layers of nests.

The service group also has the following limitations:

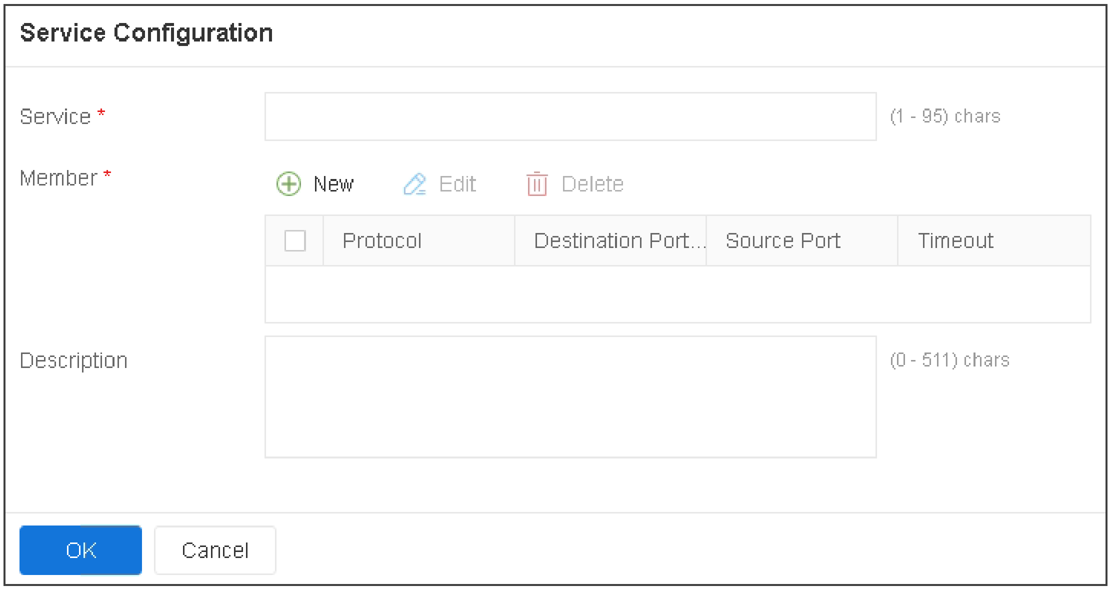
- The name of a service and service group should not be identical.
- A service group being used by any policy cannot be deleted. To delete such a service group, you must first end its relationship with the other modules.
- If a user-defined service is deleted from a service group, the service will also be deleted from all of the service groups using it.

Configuring a Service Book

This section describes how to configure a user-defined service and service group.

Configuring a User-defined Service

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



Configure the following options.

Service Configuration	
Service	Type the name for the user-defined service into the text-box.
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.

Service Configuration		
		The value range is 0 to 65535. Source 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. **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

Service Configuration		
		entry. 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, 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

Service Configuration		
		use "Min" as the single code.
	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） , 100 （Private experimentation） , 101 （Private experimentation） , 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 Information Response） , 141 （Inverse Neighbor Discovery Solicitation Message） , 142 （Inverse Neighbor Dis-

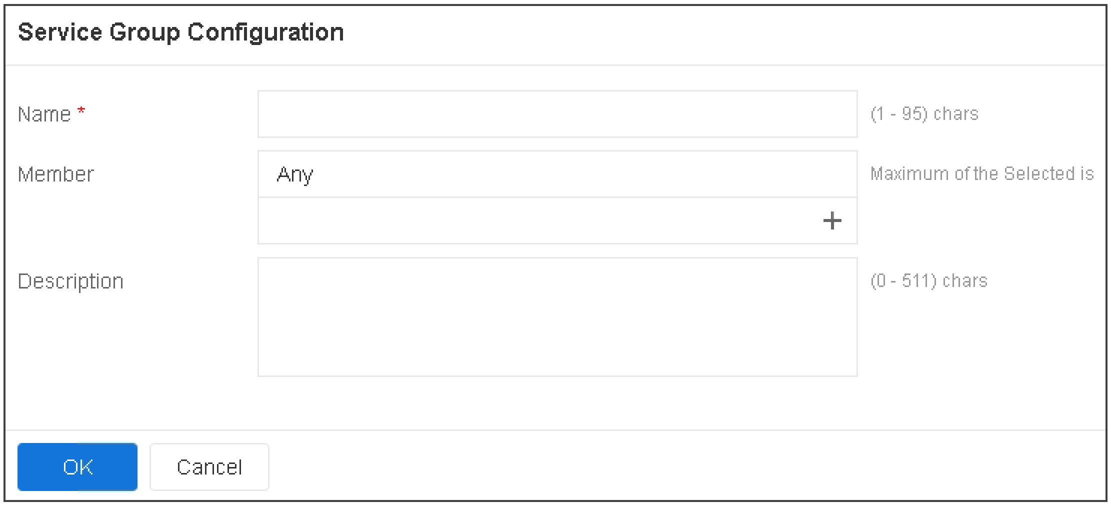
Service Configuration		
		covery Advertisement Message）, 143（Version 2 Multicast Listener Report）, 144（Home Agent Address Discovery Request Massage）, 145（Home Agent Address Discovery Reply Massage）, 146（Mobile Prefix Solicitation）, 147（Mobile Prefix Advertisement ）, 148（Certification Path Solicitation 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.
	All	Protocol: Specifies a protocol number for the service entry. The value range is 1 to 255.
Description	If it's needed, type the description for the service into the text box.	

3. Click **OK**.

Configuring a User-defined Service Group

1. Select **Object** > **Service Book** > **Service Group**.

2. Click **New**.



Service Group Configuration

Name *

Member: Any

Description

Configure the following options.

Service Group Configuration	
Name	Type the name for the user-defined service group into the text box.
Description	If needed, type the description for the service into the text box.
Member Type	Add services or service groups to the service group. System supports at most 8-layer nested service group. Expand Pre-defined Service or User-defined Service from the left pane, select services or service groups, and then

Service Group Configuration	
	click **Add** to add them to the right pane. To remove a selected service, select it from the right pane, and then click **Remove**.

3. Click **OK**.

Viewing Details

To view the details of a service entry, take the following steps, including the name, protocol, destination port and reference:

1. Click **Object>Service Book > Service**.

2. In the service dialog box, select an address entry from the member list, and view the details under the list.

Application Book

Application has some specific features, like corresponding protocol, port number, application type, etc. Application is an essential element for the configuration of multiple device modules including policy rules, NAT rules, application QoS management, etc.

System ships with multiple predefined applications and predefined application groups. Besides, you can also customize user-defined application and application groups as needed. All of these applications and applications groups are stored in and managed by StoneOS application book.

If IPv6 is enabled, IPv6 applications will be recognized by StoneOS.

Editing a Predefined Application

You can view and use all the supported predefined applications and edit TCP timeout, but cannot delete any of them. To edit a predefined application, take the following steps:

1. Select **Object > APP Book > Application**.

2. Select the application you want to edit from the application list, and click **Edit**.

3. In the Application Configuration dialog box, edit TCP timeout for the application.

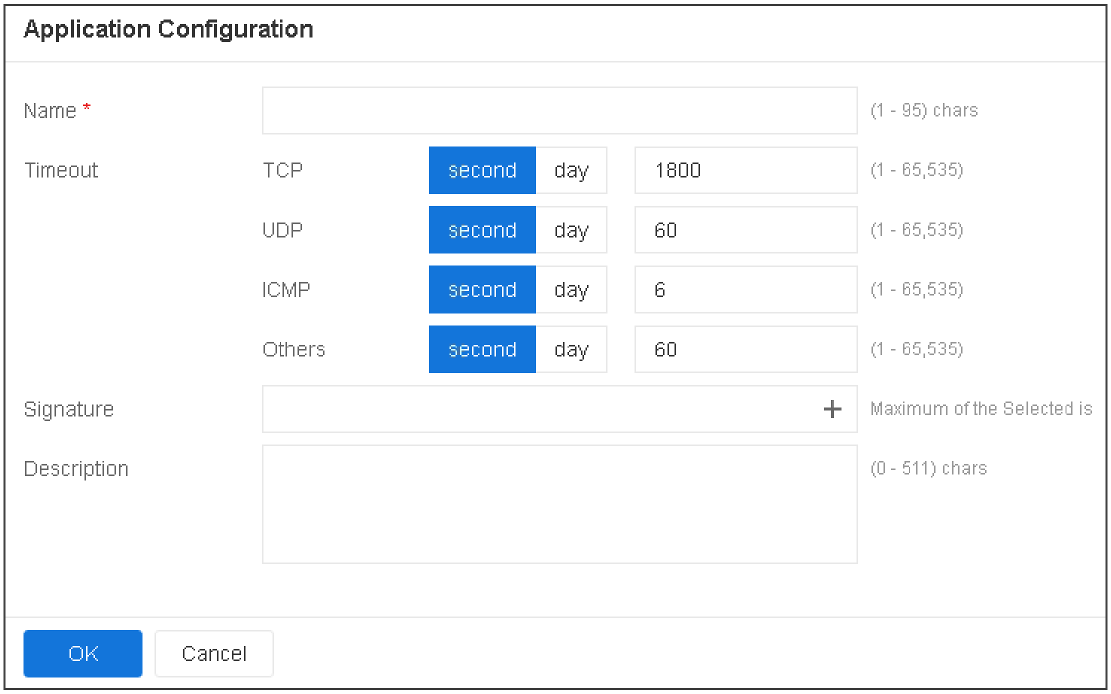
Creating a User-defined Application

You can create your own user-defined applications. By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device, thus identifying the type of the traffic.

To create a user-defined application, take the following steps:

1. Select **Object > APP Book > Application**.

2. Click **New**.



Application Configuration

Name *				(1 - 95) chars
Timeout	TCP	second day	1800	(1 - 65,535)
	UDP	second day	60	(1 - 65,535)
	ICMP	second day	6	(1 - 65,535)
	Others	second day	60	(1 - 65,535)
Signature		+		Maximum of the Selected is
Description				(0 - 511) chars

Configure the following options.

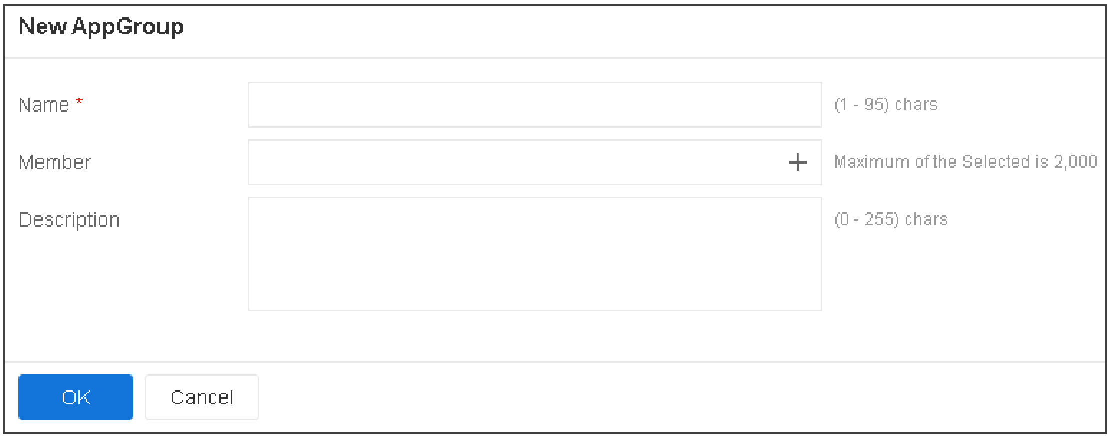
Option	Description
Name	Specify the name of the user-defined application.
Timeout	Configure the application timeout value. If not, system will use the default value of the protocol.
Signature	Select the signature of the application and then click **Add**. To create a new signature, see "Creating a Signature Rule" on Page 556.
Description	Specify the description of the user-defined application.

3. Click **OK**.

Creating a User-defined Application Group

To create a user-defined application group, take the following steps:

1. Select **Object > APP Book > Application Groups**
2. Click **New**.



New AppGroup

Name * (1 - 95) chars

Member Maximum of the Selected is 2,000

Description (0 - 255) chars

Configure the following options.

Option	Description
Name	Specifies a name for the new application group.
Member	Add applications or application groups to the application group. System supports at most 8-layer nested application group. Expand Application or Application Group from the left pane, select applications or application groups, and then click **Add** to add them to the right pane. To remove a selected application or application group, select it from the right pane, and then click **Remove**.
Description	Specifies the description for the application group.

3. Click **OK**.

Creating an Application Filter Group

Application Filter Group allows you to create a group to filter applications according to application category, sub-category, technology, risk, and attributes.

To create an application filter group, take the following steps:

1. Select **Object > APP Book > Application Filters**.
2. Click **New**.
3. Type an application filter group name in the Name text box.
4. Specifies the filter condition. Choose the category, subcategory, technology, risk and characteristic by sequence in the drop-down list. You can click Clear Filter to clear all the selected filter conditions according to your need.
5. Click **OK**.

Creating a Signature Rule

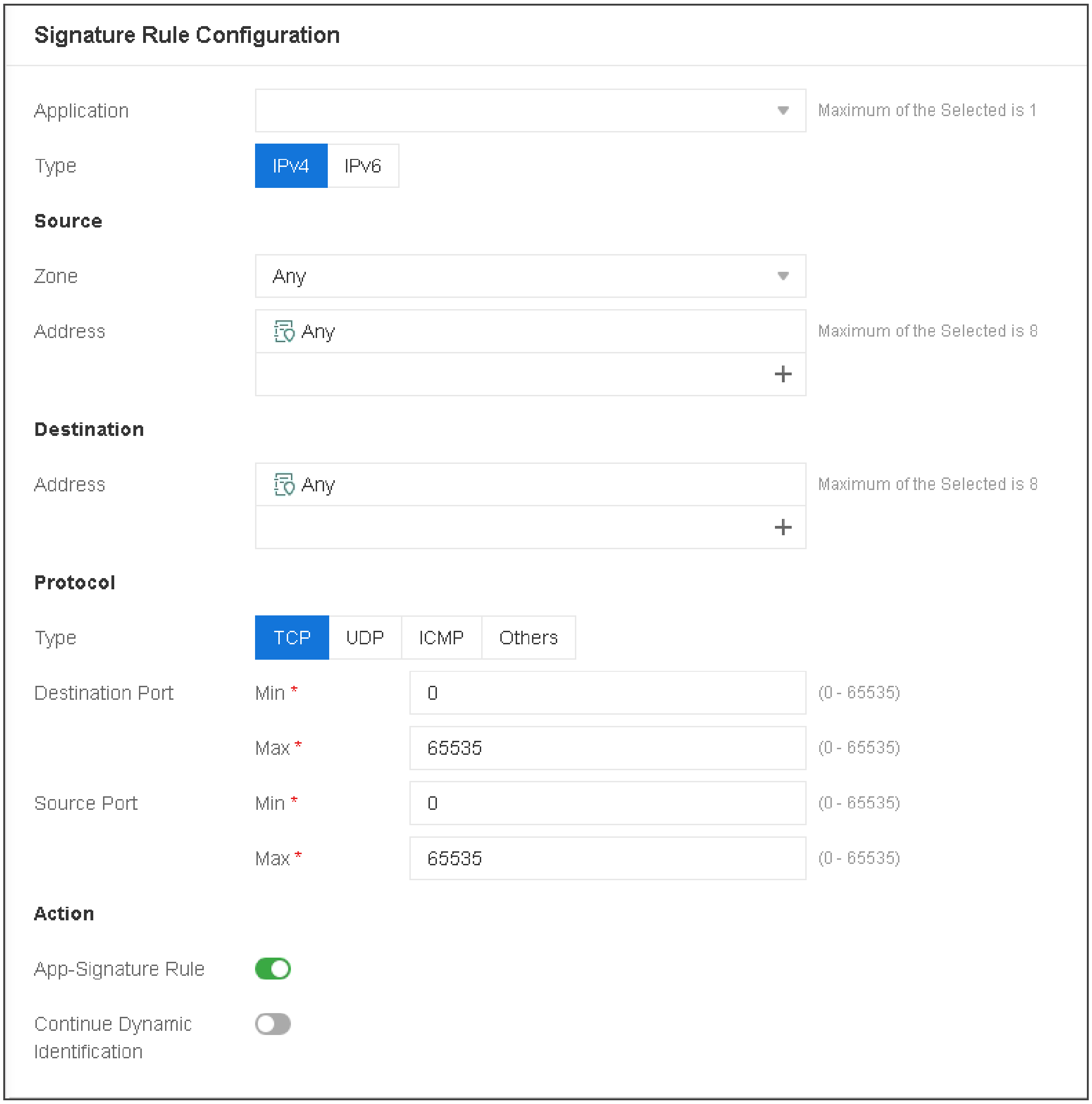
By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device. When the traffic matches all of the conditions defined in the signature rule, it hits this signature rule. Then system identifies the application type.

If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.

To create a new signature rule, take the following steps:

1. Select **Object > APP Book > Static Signature Rule**.

2. Click **New**.



Signature Rule Configuration

Application: Maximum of the Selected is 1

Type: [✓ IPv4] IPv6

Source

Zone: Any

Address: Any — Maximum of the Selected is 8

Destination

Address: Any — Maximum of the Selected is 8

Protocol

Type: [✓ TCP] UDP ICMP Others

Destination Port: Min * 0 (0 - 65535)

Max * 65535 (0 - 65535)

Source Port: Min * 0 (0 - 65535)

Max * 65535 (0 - 65535)

Action

App-Signature Rule: ●

Continue Dynamic Identification: ○

Configure the following options.

Option	Description
Type	Specify the IP address type, including IPv4 and IPv6

Option	Description
	address. If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.
Source	
Zone	Specify the source security zone of the signature rule.
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type.
Destination	
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type.
Protocol	
Enable	Select the **Enable** button to configure the protocol of the signature rule.
Type	When selecting **TCP** or **UDP**, • Destination Port: Specify the destination port number of the user-defined application signature. If the destination port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0.

Option	Description
	- Source Port: Specify the source port number of the user-defined application signature. If the source port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of source port number is 0 to 66535. When selecting **ICMP** or **ICMPv6**: - When IPv4 is selected, select **ICMP**: - Type: Specify the value of the ICMP type of the application signature. The options are as follows: 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

Option	Description
	Reply）. • Min Code: Specify the value of the ICMP code of the application signature. The ICMP code is in the range of 0 to 15. The default value is 0. • When IPv6 is selected, select **ICMPv6**: • Type: Specify the value of the ICMPv6 type of the application signature. The options are as follows: 1（Dest-Unreachable）, 2（Packet Too Big）, 3（Time Exceeded）, 4（Parameter Problem）, 100（Private experimentation）, 101（Private experimentation）, 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

Option	Description
	（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 255（Reserved for expansion of ICMPv6 informational）. • Min Code: Specify the value of the ICMPv6 code of the application signature. The ICMPv6 code is in the range of 0 to 255.

Option	Description
	The default value is 0. When selecting **Others**: • Protocol: Specifies the protocol number of the application signature. The protocol number is in the range of 1 to 255.
Action	
App-Signature Rule	Select **Enable** to make this signature rule take effect after the configurations. Otherwise, it will not take effect.
Continue Dynamic Identification	Without selecting this check box, if the traffic satisfies the user-defined signature rule and system has identified the application type, system will not continue identifying the application. To be more accurate, you can select this check box to set the system to continue dynamically identification.

3. Click **OK**.

Viewing Details

To view the details of an application entry, including the name, category, risk and reference, take the following steps:

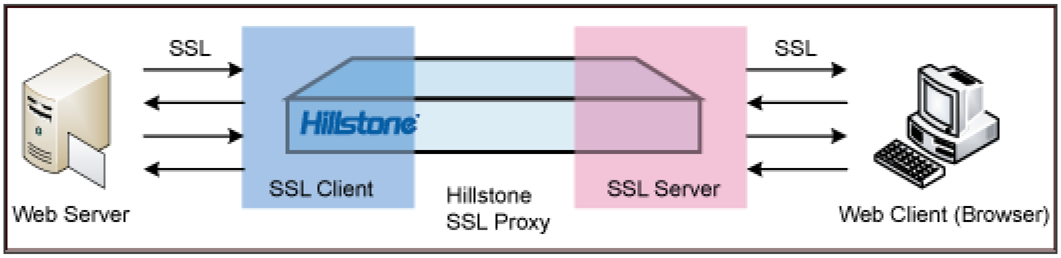
1. Click **Object > APP Book > Application**.
2. In the application dialog box, select "+" before an address entry from the member list, and view the details under the entry.

SSL Proxy

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS/POP3S/SMTPS/IMAPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificates to the client' s Web browser. During the process, the device acts as a SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are two work modes. For the first scenario, the SSL proxy function can work in the client-inspection proxy mode; for the second scenario, the SSL proxy function can work in the server-inspection proxy /offload mode.

When the SSL proxy function works in the client-inspection proxy mode, it can perform the SSL proxy on specified websites.

For the websites that do not need SSL proxy, it dynamically adds the IP address and port of the websites to a bypass list, and the HTTPS/POP3S/SMTPS/IMAPS traffic will be bypassed.

For the websites proxied by the SSL proxy function, the device will check the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS/POP3S/SMTPS/IMAPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS/POP3S/SMTPS/IMAPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS/POP3S/SMTPS/IMAPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list, and the HTTPS/POP3S/SMTPS/IMAPS traffic will be bypassed.

The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic that is not blocked or bypassed.

When the SSL proxy function works in the server-inspection offload mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

You can integrate SSL proxy function with the following:

- Integrate with the application identification function. Devices can decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.
- Support unilateral SSL proxy in WebAuth. SSL client can use SSL connection during authentication stage. When authentication is completed, SSL proxy will no longer take effect, and the client and server communicate directly without SSL encryption.

- Integrate with AV, IPS, Sandbox and URL. Devices can perform the AV protection, IPS protection, Sandbox protection and URL filter on the decrypted HTTPS/POP3S/SMTPS/IMAPS traffic

Working as Gateway of Web Clients

To implement the SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement the SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate, and import a device certificate to the Web browser.

2. Configure a SSL proxy profile, including the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS/POP3S/SMTPS/IMAPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on.

3. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate

- Obtain the CN value of the website certificate

- Import a device certificate to a Web browser

Specifying the PKI Trust Domain of Device Certificate

By default, the certificate of the default trust domain trust_domain_ssl_proxy_2048 will be used to generate the SSL proxy certificate with the Web server certificate together, and then system will issue the generated SSL proxy certificate to the client. You can specify another PKI trust domain in system as the trust domain of the device certificate. The specified trust domain must have a CA certificate, local certificate, and the private key of the local certificate. To specify a trust domain, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-right corner of the page, click **Trust Domain Configuration**.
3. Select a trust domain from the Trust domain drop-down list.
    - The trust domain of trust_domain_ssl_proxy uses RSA and the modulus size is 1024 bits.
    - The trust domain of trust_domain_ssl_proxy_2048 uses RSA and the modulus size is 2048 bits.
4. Click **OK** to save the settings.

Obtaining the CN Value

To get the CN value in the Subject field of the website certificate, take the following steps (take www.gmail.com as the example):

1. Open the IE Web browser, and visit https://www.gmail.com.
2. Click the **Security Report** button (🔒) next to the URL.
3. In the pop-up dialog box, click **View certificates**.
4. In the Details tab, click **Subject**. You can view the CN value in the text box.

Importing Device Certificate to Client Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser.

To export the device certificate to local PC firstly, take the following steps:

1. Export the device certificate to local PC. Select **System > PKI**.
2. In the Management tab in the PKI Management dialog box, configure the options as below:
    - Trust domain: trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048
    - Content: CA certificate
    - Action: Export
3. Click **OK** and select the path to save the certificate. The certificate will be saved to the specified location.

Then, import the device certificate to the client browser. Take Internet Explorer as an example:

1. Open IE.
2. From the toolbar, select **Tools > Internet** Options.
3. In the **Content** tab, click **Certificates**.
4. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab.
5. Click **Import**. Import the certificate following the Certificate Import Wizard.

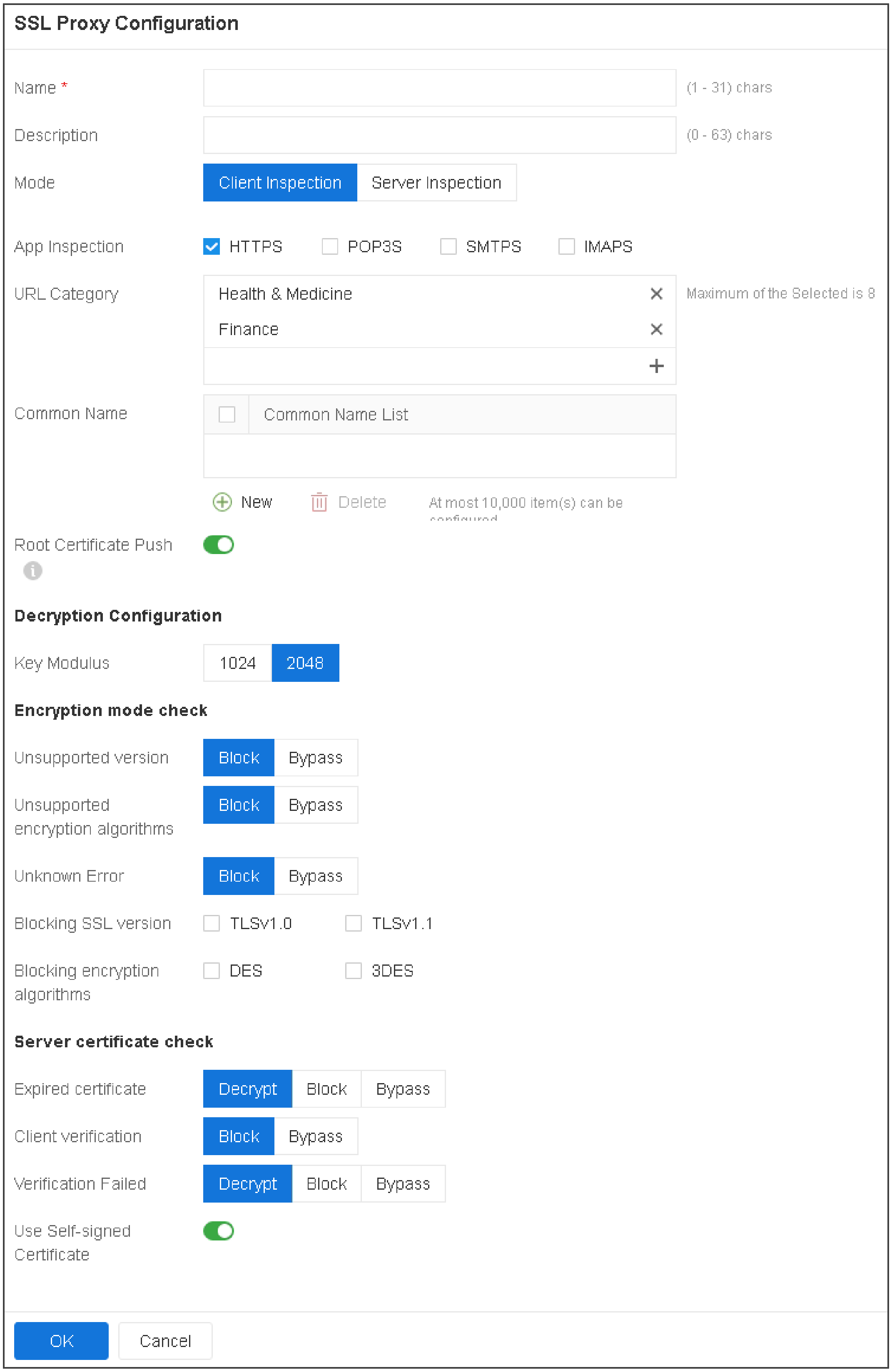
Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS/POP3S/SMTPS/IMAPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on. System supports up to 32 SSL proxy profiles and each profile supports up to 10,000 statistic website entries.

To configure a SSL proxy profile, take the following steps:

1. Click **Object> SSL Proxy**.

2. At the top-left corner, click **New** to create a new SSL proxy profile.



SSL Proxy Configuration

Name * (1 - 31) chars

Description (0 - 63) chars

Mode [✓ Client Inspection] Server Inspection

App Inspection ☑ HTTPS □ POP3S □ SMTPS □ IMAPS

URL Category
- Health & Medicine ✕
- Finance ✕
- +

Maximum of the Selected is 8

Common Name □ Common Name List

⊕ New 🗑 Delete At most 10,000 item(s) can be configured

Root Certificate Push ⓘ: on

Decryption Configuration

Key Modulus 1024 [✓ 2048]

Encryption mode check

Unsupported version [✓ Block] Bypass

Unsupported encryption algorithms [✓ Block] Bypass

Unknown Error [✓ Block] Bypass

Blocking SSL version □ TLSv1.0 □ TLSv1.1

Blocking encryption algorithms □ DES □ 3DES

Server certificate check

Expired certificate [✓ Decrypt] Block Bypass

Client verification [✓ Block] Bypass

Verification Failed [✓ Decrypt] Block Bypass

Use Self-signed Certificate: on

In the Basic tab, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	When the device works as the gateway of Web clients, the SSL proxy function can work in the client-inspection proxy mode. When the device works as the gateway of Web servers, the SSL proxy function can work in the server-inspection offload mode. • In the client-inspection proxy mode, the device does not perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be proxied by SSL proxy function. • In the server-inspection proxy /offload mode, device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.
App Inspection	Select an application to be proxied by the SSL proxy function. Currently, system supports to perform SSL proxy on the HTTPS, POP3S, SMTPS and IMAPS traffic passing through the default port. By default, only the HTTPS traffic will be proxied, but you can select multiple applic-

Option	Description
	ations as needed. To make sure the HTTPS/POP3S/SMTPS/IMAPS traffic passing through user-defined ports will be proxied by the function, you can configure the user-defined ports in **Object > APP Book >** Static Signature Rule. **Note:** Only the predefined applications created in **Object > APP Book >** Application can be proxied by the SSL proxy function.
Common Name	Set the website list based on the work mode. When the SSL proxy is in the Require mode, set the websites that will be proxied by the SSL proxy function. When the SSL proxy is in the Exempt mode, set the websites that will not be proxied by the SSL proxy function and the device will perform the SSL proxy on other websites.To set the website list, click **New** and specify the CN value of the subject field of the website certificate.
Root Certificate Push	Click the **Enable** button to enable the Root Certificate Push. When the HTTPS traffic is decrypted by the SSL proxy function, the Install Root Certificate page will display in your Web browser. In the Install Root Certificate page, you can select **Download** or **Downloaded, Ignored** as needed. • Download: Click the button to download the root certificate to your local PC. For details on import-

Option	Description
	ing a root certificate to your Web browser, refer to Importing Device Certificate to Client Browser. - Downloaded, Ignored: If you click the button, system will no longer push the Install Root Certificate page, and will redirect you to the page you want to visit. **Notes:** - When the Install Root Certificate page displays, if you close the browser, system will still push the page for your next HTTPS request. - You must install the root certificate. If you do not install the root certificate, system will prompt the access is not secure, and the access page may not be loaded completely. Click the **Enable** button to disable the Root Certificate Push. With the function disabled, when the client initiates an HTTPS request: - If the root certificate has been installed in your Web browser, you will be redirected to the page you want to visit. - If the root certificate has not been installed in your Web browser, you will be prompted that the page you're visiting is not secure.

In the Decryption Configuration tab, configure the settings. After system completes the SSL negotiation, the HTTPS/POP3S/SMTPS/IMAPS traffic that is not blocked or bypassed will be decrypted. If the parameters match multiple items in the checklist and you have configured different actions for different items, the Block action will take effect, and the corresponding traffic will be blocked.

Option	Description
Key Modulus	Specify the key pair modulus size of the private/public keys that are associated with the SSL proxy certificate. You can select 1024 bits or 2048 bits.
Encryption mode check	
Unsupported version	Check the SSL protocol version used by the server. • When the SSL protocol used by the SSL server is not supported in system, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When the SSL protocol used by the SSL server is supported, it will continue to check other items.
Unsupported encryption algorithms	Check the encryption algorithm used by the server. • When the encryption algorithm used by the SSL server is not supported in system, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic.

Option	Description
	• When the encryption algorithm used by the SSL server is supported, it will continue to check other items.
Unknown Error	Check the unknown error. • When SSL negotiation fails and the cause of failure can' t be confirmed, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When system do not need check unknown failure, it will continue to check other items.
Blocking SSL version	When the SSL server uses the specified version of SSL protocol, system can block its HTTPS/POP3S/SMTPS/IMAPS traffic.
Blocking encryption algorithm	When the SSL server uses the specified encryption algorithm, system can block its HTTPS/POP3S/SMTPS/IMAPS traffic.
Server certificate check	
Expired certificate	Check the certificate used by the server. When the certificate is overdue, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Decrypt** to decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic.

Option	Description
Client verification	Check whether the SSL server verifies the client certificate. • When the SSL server verifies the client certificate, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When the SSL server does not verify the client certificate, it will continue to check other items.
Verification Failed	Verify the server certificate. You can configure an action for the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified. • Decrypt: Decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified, and select whether to use the self-signed certificate. • Use self-signed certificate: Click the **Enable** button to use the self-signed certificate to complete the SSL negotiation with the Web browser. Then, the browser will prompt a warning message. • Do not use self-signed certificate: Click the **Enable** button to disable the self-signed cer-

Option	Description
	tificate. Then, system will use the trusted certificate "SG6000" to complete the SSL negotiation with the Web browser. If the certificate "SG6000" has been installed, the browser will not prompt a warning message. • Block: Block the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified. • Bypass: Bypass the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified.

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

Working as Gateway of Web Servers

To implement SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

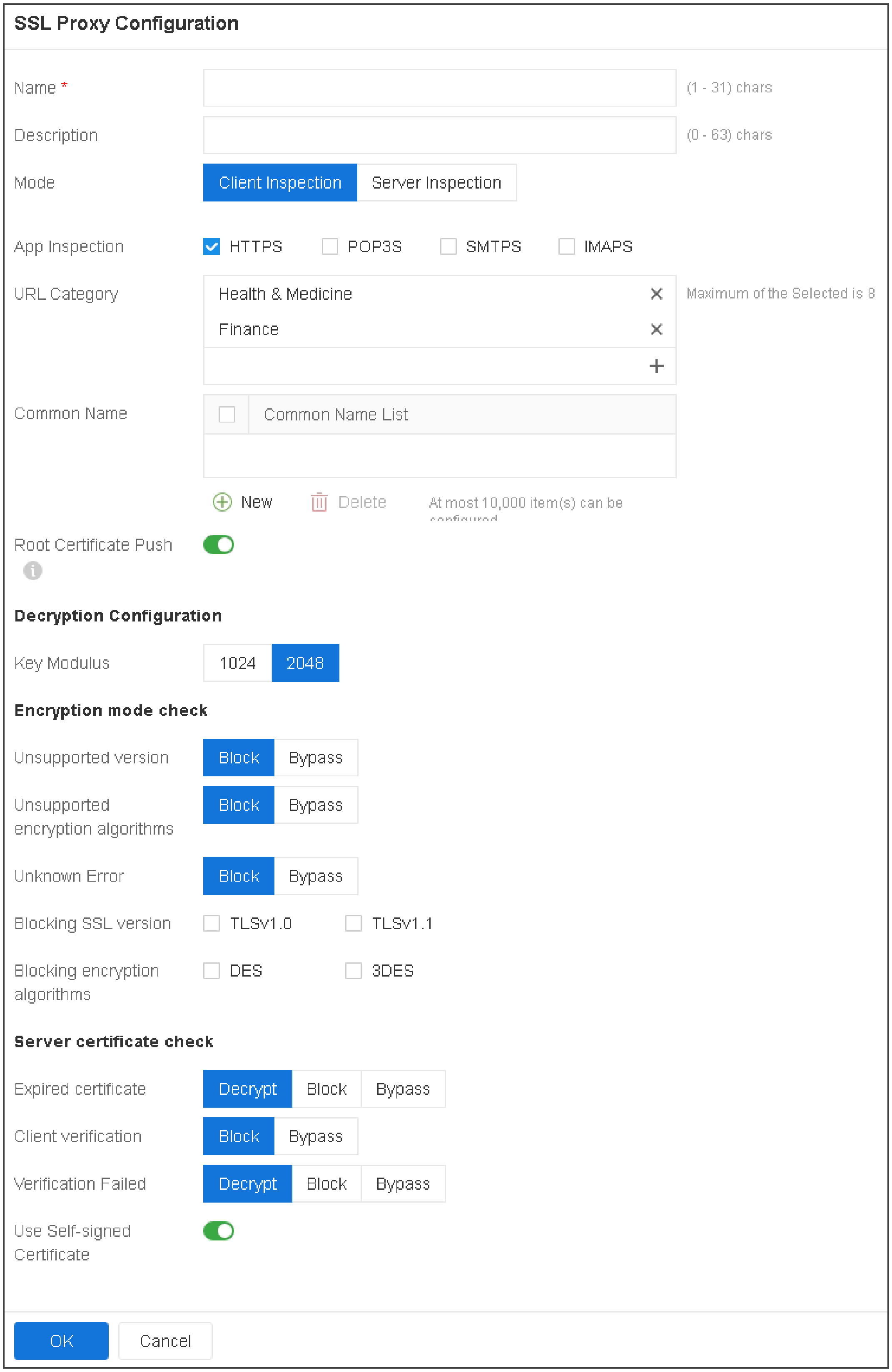
2. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS traffic that matches the policy rule.

Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

To configure a SSL proxy profile, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-left corner, click **New** to create a new SSL proxy profile.



SSL Proxy Configuration

Name * (1 - 31) chars

Description (0 - 63) chars

Mode [✓ Client Inspection] Server Inspection

App Inspection ☑ HTTPS □ POP3S □ SMTPS □ IMAPS

URL Category Maximum of the Selected is 8

- Health & Medicine ✕
- Finance ✕
- +

Common Name

□ Common Name List

⊕ New 🗑 Delete At most 10,000 item(s) can be configured

Root Certificate Push ⓘ ● (on)

Decryption Configuration

Key Modulus 1024 [✓ 2048]

Encryption mode check

Unsupported version [✓ Block] Bypass

Unsupported encryption algorithms [✓ Block] Bypass

Unknown Error [✓ Block] Bypass

Blocking SSL version □ TLSv1.0 □ TLSv1.1

Blocking encryption algorithms □ DES □ 3DES

Server certificate check

Expired certificate [✓ Decrypt] Block Bypass

Client verification [✓ Block] Bypass

Verification Failed [✓ Decrypt] Block Bypass

Use Self-signed Certificate ● (on)

OK Cancel

In this page, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	When the device works as the gatetway of Web servers, the SSL proxy function can work in the Offload mode.
Service Port	Specify the HTTP port number of the Web server.
Server Trust Domain	Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device. For more information about importing the certificate and the key pair, see "PKI" on Page 362. After you complete the importing, select the trust domain used by this SSL Profile.
Warning	Select **Enable** to enable the warning page. When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, system notifies the users that their access to HTTPS websites are being monitored and asks the users to protect their privacy.

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

Binding a SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, see "Security Policy" on Page 768.

SLB Server Pool

The SLB function uses the load balancing algorithm to distribute the traffic and this utilizes the resources of the intranet servers. You can use the following methods to balance the server load:

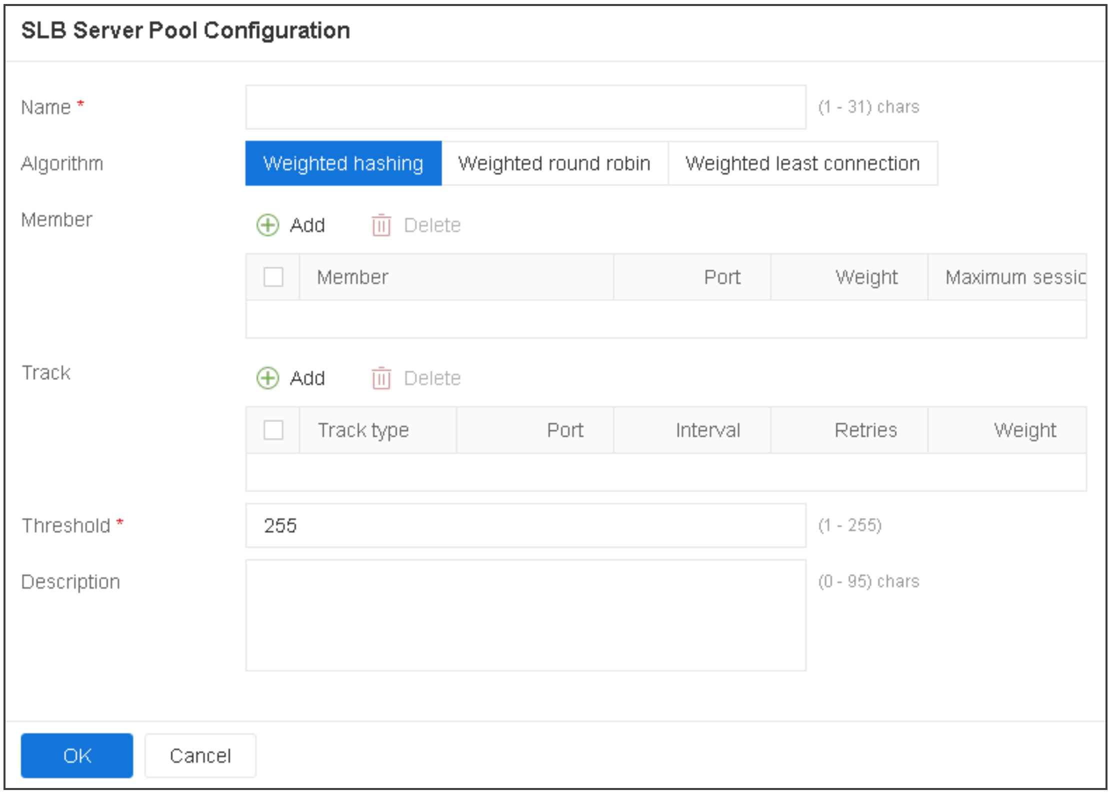
- Distribute the traffic to the specified port of each intranet server. This is applicable to the scenario that different intranet servers provide the same service via specified port at the same time.
- Distribute the traffic to different ports of an intranet server. This is applicable to the scenario that an intranet server provides the same service by running the same process at different ports.
- Combine the above two methods.

Configuring SLB Server Pool and Track Rule

To configure an SLB server pool and track rule, take the following steps:

1. Select **Object > SLB Server Pool**.

2. Click **New**. The SLB Server Pool Configuration dialog box appears.



SLB Server Pool Configuration

Name * (1 - 31) chars

Algorithm: Weighted hashing | Weighted round robin | Weighted least connection

Member: Add Delete

□	Member	Port	Weight	Maximum sessic

Track: Add Delete

□	Track type	Port	Interval	Retries	Weight

Threshold * 255 (1 - 255)

Description (0 - 95) chars

OK Cancel

In the SLB Server Pool Configuration dialog box, configure the following options.

Option	Description
Name	Specifies the name of the SLB server pool
Algorithm	Select an algorithm for load balancing.
Member	Specifies the member of the pool. You can type the IP range or the IP address and the netmask.
Port	Specifies the port number of the server.
Maximum Sessions	Specifies the allowed maximum sessions of the server. The value ranges from 0 to 1,000,000,000. The default value is 0, which represents no limitation.

Option	Description
Weight	Specifies the traffic forwarding weight during the load balancing. The value ranges from 1 to 255.
Add	Add the SLB address pool member to the SLB server pool. You can add up to 256 members.
Track	
Track Type	Selects a track type.
Port	Specifies the port number that will be tracked. The value ranges from 1 to 65535. • When the members in the SLB server pool have the same IP address and different ports, you don’ t need to specify the port when configuring the track rule. System will track each IP address and its port in the SLB server pool. • When there is a member whose port is not configured exists in the SLB sever pool, you must specify the port when configuring the track rule. System will track the specified port of the IP addresses in the SLB server pool. • When the members in the SLB server pool are all configured with IP addresses and ports and these configured IP addresses are different from each other, you can select whether to specify the port when configuring the track rule. If specified, sys-

Option	Description
	tem will track the specified port of these IP addresses. If not, system will track the configured ports of the IP addresses of the members.
Interval	Specifies the interval between each Ping/TCP/UDP packet. The unit is second. The value ranges from 3 to 255.
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.
Weight	Specifies a weight for the overall failure of the whole track rule if this track entry fails. The value range is 1 to 255.
Add	Click **Add** to add the configured track rule to the list.
Threshold	Types the threshold for the track rule into the **Threshold** box. The value range is 1 to 255. If the sum of weights for failed entries in the track rule exceeds or equals the threshold, system will conclude that the track rule fails.
Description	Types the description for this track rule.

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

Viewing Details of SLB Pool Entries

To view the details of the servers in the SLB pool, take the following steps:

1. Click **Object > SLB Server Pool**.
2. Select "+" before an SLB pool entry.
3. In the Server List tab under the entry, view the information of the servers that are in this SLB pool.
4. In the Monitoring tab, view the information of the track rules.
5. In the Referenced tab, view the DNAT rules that use the SLB pool.

Schedule

System supports a schedule. This function allows a policy rule to take effect in a specified time and controls the duration of the connection between a PPPoE interface and the Internet. The schedule consists of a periodic schedule and an absolute schedule. The periodic schedule specifies a time point or time range for periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Periodic Schedule

Periodic schedule is the collection of periods specified by all of the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into 3 types:

- Daily: The specified time of every day, such as Everyday 09:00:30 to 18:00:20.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00:15 to 13:30:45.
- Period: A continuous period during a week, such as from Monday 09:30:30 to Wednesday 15:00:05.

Absolute Schedule

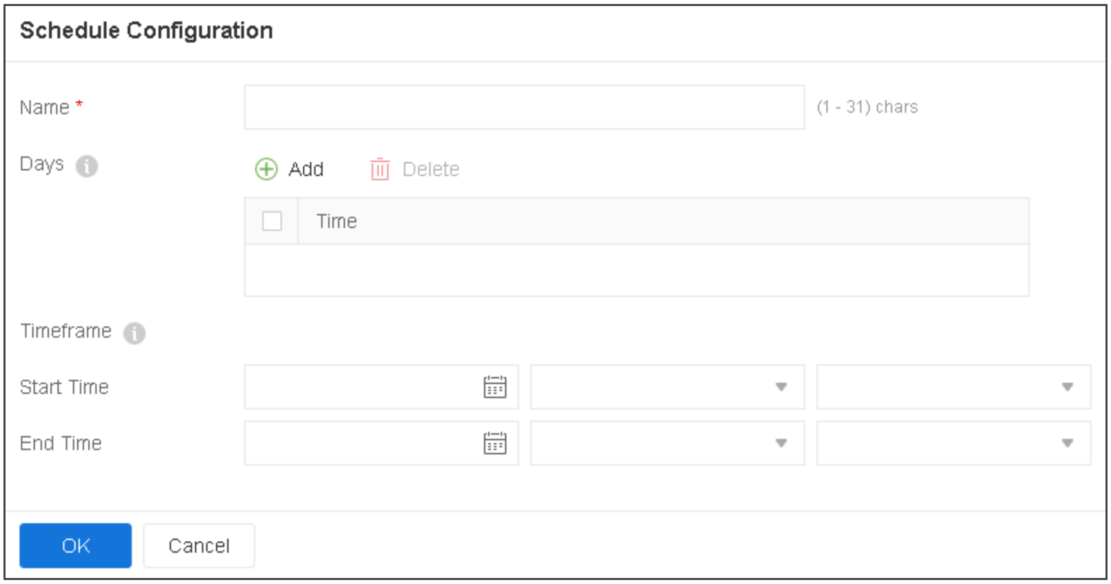
An absolute schedule is a time range in which a periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is used by some module.

Creating a Schedule

To create a schedule, take the following steps:

1. Select **Object > Schedule**.

2. Click **New**.



Configure the following options.

Schedule Configuration Dialog Box		
Name	Specifies a name for the new schedule.	
Add	Specifies a type for the periodic schedule in Add Periodic Schedules section.	
	Type	• Daily - The specified time of every day. Click this radio button, and then, in the Time section, select a start time and end time from the Start time and End time drop-down list respectively. • Days - The specified time of a specified day during a week. Click this

Schedule Configuration Dialog Box		
		radio button, and then select a day/days in the Days and Time section, and finally select a start time and end time from the Start time and End time drop-down list respectively. • Duration - A continuous period during a week. Click this radio button, and then in the Duration section select a start day/time and end day/time from the Start time and End time drop-down list respectively.
	Preview	Preview the detail of the configured periodic schedule in the Preview section.
Delete	Select the entry you want to delete from the period schedule list below, and click **Delete**.	
Absolute Schedule	The absolute schedule decides a time range in which the periodic schedule will take effect. Without configuring an absolute schedule, the periodic schedule will take effect as soon as it is used by some module.	

3. Click **OK**.

Notes: In both absolute schedule and periodic schedule, the interval between the Start time and the End time should not be less than 1 minute.

AAA Server

An AAA server is a server program that handles user requests to access computer resources, and for an enterprise, this server provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

Here in StoneOS system, authentication supports the following five types of AAA server:

- Local server: a local server is the firewall itself. The firewall stores user identity information and handles requests. A local server authentication is fast and cheap, but its storage space is limited by the firewall hardware size.
- External servers:
    - Radius Server
    - LDAP Server
    - Active-Directory Server
    - TACACS+ Server

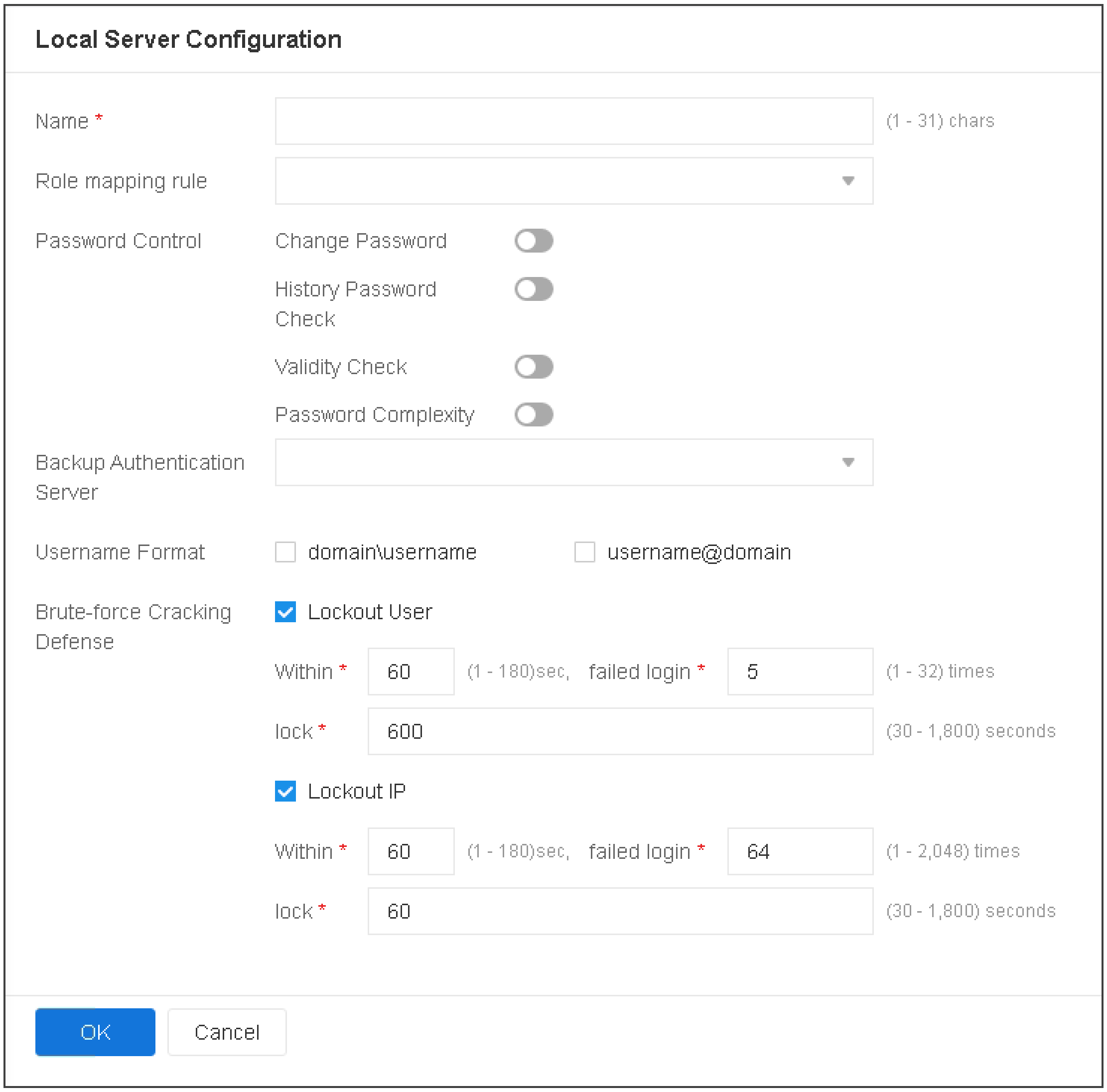
According to the type of authentication, you need to choose different AAA servers:

- "802.1x" on Page 355 : Only local and Radius servers support these two types of authentication.
- "Configuring IPSec-XAUTH Address Pool" on Page 407: Local, Radius, Ldap, AD and Tacacs+ servers are supported.
- Other authentication methods mentioned in this guide: all four servers can support the other authentication methods.

Configuring a Local AAA Server

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

2. The **Local Server Configuration** page opens.



Local Server Configuration

Name * [ ] (1 - 31) chars

Role mapping rule [▾]

Password Control
Change Password ○
History Password Check ○
Validity Check ○
Password Complexity ○

Backup Authentication Server [▾]

Username Format □ domain\username □ username@domain

Brute-force Cracking Defense ☑ Lockout User
Within * 60 (1 - 180)sec, failed login * 5 (1 - 32) times
lock * 600 (30 - 1,800) seconds
☑ Lockout IP
Within * 60 (1 - 180)sec, failed login * 64 (1 - 2,048) times
lock * 60 (30 - 1,800) seconds

OK Cancel

Configure the following.

Option	Description
Name	Type the name for the new server into the text box.

Option	Description
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.
Password Control	To prevent account security problem, you can configure the password control function. • Change Password: Selects the **Change Password** check box. With this function enabled, the system allows users to change their own passwords after the successful WebAuth or SCVPN authentication. • History Password Check: Select the **History Password Check** check box to enable the history password check function. With the function, system will verify the new password with the historical passwords when you change the password, ensuring the new password is different from the passwords set in the specified times. • Validity Check: Select the **Validity Check** check box to enable the password validity check function and configure the valid period of password. • Password Expiry Warning: Select the **Password Expiry Warning** check box to enable the pass-

Option	Description
	word expiry warning function and configure the days how long users will be reminded of password expiry before it expities. • Password Complexity: The lower the complexity of the password, the more likely it is to be cracked, such as including the username and short password length. For security reasons, you can enable the password complexity configuration and configure the password complexity requirements to ensure that the user's password has high complexity. Select the **Password Complexity** check box to enable the password complexity configuration. • Minimum Password Length: Specify the minimum password length, the range is 1-16, the default value is 1. • Minimum Capital Letter Length: Specifies the minimum length of uppercase letters contained in the password. The range is 0-16. The default value is 0. • Minimum Lowercase Letter Length: Specifies the minimum length of lowercase letters contained in the password. The range

Option	Description
	is 0-16. The default value is 0. • Minimum Number Length: Specifies the minimum length of the number contained in the password. The range is 0-16. The default value is 0. • Minimum Special Character Length: Specifies the minimum length of the password containing special characters (that is, non-numeric characters), the range is 0-16, and the default value is 0. • Password cannot contain username: Select the **Password cannot contain username** checkbox. Passwords are not allowed to contain username. • Change Password after First Login: By default, the function of changing the password for the first login is disabled. After the function of changing the password for the first login is enabled, when you log in for web authentication or SSL VPN for the first time, system will prompt the user to "Change the password for the first login" to force you to change the password according to the configured password complexity.
Backup	To configure a backup authentication server, select a

Option	Description
Authentication Server	server from the drop-down list. After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Username Format	Specifies the input format of the user name.
Brute-force Cracking Defense	To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP. • Select the **Lockout User** check box to enable the user-based brute-force cracking defense. If the failed attempts reached the specified times (1-32 times) within the specified period (1-180 seconds), the login user will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the failed attempts reached 5 times, the login user will be locked out for 600 seconds. • Select the **Lockout IP** check box to enable the IP-based brute-force cracking defense. If the failed attempts reached the specified times (1-

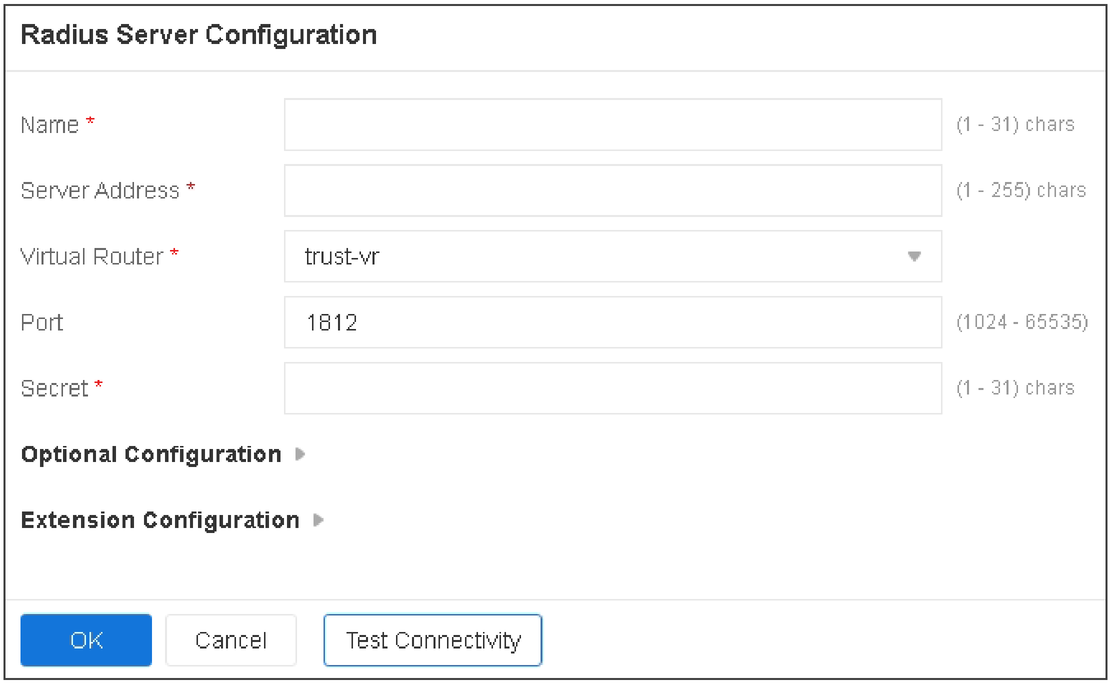
Option	Description
	2048 times) within the specified period (1-180 seconds), the IP will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the failed attempts reached 64 times, the IP will be locked out for 60 seconds.

3. Click **OK**.

Configuring Radius Server

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

2. The **Radius Sever Configuration** page opens.



Radius Server Configuration

Name * (1 - 31) chars

Server Address * (1 - 255) chars

Virtual Router * trust-vr

Port 1812 (1024 - 65535)

Secret * (1 - 31) chars

Configure the following.

Basic Configuration	
Name	Specifies a name for the Radius server.
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the Radius server.
Virtual Router	Specifies a VR for the Radius server.
Port	Specifies a port number for the Radius server. The value range is 1024 to 65535. The default value is 1812.
Secret	Specifies a secret for the Radius server. You can specify at most 31 characters.
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.

Basic Configuration	
	- By default, the authorization policy is disabled. Select the checkbox after **Authorization 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 Format	Specifies the input format of the user name.
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.

<table>
<tr><th colspan="2">Basic Configuration</th></tr>
<tr><td>Virtual Router1/ Virtual Router2</td><td>Specifies a VR for the backup server.</td></tr>
<tr><td>Retries</td><td>Specifies a retry time for the authentication packets sent to the AAA server. The value range is 1 to 10. The default value is 3.</td></tr>
<tr><td>Timeout</td><td>Specifies a timeout for the server response. The value range is 1 to 30 seconds. The default value is 3.</td></tr>
<tr><td>Backup Authentication Server</td><td>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.</td></tr>
<tr><td>Enable Accounting</td><td>Select the <b>Enable</b> checkbox to enable accounting for the Radius server, and then configure options in the sliding out area.
<table>
<tr><td>Server Address</td><td>Specifies an IP address or domain name for the accounting server.</td></tr>
<tr><td>Virtual Router</td><td>Specifies a VR for the accounting server.</td></tr>
</table></td></tr>
</table>

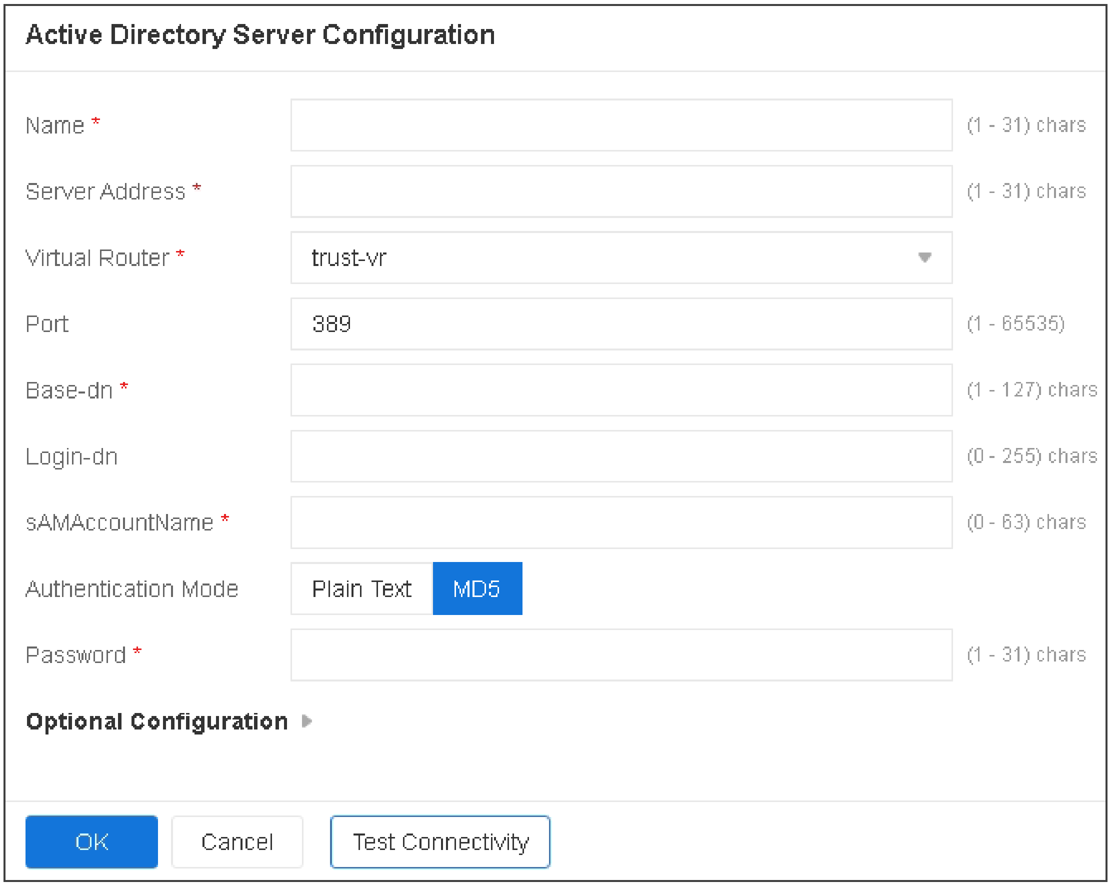
Basic Configuration		
	Port	Specifies a port number for the accounting server. The value range is 1024 to 65535. The default value is 1813.
	Password	Specifies a password for the accounting server.
	Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
	Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.
Extension Configuration		
Extended Password Encryption Algorithm	Specifies the SM4 extended password encryption algorithm for the Radius server. After configuration, the Radius server will use SM4 for the encrypted storage and encrypted transmission of passwords.	

3. Click **OK**.

Configuring Active Directory Server

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

2. The **Active Directory Server Configuration** page opens.



Active Directory Server Configuration

Name * (1 - 31) chars

Server Address * (1 - 31) chars

Virtual Router * trust-vr

Port 389 (1 - 65535)

Base-dn * (1 - 127) chars

Login-dn (0 - 255) chars

sAMAccountName * (0 - 63) chars

Authentication Mode Plain Text [✓ MD5]

Password * (1 - 31) chars

Optional Configuration ▸

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.

Basic Configuration	
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 request. For the example of abc.xyz.com as described above, the format for the Base-dn is "dc=aabc,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=aadministrator,cn=users,dc=abc,dc=xyz,dc=com".
sAMAccountName	When the authentication mode is MD5, the sAMAccountName should be configured. sAMAccountName 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

Basic Configuration	
	sAMAccountName should be "administrator".
Authentication Mode	Specifies an authentication or synchronization method (either plain text or MD5). The default 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.
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 author-

Basic Configuration	
	ization policy will be deleted automatically. • By default, the authorization policy is disabled. Select the checkbox after **Authorization 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 Format	Specifies the input format of the user name.
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.

Basic Configuration	
Virtual Router1/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. 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 30 to 1440 minutes. The default value is 30.

Basic Configuration		
	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 with the local server based on the group.	
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 punc-	

Basic Configuration	
	tuation) 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: 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.).
Security Agent	Select the **Enable** check box to enable the Security Agent. With this function enabled, system will be able to obtain the mappings between the usernames of the domain users and IP addresses from the AD server, so that the domain users can gain access to network resources. In this way "1Single Sign-On" on

<table>
<tr><th colspan="2">Basic Configuration</th></tr>
<tr><td></td><td>Page 314 is implemented. Besides, by making use of the obtained mappings, system can also implement other user-based functions, like security statistics, logging, behavior auditing, etc. To enable the Security Agent on the AD server, you first need to install and run the Security Agent on the server. Afterwards, when a domain user is logging in or logging off, the Security Agent will log the user's username, IP address, current time, and other information, and it will add the mapping between the username and the IP address to system. In this way the system can obtain every online user's IP address.</td></tr>
<tr><td></td><td><table>
<tr><td>Agent Port</td><td>Specify the monitoring port. StoneOS communicates with the AD Agent through this port. The range is 1025 to 65535. The default value is 6666. This port must be matched with the configured port of AD Agent, or system will fail to communicate with the AD Agent.</td></tr>
<tr><td>Disconnection Timeout</td><td>Specifies the disconnection timeout. The value range is 0 to</td></tr>
</table></td></tr>
</table>

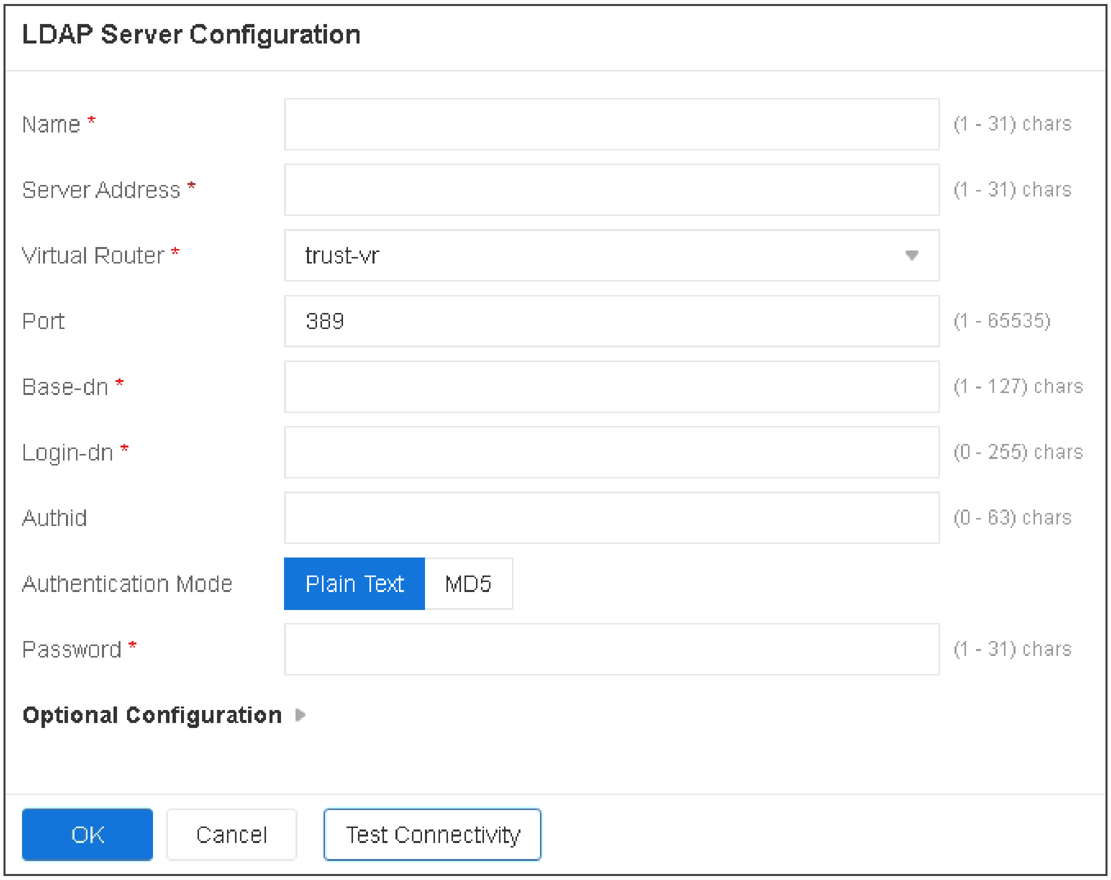
Basic Configuration	
	1800 seconds. The default value is 300. The value of 0 indicates never timeout.
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication 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.

3. Click **OK**.

Configuring LDAP Server

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

2. The **LDAP Server Configuration** page opens.



LDAP Server Configuration

Name * (1 - 31) chars

Server Address * (1 - 31) chars

Virtual Router * trust-vr

Port 389 (1 - 65535)

Base-dn * (1 - 127) chars

Login-dn * (0 - 255) chars

Authid (0 - 63) chars

Authentication Mode [✓ Plain Text] MD5

Password * (1 - 31) chars

Optional Configuration ▸

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.

Basic Configuration	
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 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.
Optional Configuration	
Username Format	Specifies the input format of the user name.
Role Mapping	Specifies a role mapping rule for the server. With this

<table>
<tr><th colspan="2">Basic Configuration</th></tr>
<tr><td>Rule</td><td>option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.</td></tr>
<tr><td>Backup server 1/Backup server 2</td><td>Specifies an IP address or domain name for backup server 1 or backup server 2.</td></tr>
<tr><td>Virtual Router-1/Virtual Router2</td><td>Specifies a VR for the backup server.</td></tr>
<tr><td>Synchronization</td><td>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.</td></tr>
<tr><td>Automatic Synchronization</td><td>Click the radio button to specify the automatic synchronization.
<table>
<tr><td>Interval Synchronization</td><td>Specifies the time interval for automatic synchronization. The value range is 30 to 1440 minutes. The default value is 30.</td></tr>
<tr><td>Daily Syn-</td><td>Specifies the time when the user</td></tr>
</table></td></tr>
</table>

Basic Configuration		
	chronization	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. 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.	
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.	

Basic Configuration	
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. 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	Specifies a backup authentication server. After con-

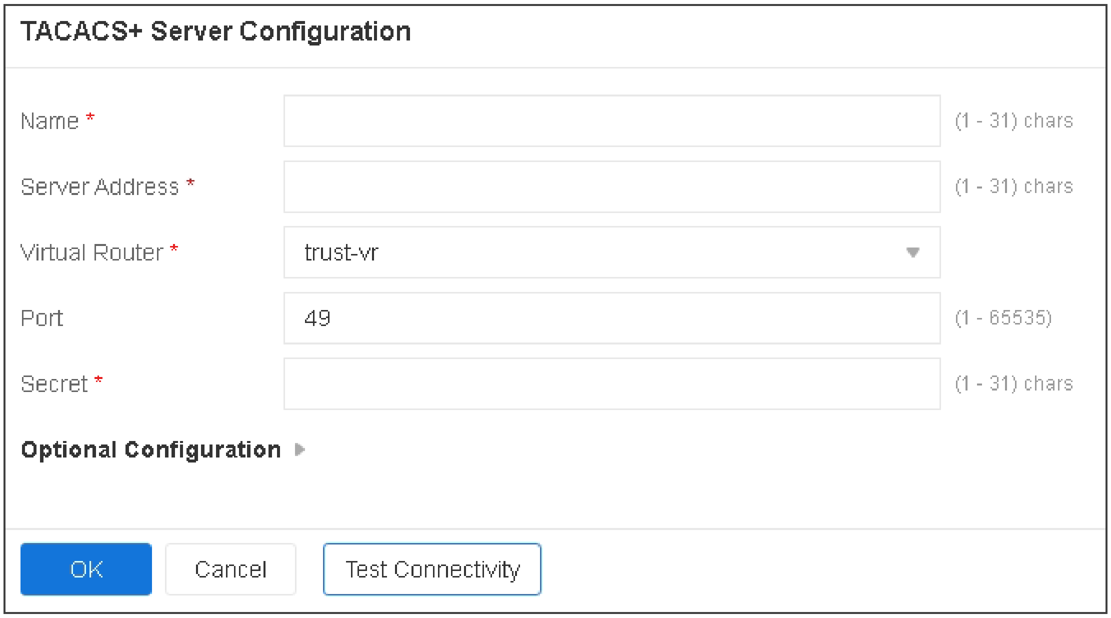
Basic Configuration	
Server	figuring a backup authentication server for the LDAP server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.

3. Click **OK**.

Configuring TACACS+ Server

1. Select **Object** > **AAA Server**.

2. Click **New** > **TACACS+ Server**, and the **TACACS+ Server Configuration** page opens.



TACACS+ Server Configuration

Name *		(1 - 31) chars
Server Address *		(1 - 31) chars
Virtual Router *	trust-vr	
Port	49	(1 - 65535)
Secret *		(1 - 31) chars

Configure the following.

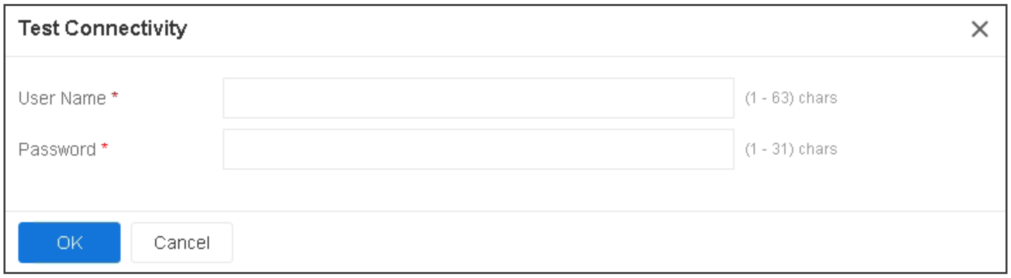
Basic Configuration	
Server Name	Enter a name for the TACACS+ server.
Server Address	Specify the IP address or host name for the TACACS+ server.
Virtual Router	Specify the VRouter of TACACS+ server.
Port	Enter port number for the TACACS+ server. The default value is 49. The value range is 1 to 65535.
Secret	Enter the shared secret to connect the TACACS+ server.
Optional	
Username Format	Specifies the input format of the user name.
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 domain name or IP address for the backup TACACS+ server.
Virtual Router 1 (2)	Select the VRouter for the backup server.

Connectivity Test

When AAA server parameters are configured, you can test if they are correct by testing server connectivity.

To test server connectivity, take the following steps:

1. Select **Object > AAA Server**, and click **New**.
2. Select your AAA server type, which can be Radius, AD, LDAP or TACACS+. The local server does not need the connectivity test.
3. After filling out the fields, click **Test Connectivity**.
4. For Radius or TACACS+ server, enter a username and password in the popped <Test Connectivity> dialog box. If the server is AD or LDAP, the login-dn and secret is used to test connectivity.



Test Connectivity

User Name * (1 - 63) chars

Password * (1 - 31) chars

5. Click **Test Connectivity**. If "Test connectivity success" message appears, the AAA server settings are correct.

If there is an error message, here are the causes:

- Connect AAA server timeout: Wrong server address, port or virtual router.
- AAA server configuration error: Secret is wrong.
- Wrong name or password: Username or password for testing is wrong.

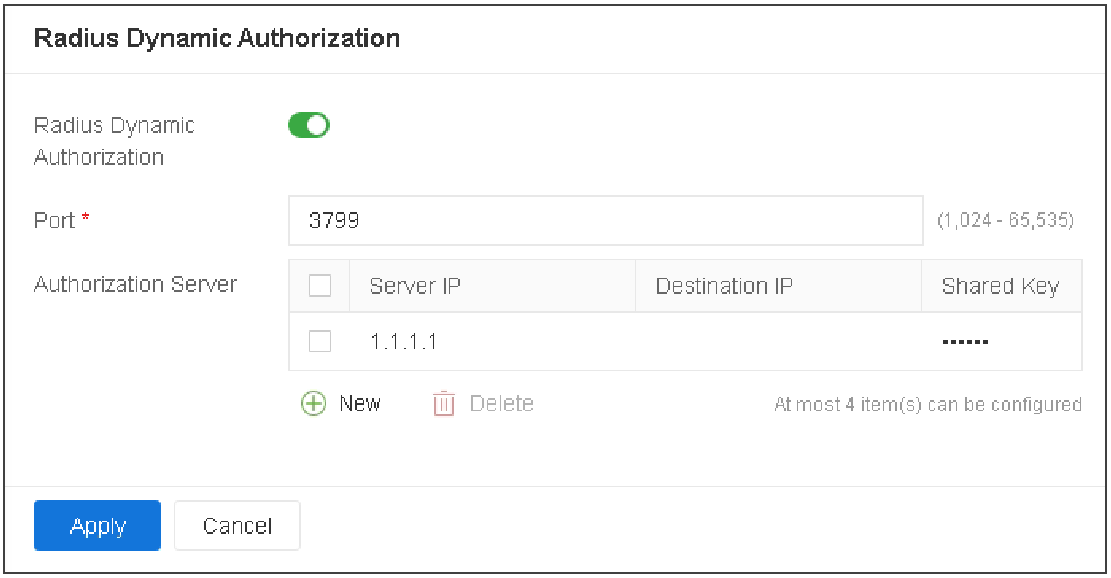
Radius Dynamic Authorization

The Radius dynamic authorization function, includes:

- When the user is authenticated successfully, the Radius server can send a Radius CoA (Change of Authorization) request message to the authority of the authenticated user to the device. The device automatically generates the security policy rule for the user. When the user goes offline, the device delete this user's security policy rule automatically
- When the SCVPN user is authenticated successfully, the Radius server can send a Radius DM (Disconnect Messages) request message to send the accounting user information (including the user name, user IP address, user accounting ID, etc.) to the device, and the device can disconnect the specified scvpn authentication user and end the accounting.

To configure the Radius dynamic authorization function, take the following steps:

1. Select **Object** > **Radius Dynamic Authorization**.



Radius Dynamic Authorization

Radius Dynamic Authorization: ●

Port *: 3799 (1,024 - 65,535)

Authorization Server

□	Server IP	Destination IP	Shared Key
□	1.1.1.1		······

At most 4 item(s) can be configured

2. Click the **Enable** button after **Radius Dynamic Authorization** to enable the Radius dynamic authorization function.

3. Type the port number of the Radius dynamic authorization server into the **Port** textbox. The value range is 1024 to 65535. The default value is 3799.

4. In the Authorization Server section, click **New**, and then specify the IP address, destination IP and shared key of the Radius dynamic authorization server.

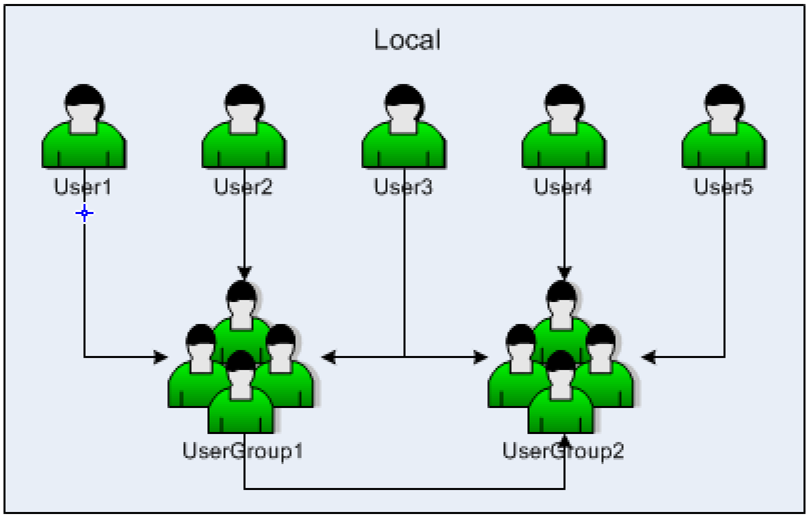
5. To delete the Radius dynamic authorization server, select the checkbox in the list, and then click **Delete**.

6. Click **Apply**.

Notes: If you need to use the Radius dynamic authorization function, first enable and configure the Radius accounting server. For the configuration, refer to Enable Accounting.

User

User refers to the user who uses the functions and services provided by the Hillstone device, or who is authenticated or managed by the device. The authenticated users consist of local user and external user. The local users are created by administrators. They belong to different local authentication servers, and are stored in system's configuration files. The external users are stored in external servers, such as AD server or LDAP server. System supports User Group to facilitate user management. Users belonging to one local authentication server can be allocated to different user groups, while one single user can belong to different user groups simultaneously; similarly, user groups belonging to one local authentication server can be allocated to different user groups, while one single user group can belong to different user groups simultaneously. The following diagram uses the default AAA server, Local, as an example and shows the relationship between users and user groups:



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Configuring a Local User

This section describes how to configure a local user and user group.

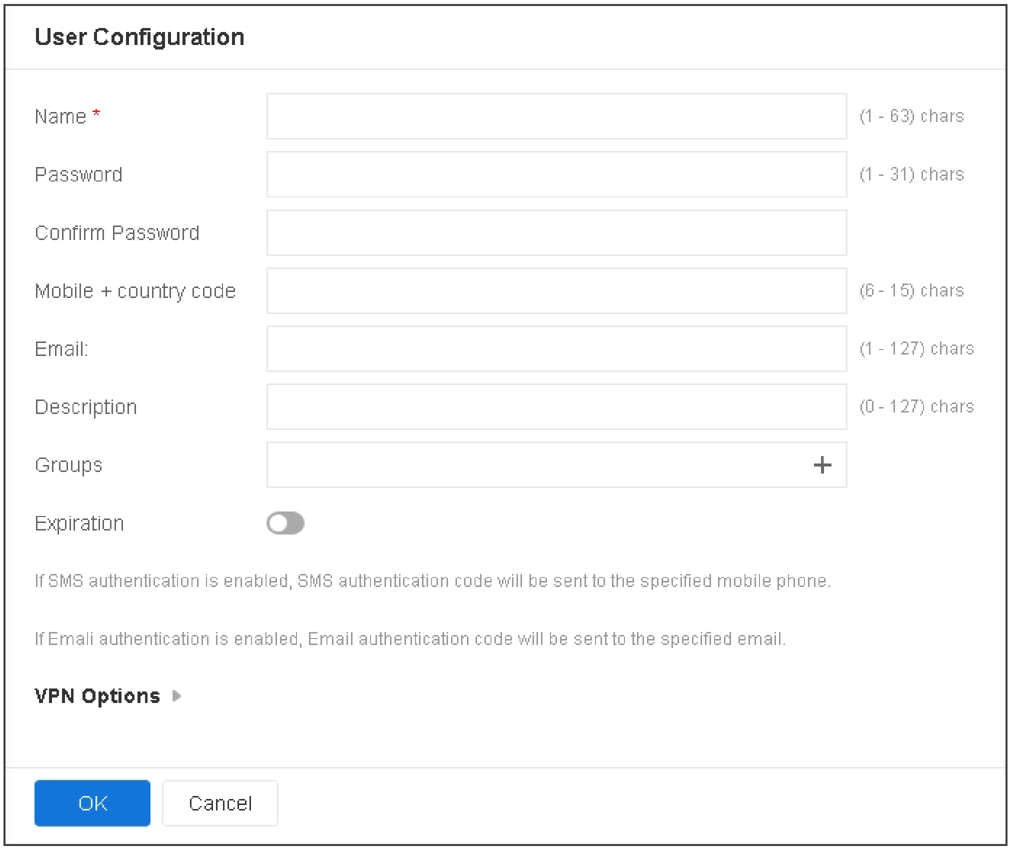
Click **Object** > **User** > **Local User**, some information and operations are provided as below:

- Click the "Local server" drop-down box in the upper left corner of the page to switch the local user's server.
- Red Expired , orange Will expire within a week and yellow Will expire within a month colors are used to mark the expired users , expired within a week, expired within a month in the list.
- Check the information of the local user in the list, including user, user group, expiration, mobile and description.

Creating a Local User

To create a local user, take the following steps:

1. Select **Object > User > Local User**.
2. Click **New > User.**



User Configuration

Name * (1 - 63) chars

Password (1 - 31) chars

Confirm Password

Mobile + country code (6 - 15) chars

Email: (1 - 127) chars

Description (0 - 127) chars

Groups +

Expiration

If SMS authentication is enabled, SMS authentication code will be sent to the specified mobile phone.

If Email authentication is enabled, Email authentication code will be sent to the specified email.

VPN Options ▸

OK Cancel

Configure the following.

Option	Description
Name	Specifies a name for the user.
Password	Specifies a password for the user.
Confirm password	Type the password again to confirm.
Mobile+country code	Specifies the user's mobile number. When users log into the SCVPN client, system will send the verification code to the mobile number.
Email	Specifies the user's Email address. The value range is 1 to 127 characters. If the Email authentication function is enabled, users will receive the verification code via this Email. For more information about Email authentication, see Configuring an SSL VPN.
Description	If needed, type the description of the user.
Group	Add the user to a selected usergroup. Select the usergroup you want and click **Add**.
Expiration	Select the **Enable** check box to enable expiration for the user, and then specify a date and time. After expiration, the user cannot be authenticated, therefore cannot be used in system. By default expiration is not enabled.

Expand VPN Options, configure network parameters for the PnPVPN client.

Option	Description
IKE ID	Specifies a IKE ID type for dial-up VPN users. If FQDN or ASN1 is selected, type the ID's content in the text box below.
DHCP Start IP	Specifies a start IP for the DHCP address pool.

Option	Description
DHCP End IP	Specifies an end IP for the DHCP address pool.
DHCP Netmask	Specifies a netmask for the DHCP address pool.
DHCP Gateway	Specifies a gateway for the DHCP address pool. The IP address of the gateway corresponds to the IP address of PnPVPN client's Intranet interface and PC's gateway address. The PC's IP address is determined by the segment and netmask configured in the above DHCP address pool. Therefore, the gateway's address and DHCP address pool should be in the same segment.
DNS1	Specifies an IP address for the DNS server. You can specify one primary DNS server (DNS1) and up to three alternative DNS servers.
DNS2	
DNS3	
DNS4	
WINS1	Specifies an IP address for the WINS server. You can specify one primary WINS server (WINS1)and one alternative WINS server.
WINS2	
Tunnel IP 1	Specifies an IP address for the master PnPVPN client's tunnel interface. Select the **Enable SNAT** check box to enable SNAT.
Tunnel IP 2	Specifies an IP address for the backup PnPVPN client's tunnel interface.

3. Click **OK**.

Creating a User Group

To create a user group, take the following steps:

1. Select **Object > User > Local User**.

2. Click **New > User Group**.

3. Type the name of the user group into the Name box.

4. Specify members for the user group. Expand User or User Group in the Available list, select a user or user group and click **Add** to add it to the Selected list on the right. To delete a selected user or user group, select it in the Selected list and then click **Remove**. One user group can contain multiple users or user groups, but system only supports up to 5 layers of nested user groups and does not support the loopback nest. Therefore, a user group should not nest the upper-layer user group it belongs to.

5. Click **OK**.

Export User List

The system exports the user-list file in .csv format, of which the content is the real-time information of the user list in the system.

Export user binding list from system to local, take the following steps:

1. Select **Object > User > Local User**.

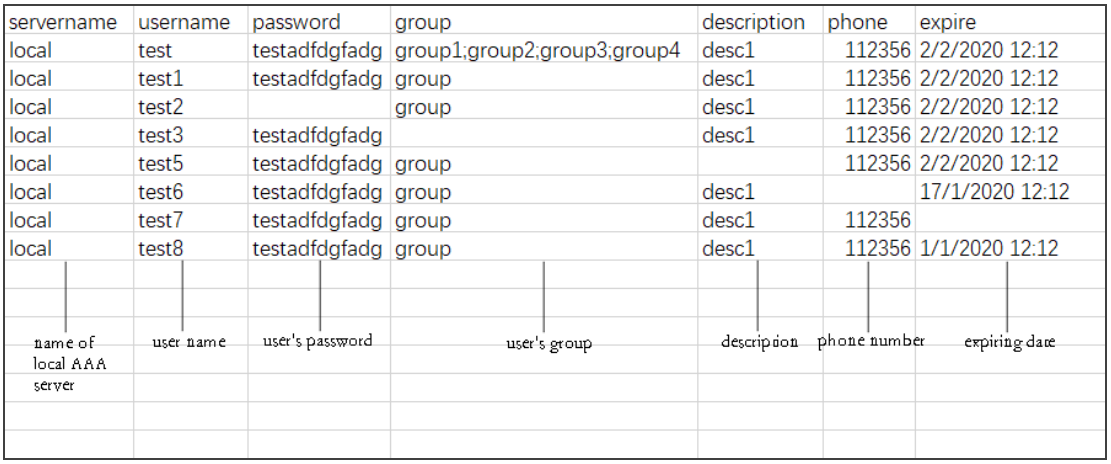
2. Click **Export User List** to open the **Export User List** page, and select the saved position in local.

3. Click **OK** to finish export.

Import User List

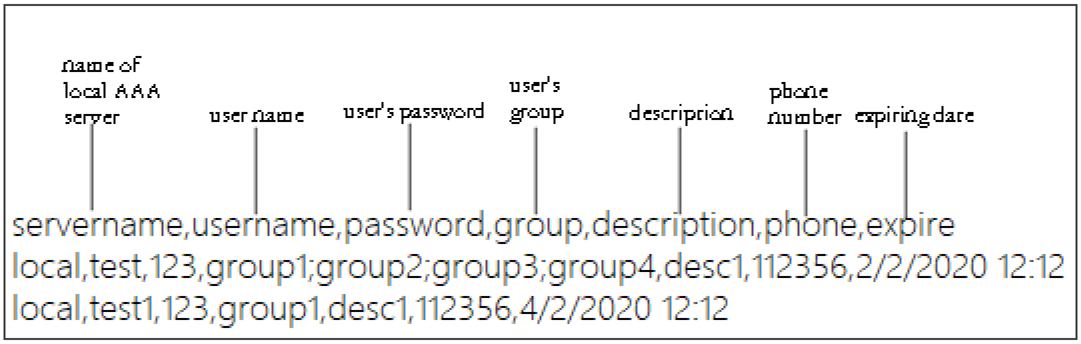
The system supports the import of user-list files in UTF-8 or GBK ecoding with .txt and .csv format.csv format. When the user-list file is imported, the system will carry out validity test and complexity check of the user password. If the results turn out to be successful, the importing is successful; if the results turn out to be unsuccessful, the importing is unsuccessful.

The user-list in .csv file is illustrated in the figure below.



servername	username	password	group	description	phone	expire
local	test	testadfdgfadg	group1;group2;group3;group4	desc1	112356	2/2/2020 12:12
local	test1	testadfdgfadg	group	desc1	112356	2/2/2020 12:12
local	test2		group	desc1	112356	2/2/2020 12:12
local	test3	testadfdgfadg		desc1	112356	2/2/2020 12:12
local	test5	testadfdgfadg	group		112356	2/2/2020 12:12
local	test6	testadfdgfadg	group	desc1		17/1/2020 12:12
local	test7	testadfdgfadg	group	desc1	112356	
local	test8	testadfdgfadg	group	desc1	112356	1/1/2020 12:12

The user-list in text file is illustrated in the figure below.



```
servername,username,password,group,description,phone,expire
local,test,123,group1;group2;group3;group4,desc1,112356,2/2/2020 12:12
local,test1,123,group1,desc1,112356,4/2/2020 12:12
```

Notes: Before importing the user-list file, please read carefully the annotations in the above figures and fill in the user information according to the format.

Import user binding list to system, take the following steps:

1. Select **Object>User> Local User**.

2. Click **Import User List** to open the **Import User List** page.

3. Click **Browse** to select the file name needed to be imported.

4. Click **OK** to finish import.

Notes:

- The user password in the import/export file is not encrypted, unless the password strings match the AES encryption format.
- Please try to keep the import file format consistent with the export file.
- When imported, if the same user name exists under the same server, the original user information will be overwritten.
- When imported, if a user is new to the system, it and its user information will be added to the system automatically.
- In the imported user-list file, the "username" field should not contain slash/-comma/double quotation marks/question mark/@; the "group" field should not contain comma/double quotation marks/question mark.
- In the imported user-list file, the date in the "expire" field should be typed in the format of DD/MM/YYYY HH:SS.
- If the user-list is imported in the format of text file, special notice should be given to the following points:
  - Every parameter in the file should be separated by half-width commas
  - If a parameter does not exist, use a half-width comma to replace it, etc. "123123,,local".
  - The sequence of the parameters in the first row is fixed and case-insensitive, etc. "Servername,userName,pAssWord".
  - The file should not contain blank lines or gibberish lines, or it is not able be imported successfully.

- If the length of a parameter is less or more than its length range, it is not able be imported successfully.

  The length range of "username": 1-63 characters

  The length range of "password": 1-31 characters

  The length range of "phone": 6-15characters

  The length range of "email": 1-127 characters

  The length range of "description": 0-127 characters

Configuring a LDAP User

This section describes how to configure a LDAP user.

Synchronizing Users

To synchronize users in a LDAP server, firstly, you need to configure a LDAP server, refer to "Configuring LDAP Server" on Page 609. To synchronize users:

1. Select **Object > User > LDAP User**.
2. Select a server from the LDAP Server drop-down list, and click **Sync Users**.

Notes: By default, after creating a LDAP server, system will synchronize the users of the LDAP server automatically, and then continue to synchronize every 30 minutes.

Configuring an Active Directory User

This section describes how to configure an active directory (AD) user.

Synchronizing Users

To synchronize users in an AD server to the device, first you need to configure an AD server ,refer to "Configuring Active Directory Server" on Page 599. To synchronize users, take the following steps:

1. Select **Object > User >AD User**.
2. Select an AD server from the Active Directory Server drop-down list, and click **Sync Users**.

Notes: By default, after creating an AD server, system will synchronize the users of the AD server automatically, and then continue to synchronize every 30 minutes.

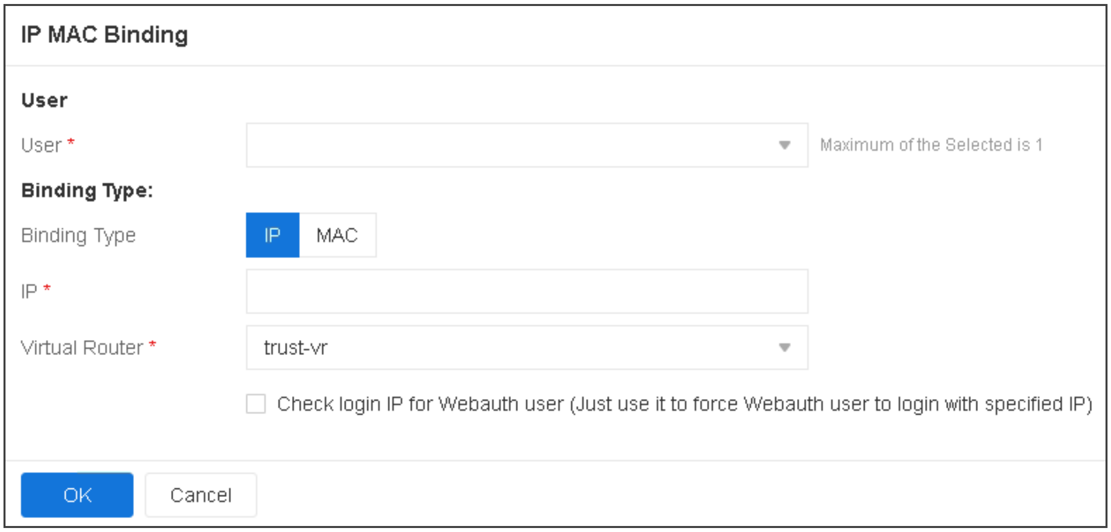
Configuring a IP-User Binding

Adding User Binding

To bind an IP or MAC address to a user, take the following steps:

1. Select **Object > User > IP-User Binding** .

2. Click **Add User Binding**.



IP MAC Binding

User

User * ▾ Maximum of the Selected is 1

Binding Type:

Binding Type [✓ IP] MAC

IP *

Virtual Router * trust-vr ▾

□ Check login IP for Webauth user (Just use it to force Webauth user to login with specified IP)

OK Cancel

Configure the following options.

User	
AAA Server	Select an AAA server from the drop-down list.
User	Select a user for the binding from the drop-down list.
Binding Type	
Binding Type	By specifying the binding type, you can bind the user to a IP address or MAC address. • IP - If IP is selected, type the IP address into the IP text box. And select a VR from the Virtual Router drop-down list. Select the **Check WebAuth IP-User Mapping Relationship** check box to apply the IP-User mapping only to the check for IP-user mapping during Web authentication if needed.

User	
	- MAC - If MAC is selected, type the MAC address into the MAC text box. And select a VR from the Virtual Router drop-down list.

3. Click **OK**.

Import Binding

Import user binding list to system, take the following steps:

1. Select **Object>User> IP-User Binding**.
2. Click **Import** , and the **Import User Binding List** dialog box pops up.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export Binding

Export user binding list from system to local, take the following steps:

1. Select **Object>User> IP-User Binding**.
2. Select the exported user category(include local, LDAP, AD and all users) in the **Export** drop-down list to pop up the export dialog box, and select the saved position in local.
3. Click **OK** to finish export.

Role

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or make exclusive use of some bandwidth. In StoneOS, users and privileges are not directly associated. Instead, they are associated by roles.

The mappings between roles and users are defined by role mapping rules. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.

System supports role combination, i.e., the AND, NOT or OR operation on roles. If a role is used by different modules, the user will be mapped to the result role generated by the specified operation.

System supports the following role-based functions:

- Role-based policy rules: Implements access control for users of different types.
- Role-based QoS: Implements QoS for users of different types.
- Role-based statistics: Collects statistics on bandwidth, sessions and new sessions for users of different types.
- Role-based session limits: Implements session limits for specific users.
- SCVPN role-based host security detection: Implements control over accesses to specific resources for users of different types.
- Role-based PBR: Implements routing for users of different types.

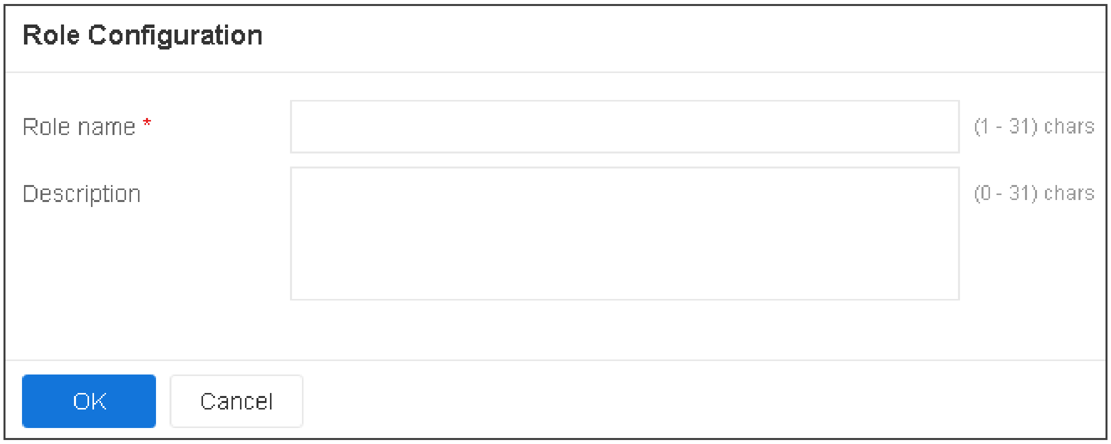
Configuring a Role

Creating a Role

To create a role, take the following steps:

1. Select **Object > Role > Role**.

2. Click **New**.



Role Configuration

Role name * (1 - 31) chars

Description (0 - 31) chars

Configure the following options.

Option	Description
Role Name	Type the role name into the Role Name box.
Description	Type the description for the role into the Description box.

3. Click **OK**.

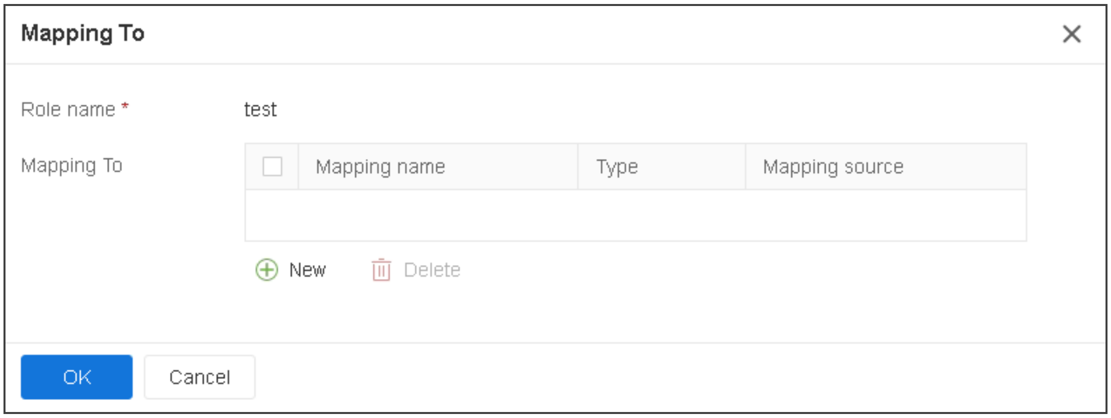
Mapping to a Role Mapping Rule

You can map the role to user, user group, CN or OU through this function or Creating a Role Mapping Rule. After Creating a Role Mapping Rule, you can click Mapping To to map the selected role again.

To map the selected role again, take the following steps:

1. Select **Object > Role > Role**.

2. Select the role need to be mapped, and click **Mapping To**.



3. In the Mapping name section, select a created mapping rule name from the first drop-down list (For detailed information of creating a role mapping role, see [Creating a Role Mapping Rule](#).), and then select a user, user group, certificate name (the CN field of USB Key certificate), organization unit (the OU field of USB Key certificate) or any from the second drop-down list. If User, User group, CN or OU is selected, also select or enter the corresponding user name, user group name, CN or OU into the box behind.

4. Click **Add** to add to the role mapping list.

5. If needed, repeat Step 3 and Step 4 to add more mappings. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.

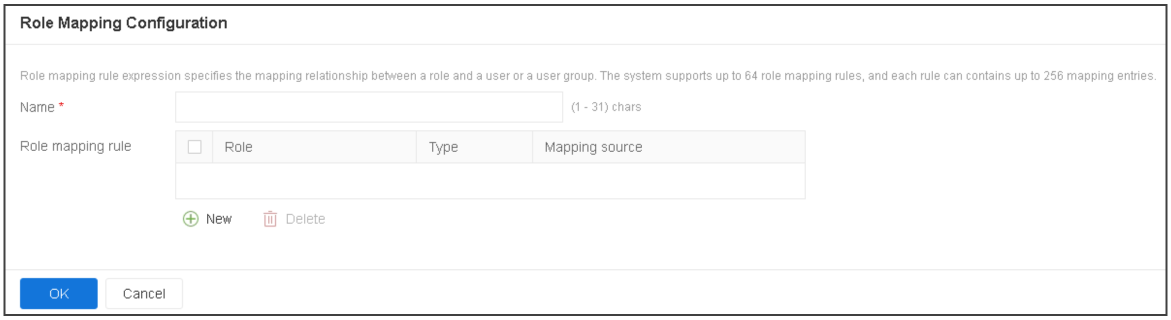
6. Click **OK**.

Creating a Role Mapping Rule

To create a role mapping rule, take the following steps:

1. Select **Object > Role > Role Mapping** .

2. Click **New**.



Role Mapping Configuration

Role mapping rule expression specifies the mapping relationship between a role and a user or a user group. The system supports up to 64 role mapping rules, and each rule can contains up to 256 mapping entries.

Name * (1 - 31) chars

Role mapping rule

□	Role	Type	Mapping source

3. Type the name for the rule mapping rule into the Name box.

4. In the Member section, select a role name from the first drop-down list, and then select a user, user group, certificate name (the CN field of USB Key certificate) or organization unit (the OU field of USB Key certificate) from the second drop-down list. If User, User group, CN or OU is selected, also select or enter the corresponding user name, user group name, CN or OU into the box behind.

5. Click **Add** to add to the role mapping list.

6. If needed, repeat Step 4 and Step 5 to add more mappings. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.

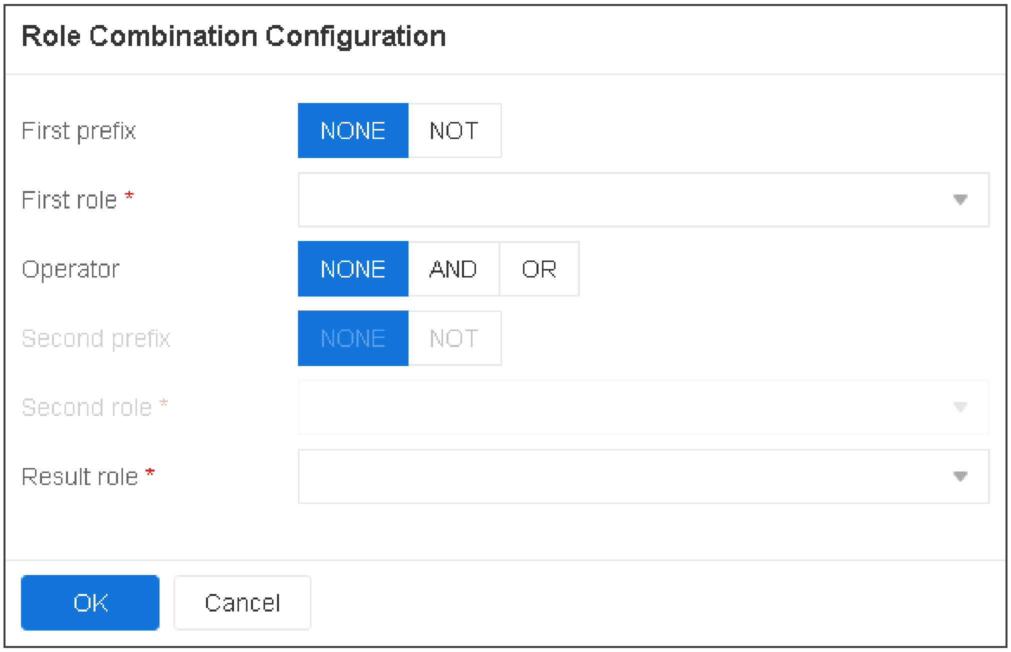
7. Click **OK**.

Creating a Role Combination

To create a role combination, take the following steps:

1. Select **Object > Role > Role Combination**.

2. Click **New**.



Role Combination Configuration

First prefix: NONE | NOT

First role *

Operator: NONE | AND | OR

Second prefix: NONE | NOT

Second role *

Result role *

Configure the following options.

Option	Description
First Prefix	Specifies a prefix for the first role in the role regular expression.
First Role	Select a role name from the First Role drop-down list to specify a name for the first role in the role regular expression.
Operator	Specifies an operator for the role regular expression.
Second Prefix	Specifies a prefix for the second role in the role regular expression.
Second Role	Select a role name from the Second Role drop-down list to specify a name for the second role in the role regular expression.

Option	Description
Result Role	Select a role name from the Result Role drop-down list to specify a name for the result role in the role regular expression.

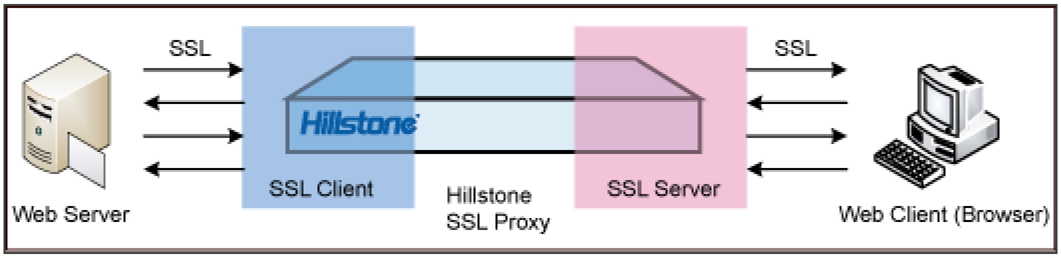
3. Click **OK**.

SSL Proxy

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS/POP3S/SMTPS/IMAPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificates to the client' s Web browser. During the process, the device acts as a SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are two work modes. For the first scenario, the SSL proxy function can work in the client-inspection proxy mode; for the second scenario, the SSL proxy function can work in the server-inspection proxy /offload mode.

When the SSL proxy function works in the client-inspection proxy mode, it can perform the SSL proxy on specified websites.

For the websites that do not need SSL proxy, it dynamically adds the IP address and port of the websites to a bypass list, and the HTTPS/POP3S/SMTPS/IMAPS traffic will be bypassed.

For the websites proxied by the SSL proxy function, the device will check the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS/POP3S/SMTPS/IMAPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS/POP3S/SMTPS/IMAPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS/POP3S/SMTPS/IMAPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list, and the HTTPS/POP3S/SMTPS/IMAPS traffic will be bypassed.

The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic that is not blocked or bypassed.

When the SSL proxy function works in the server-inspection offload mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

You can integrate SSL proxy function with the following:

- Integrate with the application identification function. Devices can decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.
- Support unilateral SSL proxy in WebAuth. SSL client can use SSL connection during authentication stage. When authentication is completed, SSL proxy will no longer take effect, and the client and server communicate directly without SSL encryption.

- Integrate with AV, IPS, Sandbox and URL. Devices can perform the AV protection, IPS protection, Sandbox protection and URL filter on the decrypted HTTPS/POP3S/SMTPS/IMAPS traffic

Working as Gateway of Web Clients

To implement the SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement the SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate, and import a device certificate to the Web browser.

2. Configure a SSL proxy profile, including the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS/POP3S/SMTPS/IMAPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on.

3. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate

- Obtain the CN value of the website certificate

- Import a device certificate to a Web browser

Specifying the PKI Trust Domain of Device Certificate

By default, the certificate of the default trust domain trust_domain_ssl_proxy_2048 will be used to generate the SSL proxy certificate with the Web server certificate together, and then system will issue the generated SSL proxy certificate to the client. You can specify another PKI trust domain in system as the trust domain of the device certificate. The specified trust domain must have a CA certificate, local certificate, and the private key of the local certificate. To specify a trust domain, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-right corner of the page, click **Trust Domain Configuration**.
3. Select a trust domain from the Trust domain drop-down list.
    - The trust domain of trust_domain_ssl_proxy uses RSA and the modulus size is 1024 bits.
    - The trust domain of trust_domain_ssl_proxy_2048 uses RSA and the modulus size is 2048 bits.
4. Click **OK** to save the settings.

Obtaining the CN Value

To get the CN value in the Subject field of the website certificate, take the following steps (take www.gmail.com as the example):

1. Open the IE Web browser, and visit https://www.gmail.com.
2. Click the **Security Report** button (🔒) next to the URL.
3. In the pop-up dialog box, click **View certificates**.
4. In the Details tab, click **Subject**. You can view the CN value in the text box.

Importing Device Certificate to Client Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser.

To export the device certificate to local PC firstly, take the following steps:

1. Export the device certificate to local PC. Select **System > PKI**.
2. In the Management tab in the PKI Management dialog box, configure the options as below:
   - Trust domain: trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048
   - Content: CA certificate
   - Action: Export
3. Click **OK** and select the path to save the certificate. The certificate will be saved to the specified location.

Then, import the device certificate to the client browser. Take Internet Explorer as an example:

1. Open IE.
2. From the toolbar, select **Tools > Internet** Options.
3. In the **Content** tab, click **Certificates**.
4. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab.
5. Click **Import**. Import the certificate following the Certificate Import Wizard.

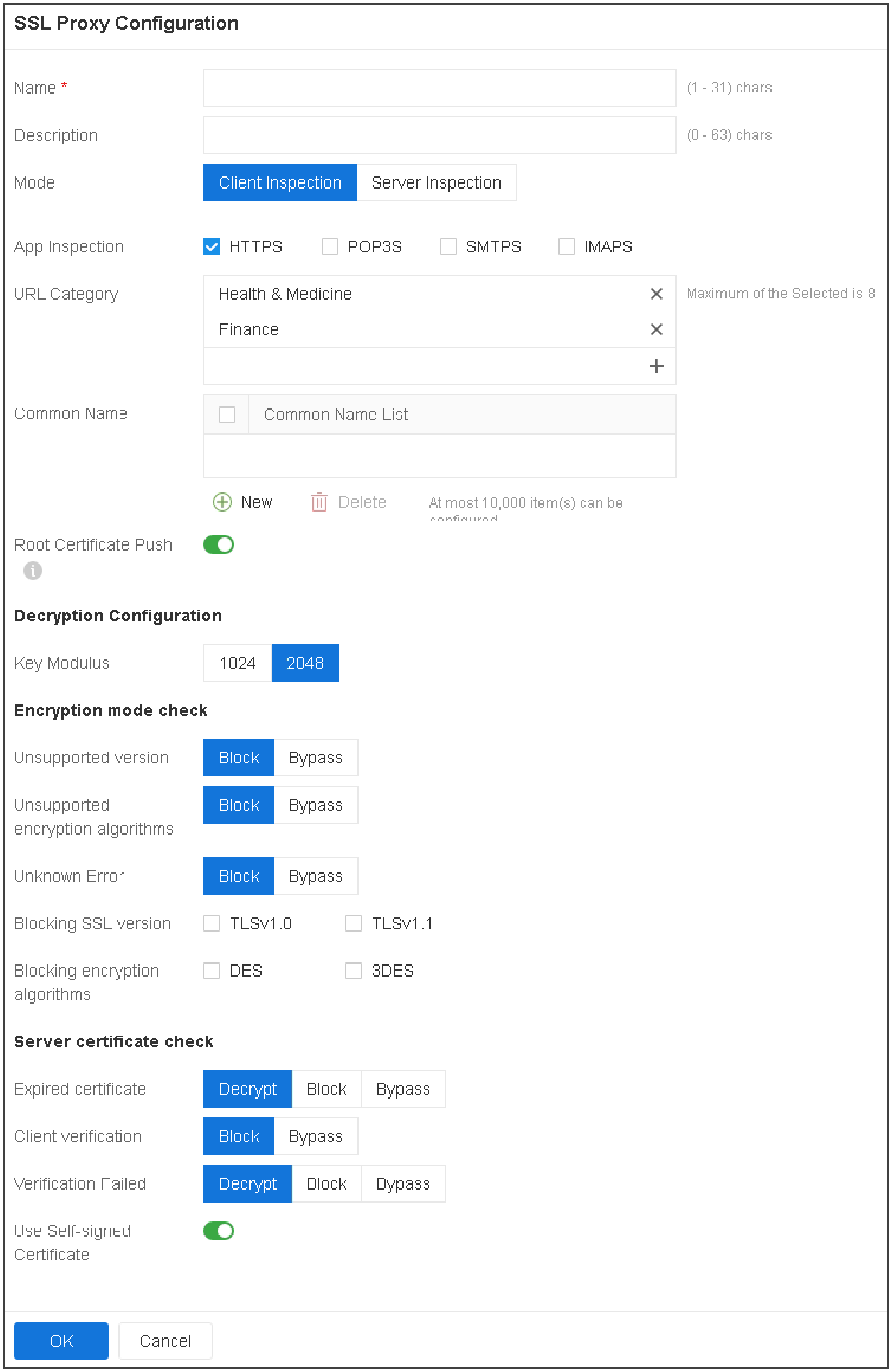
Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, set the website list (use the CN value of the Subject field of the website certificate), configure the actions to the HTTPS/POP3S/SMTPS/IMAPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on. System supports up to 32 SSL proxy profiles and each profile supports up to 10,000 statistic website entries.

To configure a SSL proxy profile, take the following steps:

1. Click **Object> SSL Proxy**.

2. At the top-left corner, click **New** to create a new SSL proxy profile.



SSL Proxy Configuration

Name * (1 - 31) chars

Description (0 - 63) chars

Mode [✓ Client Inspection] Server Inspection

App Inspection ☑ HTTPS □ POP3S □ SMTPS □ IMAPS

URL Category Maximum of the Selected is 8
- Health & Medicine ✕
- Finance ✕
- +

Common Name
□ Common Name List

⊕ New 🗑 Delete At most 10,000 item(s) can be configured

Root Certificate Push ⓘ [✓]

Decryption Configuration

Key Modulus 1024 [✓ 2048]

Encryption mode check

Unsupported version [✓ Block] Bypass

Unsupported encryption algorithms [✓ Block] Bypass

Unknown Error [✓ Block] Bypass

Blocking SSL version □ TLSv1.0 □ TLSv1.1

Blocking encryption algorithms □ DES □ 3DES

Server certificate check

Expired certificate [✓ Decrypt] Block Bypass

Client verification [✓ Block] Bypass

Verification Failed [✓ Decrypt] Block Bypass

Use Self-signed Certificate [✓]

In the Basic tab, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	When the device works as the gateway of Web clients, the SSL proxy function can work in the client-inspection proxy mode. When the device works as the gateway of Web servers, the SSL proxy function can work in the server-inspection offload mode. • In the client-inspection proxy mode, the device does not perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be proxied by SSL proxy function. • In the server-inspection proxy /offload mode, device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.
App Inspection	Select an application to be proxied by the SSL proxy function. Currently, system supports to perform SSL proxy on the HTTPS, POP3S, SMTPS and IMAPS traffic passing through the default port. By default, only the HTTPS

Option	Description
	traffic will be proxied, but you can select multiple applications as needed. To make sure the HTTPS/POP3S/SMTPS/IMAPS traffic passing through user-defined ports will be proxied by the function, you can configure the user-defined ports in **Object > APP Book >** Static Signature Rule. **Note:** Only the predefined applications created in **Object > APP Book >** Application can be proxied by the SSL proxy function.
Common Name	Set the website list based on the work mode. When the SSL proxy is in the Require mode, set the websites that will be proxied by the SSL proxy function. When the SSL proxy is in the Exempt mode, set the websites that will not be proxied by the SSL proxy function and the device will perform the SSL proxy on other websites.To set the website list, click **New** and specify the CN value of the subject field of the website certificate.
Root Certificate Push	Click the **Enable** button to enable the Root Certificate Push. When the HTTPS traffic is decrypted by the SSL proxy function, the Install Root Certificate page will display in your Web browser. In the Install Root Certificate page, you can select **Download** or **Downloaded, Ignored** as needed. • Download: Click the button to download the root

Option	Description
	certificate to your local PC. For details on importing a root certificate to your Web browser, refer to Importing Device Certificate to Client Browser. • Downloaded, Ignored: If you click the button, system will no longer push the Install Root Certificate page, and will redirect you to the page you want to visit. **Notes:** • When the Install Root Certificate page displays, if you close the browser, system will still push the page for your next HTTPS request. • You must install the root certificate. If you do not install the root certificate, system will prompt the access is not secure, and the access page may not be loaded completely. Click the **Enable** button to disable the Root Certificate Push. With the function disabled, when the client initiates an HTTPS request: • If the root certificate has been installed in your Web browser, you will be redirected to the page you want to visit. • If the root certificate has not been installed in your Web browser, you will be prompted that the page

Option	Description
	you're visiting is not secure.

In the Decryption Configuration tab, configure the settings. After system completes the SSL negotiation, the HTTPS/POP3S/SMTPS/IMAPS traffic that is not blocked or bypassed will be decrypted. If the parameters match multiple items in the checklist and you have configured different actions for different items, the Block action will take effect, and the corresponding traffic will be blocked.

Option	Description
Key Modulus	Specify the key pair modulus size of the private/public keys that are associated with the SSL proxy certificate. You can select 1024 bits or 2048 bits.
Encryption mode check	
Unsupported version	Check the SSL protocol version used by the server. • When the SSL protocol used by the SSL server is not supported in system, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When the SSL protocol used by the SSL server is supported, it will continue to check other items.
Unsupported encryption algorithms	Check the encryption algorithm used by the server. • When the encryption algorithm used by the SSL server is not supported in system, you can select **Block** to block its

Option	Description
	HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When the encryption algorithm used by the SSL server is supported, it will continue to check other items.
Unknown Error	Check the unknown error. • When SSL negotiation fails and the cause of failure can’ t be confirmed, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When system do not need check unknown failure, it will continue to check other items.
Blocking SSL version	When the SSL server uses the specified version of SSL protocol, system can block its HTTPS/POP3S/SMTPS/IMAPS traffic.
Blocking encryption algorithm	When the SSL server uses the specified encryption algorithm, system can block its HTTPS/POP3S/SMTPS/IMAPS traffic.
Server certificate check	
Expired certificate	Check the certificate used by the server. When the certificate is overdue, you can select **Block** to block its

Option	Description
	HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Decrypt** to decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic.
Client verification	Check whether the SSL server verifies the client certificate. • When the SSL server verifies the client certificate, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. • When the SSL server does not verify the client certificate, it will continue to check other items.
Verification Failed	Verify the server certificate. You can configure an action for the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified. • Decrypt: Decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified, and select whether to use the self-signed certificate. • Use self-signed certificate: Click the **Enable** button to use the self-signed certificate to complete the SSL negotiation with the Web

Option	Description
	browser. Then, the browser will prompt a warning message. • Do not use self-signed certificate: Click the **Enable** button to disable the self-signed certificate. Then, system will use the trusted certificate "SG6000" to complete the SSL negotiation with the Web browser. If the certificate "SG6000" has been installed, the browser will not prompt a warning message. • Block: Block the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified. • Bypass: Bypass the HTTPS/POP3S/SMTPS/IMAPS traffic when the certificate is failed to be verified.

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

Working as Gateway of Web Servers

To implement SSL proxy, you need to bind a SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

2. Bind a SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS traffic that matches the policy rule.

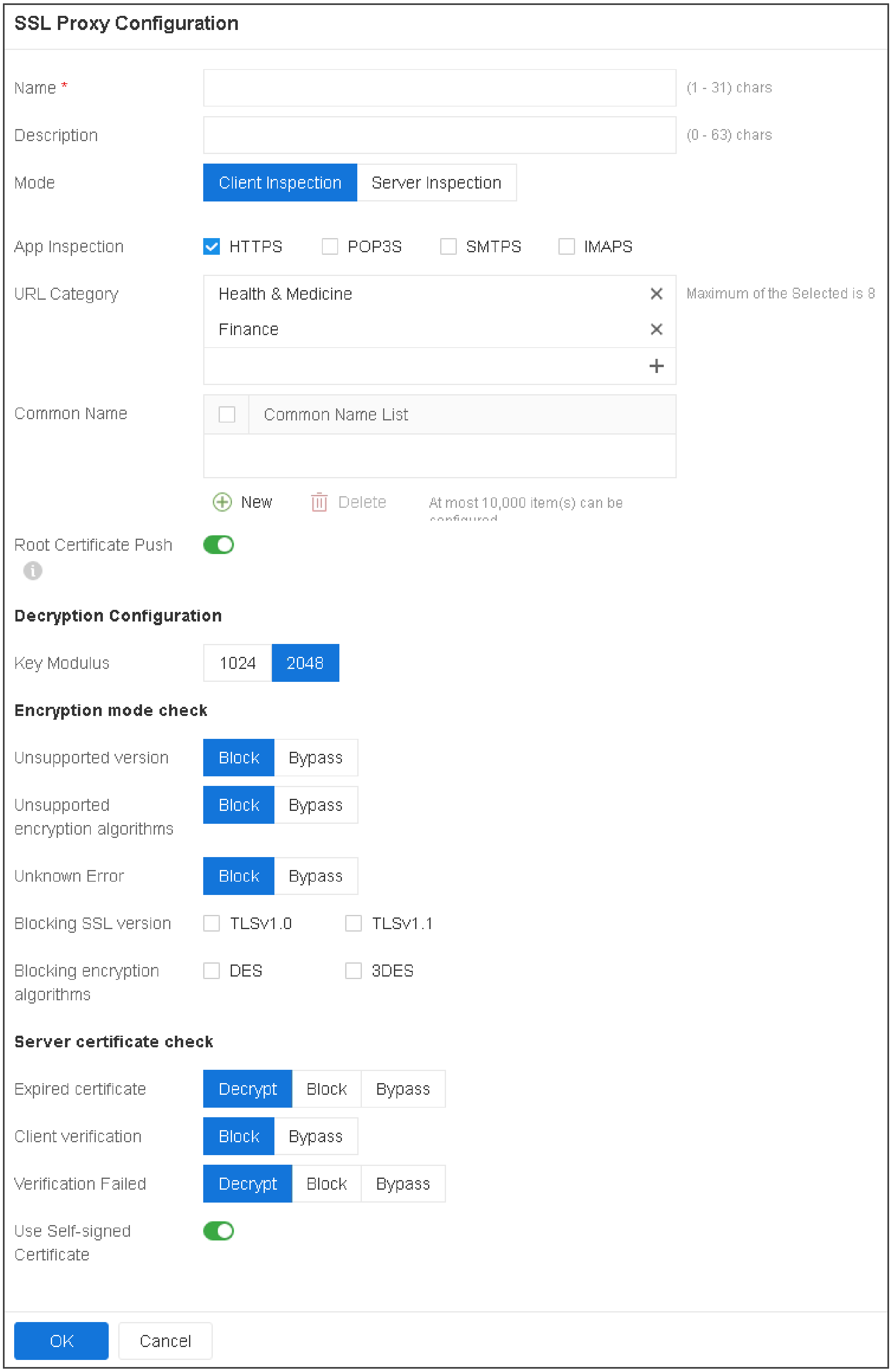
Configuring a SSL Proxy Profile

Configuring a SSL proxy profile includes the following items: choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.

To configure a SSL proxy profile, take the following steps:

1. Click **Policy > SSL Proxy**.

2. At the top-left corner, click **New** to create a new SSL proxy profile.



SSL Proxy Configuration

Name * [ ] (1 - 31) chars

Description [ ] (0 - 63) chars

Mode: [Client Inspection] Server Inspection

App Inspection: ☑ HTTPS ☐ POP3S ☐ SMTPS ☐ IMAPS

URL Category: Health & Medicine ✕ / Finance ✕ / + — Maximum of the Selected is 8

Common Name: ☐ Common Name List

Root Certificate Push: ● on

Decryption Configuration

Key Modulus: 1024 [2048]

Encryption mode check

Unsupported version: [Block] Bypass

Unsupported encryption algorithms: [Block] Bypass

Unknown Error: [Block] Bypass

Blocking SSL version: ☐ TLSv1.0 ☐ TLSv1.1

Blocking encryption algorithms: ☐ DES ☐ 3DES

Server certificate check

Expired certificate: [Decrypt] Block Bypass

Client verification: [Block] Bypass

Verification Failed: [Decrypt] Block Bypass

Use Self-signed Certificate: ● on

In this page, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description.
Mode	When the device works as the gatetway of Web servers, the SSL proxy function can work in the Offload mode.
Service Port	Specify the HTTP port number of the Web server.
Server Trust Domain	Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device. For more information about importing the certificate and the key pair, see "PKI" on Page 362. After you complete the importing, select the trust domain used by this SSL Profile.
Warning	Select **Enable** to enable the warning page. When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, system notifies the users that their access to HTTPS websites are being monitored and asks the users to protect their privacy.

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

Binding a SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, see "Security Policy" on Page 768.

Track Object

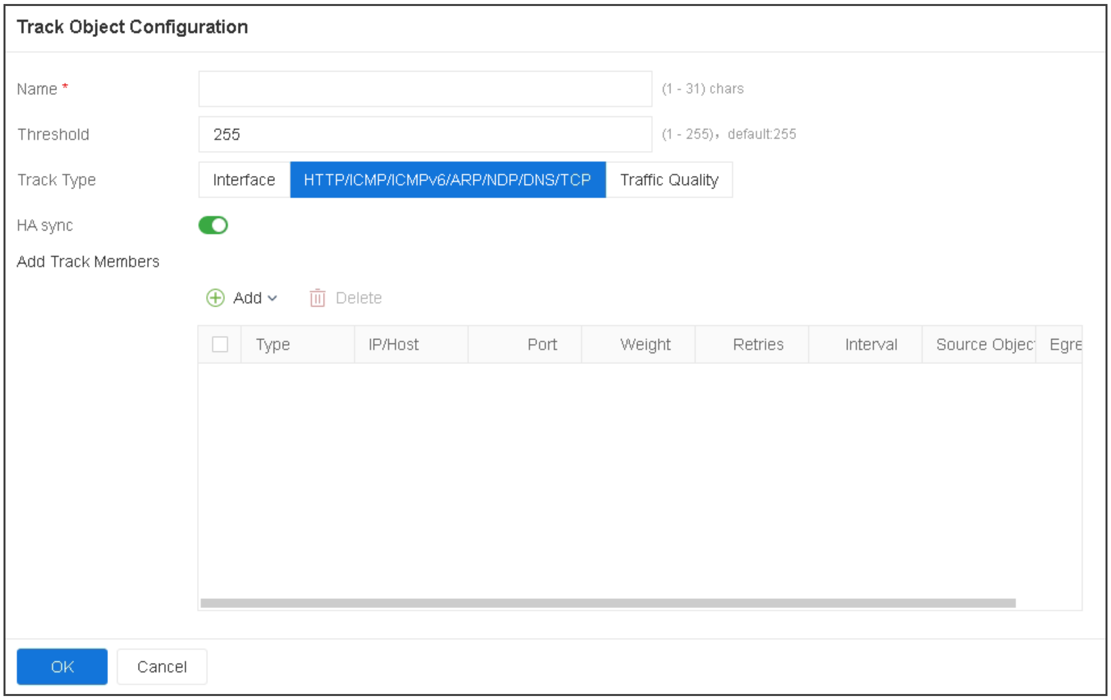
The devices provide the track object to track if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

Creating a Track Object

To create a track object, take the following steps:

1. Select **Object > Track Object**.

2. Click **New**.



Track Object Configuration

Name * (1 - 31) chars

Threshold 255 (1 - 255)，default:255

Track Type: Interface | [✓ HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP] | Traffic Quality

HA sync: ●

Add Track Members

□	Type	IP/Host	Port	Weight	Retries	Interval	Source Objec	Egre

Configure the following options.

Option	Description
Name	Specifies a name for the new track object.
Threshold	Type the threshold for the track object into the text box. If

Option	Description
	the sum of weights for failed entries in the track object exceeds the threshold, system will conclude that the whole track object fails.
Track Type	Select a track object type. One track object can only be configured with one type. Select **Interface** radio button: • 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. Select **HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP** radio button: • 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.

Option	Description
	• 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. 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

Option	Description
	HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP packets are sent. - Source Interface- Specifies a source interface for HTTP/ICMP/ICMPv6/ARP/DNS/TCP packets.
	Select **Traffic Quality** radio button: - Click **Add** in Add Track Members section and then configure the following options in the Add Traffic Quality Member dialog box: - 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

Option	Description
	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 successful. **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.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.

3. Click **OK.** The created track object will be displayed in the track object list.

URL Filtering

URL filtering controls the access to some certain websites and records log messages for the access actions. URL filtering helps you control the network behaviors in the following aspects:

- Access control to certain category of websites, such as gambling and pornographic websites.
- Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours.
- Access control to the website whose URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.

If IPv6 is enabled, you can configure URL and keyword for both IPv4 and IPv6 address. How to enable IPv6, see StoneOS_CLI_User_Guide_IPv6.

Configuring URL Filtering

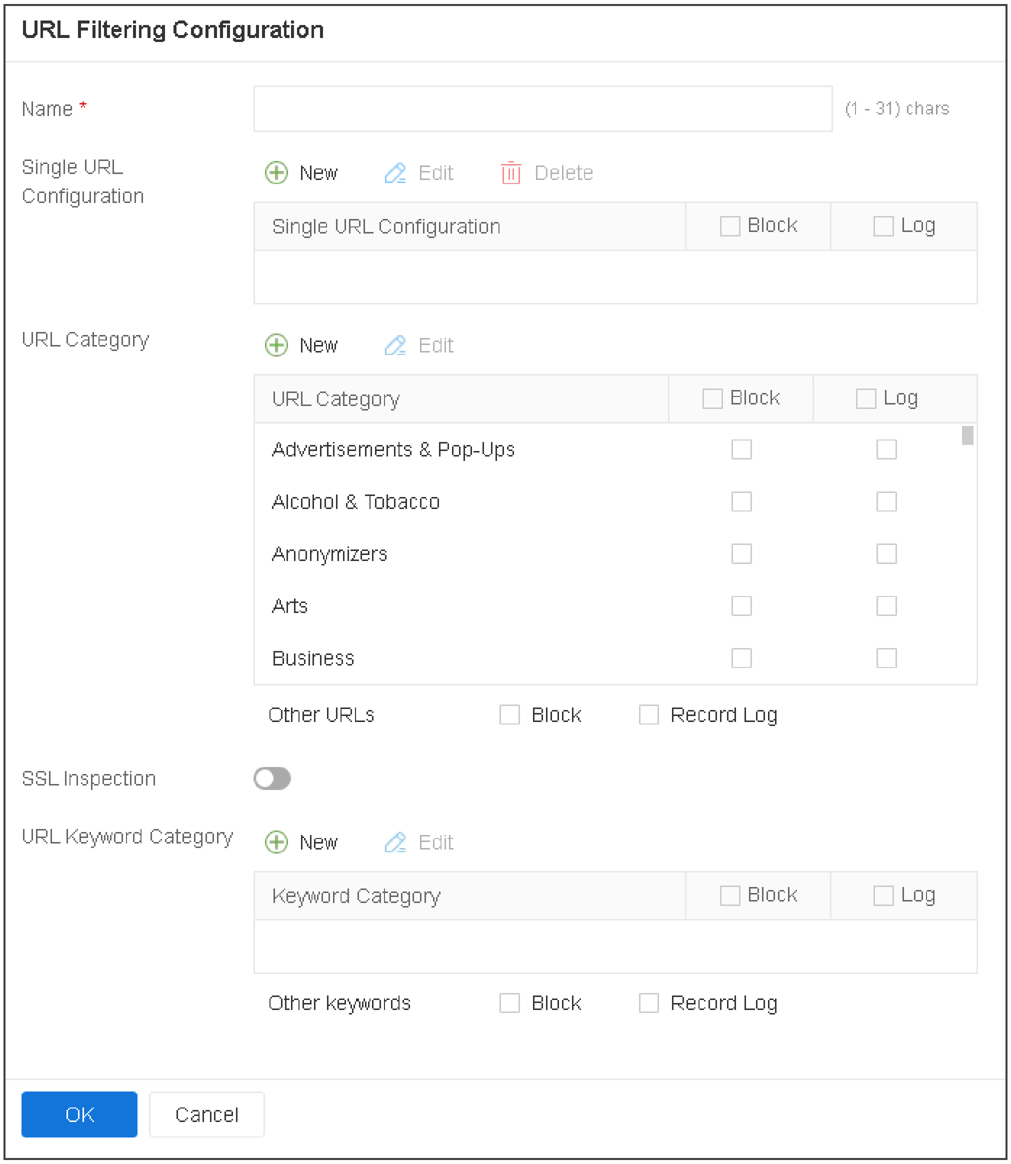
Configuring URL filtering contains two parts:

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

Part 1: Creating a URL filtering rule

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

2. Click **New**.



URL Filtering Configuration

Name * (1 - 31) chars

Single URL Configuration ⊕ New Edit Delete

Single URL Configuration	□ Block	□ Log

URL Category ⊕ New Edit

URL Category	□ Block	□ Log
Advertisements & Pop-Ups	□	□
Alcohol & Tobacco	□	□
Anonymizers	□	□
Arts	□	□
Business	□	□

Other URLs □ Block □ Record Log

SSL Inspection ○

URL Keyword Category ⊕ New Edit

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.

Option	Description
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 **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 only can be used in combination with the SSL proxy function because the search engine uses the HTTPS protocol. Therefore, when the “SafeSearch” is enabled, enable the SSL proxy function for the policy rule which is bound with

Option	Description
	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 port.
Control Action	Specifies the safe search action. o Block: Selects the check box to specify the action as block, When the " SafeSearch" setting of search engine is not set, users will be prevented from accessing the search page and a warning page will pop up which provides users with the link for "SafeSearch" setting. o Enforce: Selects the check box to specify the action as execute. When the "SafeSearch" setting of search engine is not set, system will force to set it at the "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 "User-defined URL DB" on Page 673.
Edit	Selects a URL category from the list, and click **Edit** to

Option	Description
	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 "Keyword Category" on Page 677. • 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**.
URL category	Shows the name of pre-defined and user-defined URL categories in the VSYS.

Option	Description
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**.
SSL inspection	Select the **Enable** button to enable SSL negotiation packets inspection. For HTTPS traffic, system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this feature is configured. Then, 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.

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. For more information about keyword category, see "Keyword Category" on Page 677.
Edit	Select a URL keyword category from the list, and click

Option	Description
	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.

Part 2: Binding a URL filtering rule to a security zone or security policy rule

The URL filtering configurations are based on security zones or policies.

- If a security zone is configured with the URL filtering function, system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the URL filtering function, system will perform detection on the traffic that is destined to the policy rule you specified, and then respond.

- The threat protection configurations in a policy rule are superior to that in a zone rule if they are specified at the same time, and the URL filtering configurations in a destination zone are superior to that in a source zone if they are specified at the same time.
- To perform the URL filtering function on the HTTPS traffic, see the policy-based URL filtering.

To create the zone-based URL filtering, take the following steps:

1. Create a zone. For more information about how to create this, refer to "Security Zone" on Page 74.
2. In the Zone Configuration dialog box, select the Threat Protection tab.
3. Enable the threat protection that you need, and select the URL filtering rules from the profile drop-down list below; you can click **Add Profile** from the profile drop-down list below to create a URL filtering rule. For more information, see "Part 1: Creating a URL filtering rule" on Page 659.
4. Click **OK** to save the settings.

To create the policy-based URL filtering, take the following steps:

1. Configure a security policy rule. For more information, see "Configuring a Security Policy Rule" on Page 769.
2. In the Protection tab, select the **Enable** check box of URL Filtering.
3. From the **Profile** drop-down list, select a URL filtering rule. You can also click **Add Profile** to create a new URL filtering rule.
4. To perform the URL filtering function on the HTTPS traffic, you need to enable the SSL proxy function for this security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the URL filtering function on the decrypted

traffic.

According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled URL filtering disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the URL filtering function on the decrypted traffic.
SSL proxy enabled URL filtering enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic.
SSL proxy disabled URL filtering enabled	System performs the URL filtering function on the HTTP traffic according to the URL filtering profile. The HTTPS traffic will not be decrypted and system will transfer it.

If the SSL proxy and URL filtering functions are enabled on a security policy rule but the control type of the selected URL filtering rule is the Web surfing record, the system will not record the GET and POST methods and the posted contents via HTTPS.

If the zone which the security policy rule binds with is also configured with a URL filtering, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled URL fil-	URL filtering enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic according to the

Policy Rule Configurations	Zone Configurations	Actions
tering disabled		URL filter rule of the zone.
SSL proxy enabled URL filtering enabled	URL filtering enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the URL filtering function on the decrypted traffic according to the URL filtering rule of the policy rule.
SSL proxy disabled URL filtering enabled	URL filtering enabled	System performs the URL filtering function on the HTTP traffic according to the URL filtering rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

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

If necessary, you can go on to configure the functions of "Predefined URL DB" on Page 671, "URL Lookup" on Page 675, and "Warning Page" on Page 679.

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database, including the URL category and the category type.
Warning Page	• Block warning: When your network access is blocked, a warning page will prompt in the Web browser.

Object	Description
	- Audit warning: When your network access is audited, a warning page will prompt in the Web browser.

Notes:

- Only after canceling the binding can you delete the URL filtering rule.
- To get the latest URL categories, you are recommended to update the URL database first. For more information about URL database, see "Predefined URL DB" on Page 671.
- You can export the log messages to specified destinations. For more information about log messages, see "Log Configuration" on Page 1115.

Cloning a URL filtering Rule

System supports the rapid clone of a URL filtering rule. You can clone and generate a new URL filtering rule by modifying some parameters of the one current URL filtering rule.

To clone a URL filtering rule, take the following steps:

1. Select **Object > URL Filtering**.
2. Select a URL filtering rule in the list.
3. Click the **Clone** button above the list, and the **Name** configuration box will appear below the button. Then enter the name of the new URL filtering rule.
4. The cloned URL filtering rule will be generated in the list.

Viewing URL Hit Statistics

The URL access statistics includes the following parts:

- Summary: The statistical information of the top 10 user/IPs, the top 10 URLs, and the top 10 URL categories during the specified period of time are displayed.
- User/IP: The user/IP and detailed hit count are displayed.
- URL: The URL and detailed hit count are displayed.
- URL Category: The URL category and detailed hit count and traffic are displayed.

To view the URL hit statistics, see "URL Hit" on Page 1040 in Monitor.

- To view the URL hit statistics, enable **URL Hit** in "Monitor Configuration" on Page 1063.
- To view the traffic of the URL category, enable **URL Hit** and **URL Category Bandwidth** in "Monitor Configuration" on Page 1063.

Viewing Web Surfing Records

To view the Web surfing records, view "URL Log" on Page 1109. Before you view the Web surfing records, see "Log Configuration" on Page 1115 to enable URL Log function.

Configuring URL Filtering Objects

When using URL filtering function, you need to configure the following objects:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
User-defined URL DB	The user-defined URL database is defined by you and you can use it to specify the URL category.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Cat-	Use the keyword category function to customize the keyword

Object	Description
egory	categories.
Warning Page	Enable or disable the warning page. • Block warning: When your network access is blocked, a warning page will prompt in the Web browser. • Audit warning: When your network access is audited, a warning page will prompt in the Web browser.

Predefined URL DB

System contains a predefined URL database.

Notes: The predefined URL database is controlled by a license . Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of a URL filtering. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

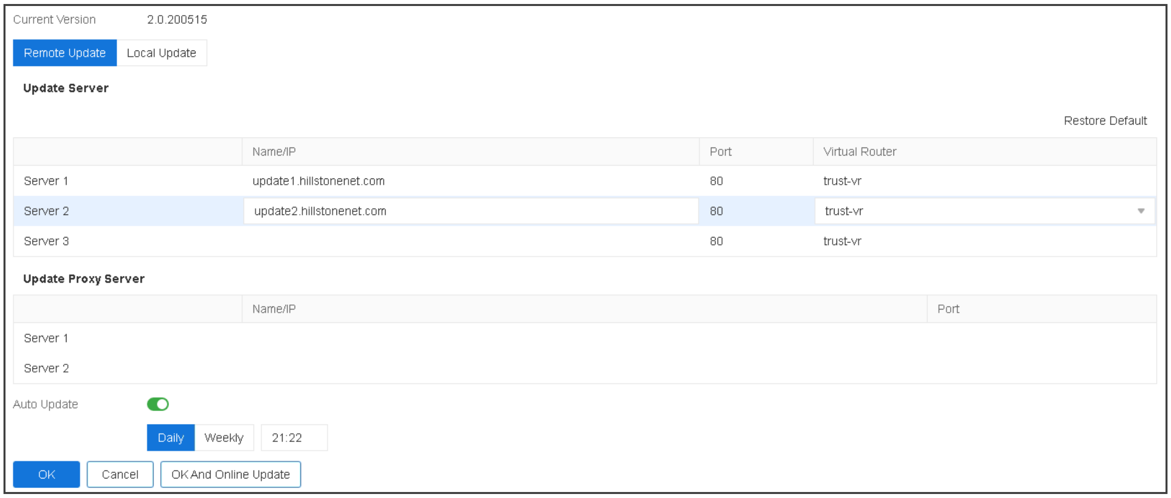
Configuring Predefined URL Database Update Parameters

By default, system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provided: https://update1.hillstonenet.com and https://update2.hillstonenet.com. Besides, you can update the predefined URL database from your local disk.

To change the update parameters, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.

2. In the URL category database update section, you can view the current version of the database, perform the remote update, configure the remote update, and perform the local update.



Current Version 2.0.200515

Update Server

	Name/IP	Port	Virtual Router
Server 1	update1.hillstonenet.com	80	trust-vr
Server 2	update2.hillstonenet.com	80	trust-vr
Server 3		80	trust-vr

Update Proxy Server

	Name/IP	Port
Server 1		
Server 2		

Auto Update ●

Daily Weekly 21:22

3. Click **Enable** button of **Auto Update** to enable the automatic update function and then continue to specify the frequency and time. Click **OK** to save your settings.

4. Double click an entry of **Update Server** to configure the update server URL. Specify the URL or IP address of the update server, and select the virtual router that can connect to the server. To restore the URL settings to the default ones, click **Restore Default**.

5. Double click an entry of **Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup 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 databases can update normally.

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

Upgrading Predefined URL Database Online

To upgrade the URL database online, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local, take the following steps:

1. **System > Upgrade Management > Signature Database Update**
2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.
3. Click **Upload** to update the predefined URL database.

> **Notes:** You can not upgrade the predefined URL database from local in non-root VSYS.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of URL filtering. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

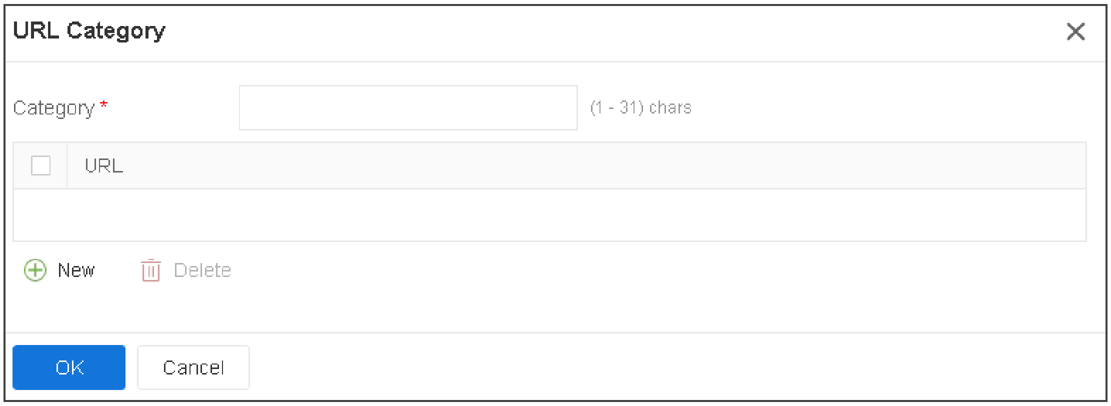
System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL categories.

> **Notes:** You can not import your own URL lists into one of the predefined URL category in non-root VSYS.

Configuring User-defined URL DB

To configure a user-defined URL category, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.
3. Click **New**. The URL Category dialog box will appear.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.
5. Type a URL into the **URL http(s)://** box.
6. Click **Add** to add the URL and its category to the table.
7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.
8. Click **OK** to save the settings.

Importing User-defined URL

System supports to batch imported user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL, take the following steps:

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

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.

3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.

4. In the Batch Import URL dialog box, click **Browse** button to select your local URL file. The file should be less than 1 M, and have at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.

5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear a user-defined URL, take the following steps:

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

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.

3. Select one of the predefined URL categories(custom1/2/3), and then click **Clear**. The URL in the custom 1/2/3 will be cleared from the system.

URL Lookup

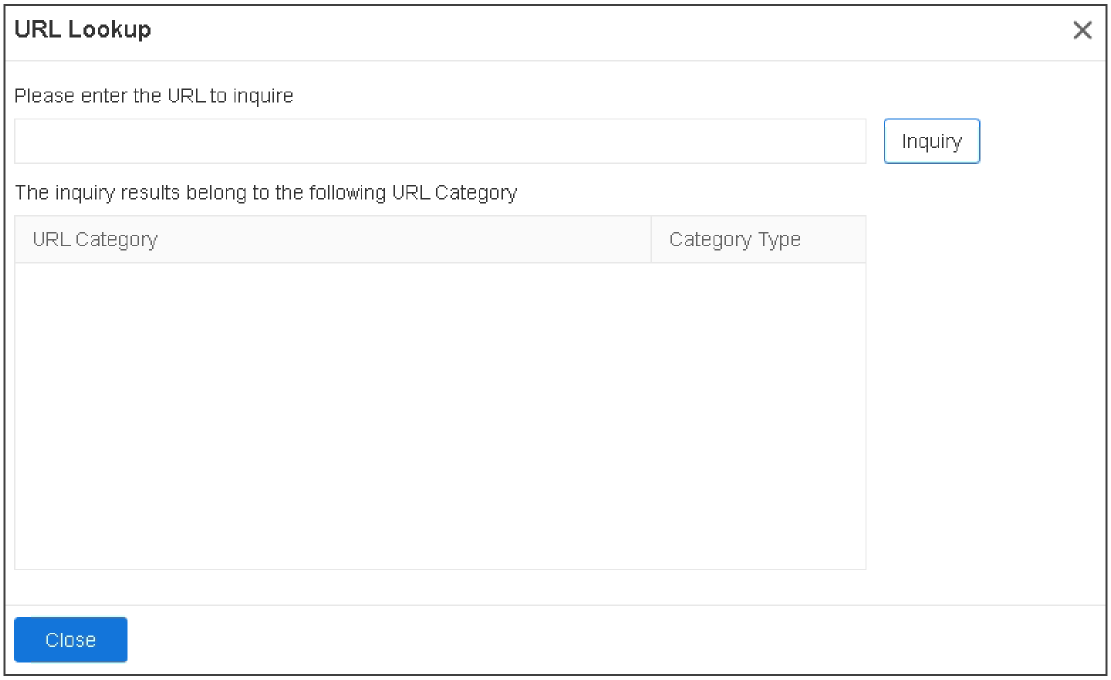
You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information, take the following steps:

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

2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog box will appear.


URL Lookup
×
Please enter the URL to inquire
Inquiry
The inquiry results belong to the following URL Category
URL Category
Category Type
Close

3. Type the URL into the **Please enter the URL to inquire** box.

4. Click **Inquire**, and the results will be displayed at the bottom of the dialog box.

Configuring URL Lookup Servers

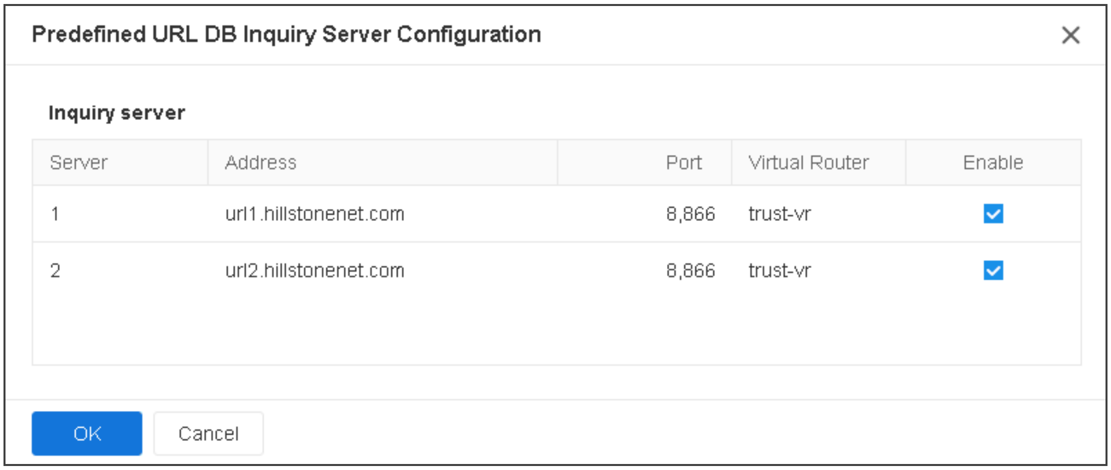
URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server, take the following steps:

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

2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog box will appear.

3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog box will appear.



Predefined URL DB Inquiry Server Configuration

Inquiry server

Server	Address	Port	Virtual Router	Enable
1	url1.hillstonenet.com	8,866	trust-vr	☑
2	url2.hillstonenet.com	8,866	trust-vr	☑

4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.

5. Select the check box in the **Enable** column to enable this URL lookup server.

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

Keyword Category

You can customize the keyword category and use it in the URL filtering function.

After configuring a URL filtering rule, system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times * trust value* of each keyword that belongs to the category. Then system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a URL filtering rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

If system detects 1 occurrence of K1 and K2 each on a URL, then C1 trust value is 20*1＋40*1-1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the URL access is permitted.

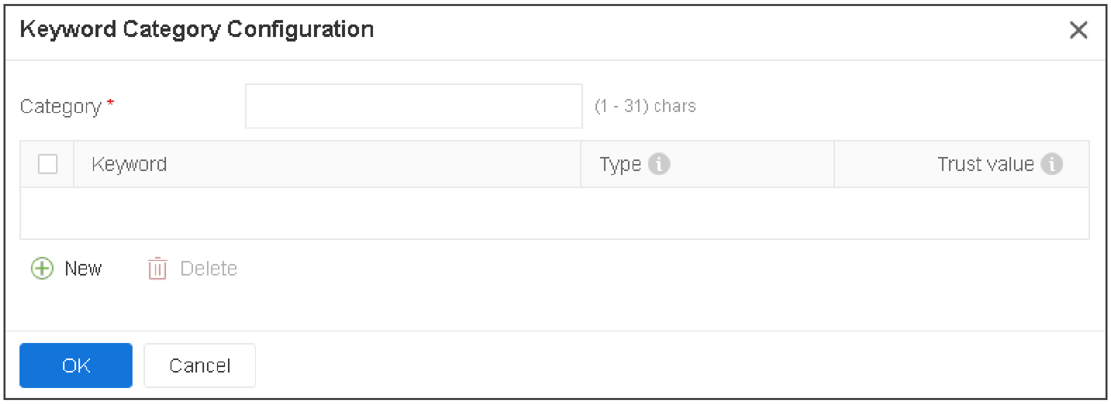
If system detects 3 occurrences of K1 and 1 occurrence of K2 on a URL, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > Keyword Category**. The Keyword Category dialog box will appear.

3. Click **New**. The **Keyword Category Configuration** dialog box will appear.



4. Type the category name.

5. Click **New**. In the slide area, specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).

6. Click **Add** to add the keyword to the list below.

7. Repeat the above steps to add more keywords.

8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.

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

Warning Page

The warning page shows the user block information and user audit information. You can enable or disable the warning page as needed.

The warning page include predefined warning page and user-defined warning page.

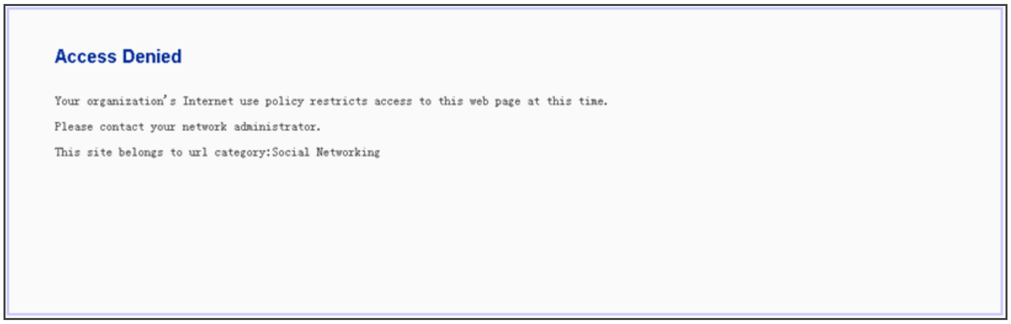
- Predefined warning page: Displays the predefined warning information content, including prompt information and warning reasons.

- User-defined warning page: You can customize the warning page by custom warning information and pictures. For details, please refer to "Warning Page Management" on Page 1198..

Enabling/ Disabling the Block Warning

The block warning is disabled by default. If the internet behavior is blocked by the URL filtering function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. According to the different network behaviors, the predefined warning page includes the following two situations:

- Visiting a certain type of URL.



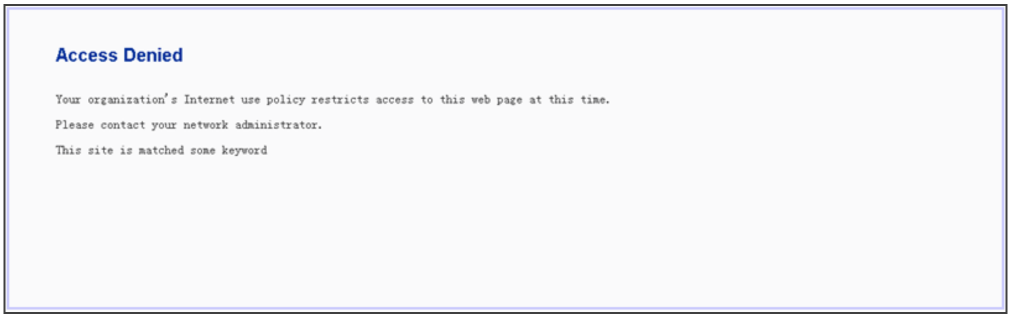
Access Denied

Your organization's Internet use policy restricts access to this web page at this time.

Please contact your network administrator.

This site belongs to url category:Social Networking

- Visiting the URL that contains a certain type of keyword category.



Access Denied

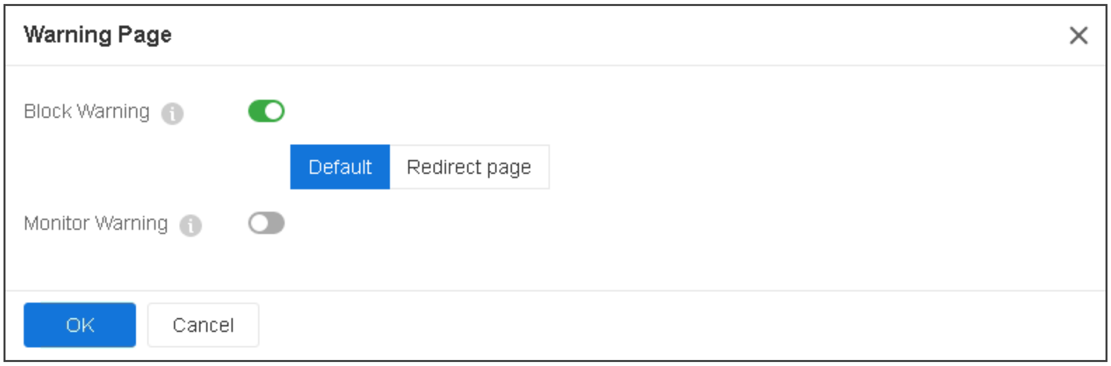
Your organization's Internet use policy restricts access to this web page at this time.

Please contact your network administrator.

This site is matched some keyword

To enable or disable the block warning , take the following steps:

1. Click **Object > URL Filtering > Profile**.
2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.



3. In the Block Warning section, select **Enable**. To disable this function, unselect the **Enable** check box.

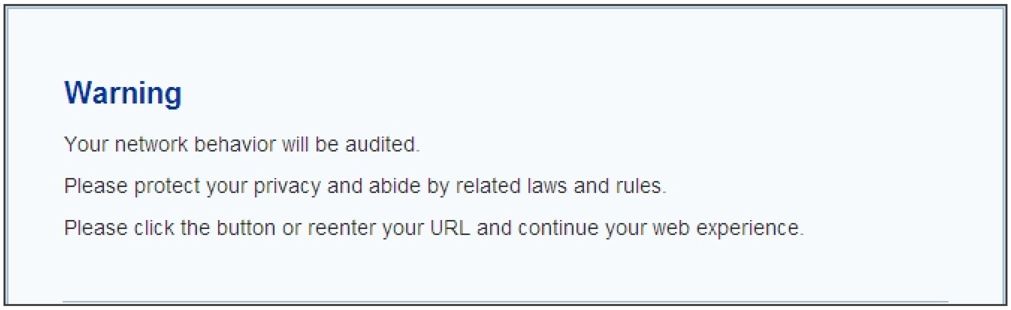
4. Configure the display information in the blocking warning page.

Option	Description
Default	Use the default blocking warning page as shown above. After selecting the **Default** radio button: • If the user-defined warning page is not configured, the predefined warning page will be used. • If the user-defined warning page is configured and enabled, the user-defined warning page will be used.
Redirect page	Redirect to the specified URL. Type the URL in the **URL http://** box. You can click Detection to verify whether the URL is valid.

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

Enabling/ Disabling the Audit Warning

The audit warning function is disabled by default. After enabling the audit warning function, when your network behavior matches the configured URL filtering rule, your HTTP request will be redirected to a warning page where the audit and privacy protection information is displayed. See the picture below:



Warning

Your network behavior will be audited.

Please protect your privacy and abide by related laws and rules.

Please click the button or reenter your URL and continue your web experience.

To enable or disable the audit warning function, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.
3. In the Audit Warning section, select **Enable**.To disable this function, unselect the **Enable** check box.
   - If the user-defined warning page is not configured, the predefined warning page will be used.
   - If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

   For details, please refer to "Warning Page Management" on Page 1198..
4. Click **OK** to save the settings.

First Access of Uncategorized URL

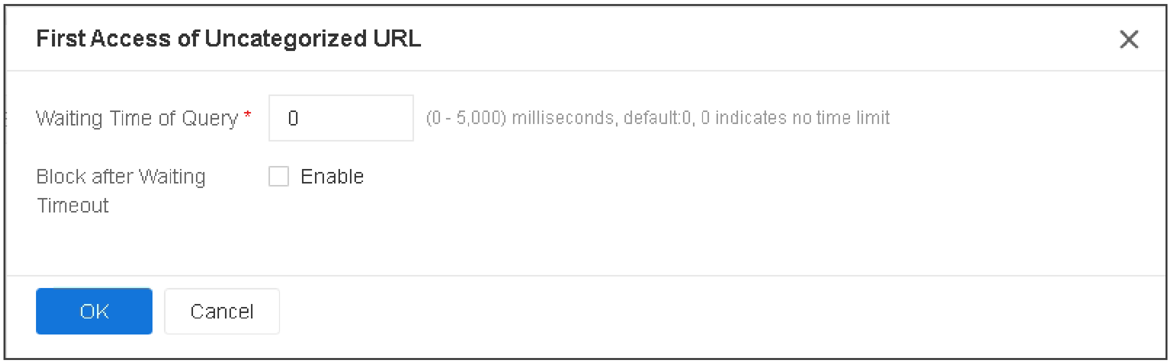
For the uncategorized URL that you visit for the first time, that is, the URL which is neither in the system's predefined URL database nor in the user-defined URL database, system will continue to query the category of the URL in the cloud. Because the query may takes a litter while, system cannot process the uncategorized URL immediately until the query result is returned.

To solve the above problem, you can specify the waiting time of query and enable the block action when waiting times out. After the waiting time of query is exceeded, system will block the access to the uncategorized URL.

To configure related content of the first access of an uncategorized URL, take the following steps:

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

At the top-right corner, select **Configuration** > **First Access of Uncategorized URL**. The First Access of Uncategorized URL dialog box will appear.



First Access of Uncategorized URL

Waiting Time of Query * 0 (0 - 5,000) milliseconds, default:0, 0 indicates no time limit

Block after Waiting Timeout □ Enable

Type the waiting time value of query into the Waiting Time of Query text box. The range is 0 to 5000ms. The default value is 0, which means there is no wait time limit.

Select the Enable check box after Block after Waiting Timeout to enable the block action, after the waiting time of query is exceeded, system will block the access of uncategorized URL. After clearing the Enable check box, after the waiting time of query is exceeded, system will continue to perform URL filtering according to the configuration of URL filtering profile.

Click **OK** to save the settings.

Configuring the URL Blacklist/Whitelist

You can further control the access to some websites by configuring URL blacklists and whitelists.

- After the URL blacklist is configured, when you send an access request to the specified URL in the blacklist, the system will block the request.
- After the URL whitelist is configured, when you send an access request to the specified URL in the whitelist, system will not perform URL filtering for the access request and let the request pass
- The URL blacklist, the URL whitelist and the URL filtering rule all configured with URL categories, the matching priority for URL category filtering is: the URL blacklist > the URL whitelist > the URL filtering rule.

Notes:

- An URL category can only be referenced by an object (URL blacklist, URL whitelist or URL filtering profile). For example, when the URL category "Advertisement" has been added to the URL blacklist, this URL category cannot be added to the URL whitelist, and it will not be referenced in the URL filtering profile.
- Non-root VSYS does not support the URL blacklist\whitelist function, and the URL blacklist/whitelist configuration under root VSYS does not take effect and has no effect on non-root VSYS.

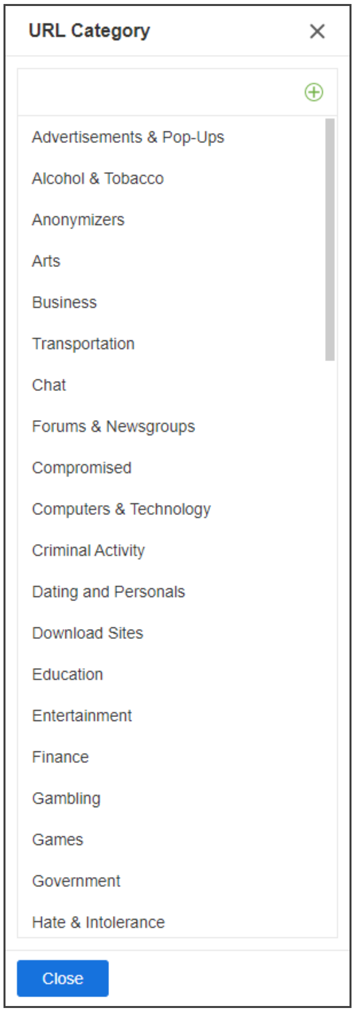
Configuring the URL Blacklist

To configure the URL blacklist, take the following steps:

1. Select **Object > URL Filtering > URL Blacklist/Whitelist**.

2. Select **URL Blacklist** tab to open the URL blacklist page, which displays all URL categories that have been added to the URL blacklist and the corresponding URL type and description.

3. Click "+" , and select the add the URL category needed to add to the URL black list.



4. The "URL category" on the left contains all URL categories that can be referenced (pre-defined URL DB and user-defined URL DB). You can also click ⊕ to create a new URL category. For specific steps, see Configuring User-defined URL DB.

5. If you need to delete the URL category entry in the URL blacklist, in the "URL blacklist" list on the right, select the URL category entry you want to delete and click × .

6. Click **OK**.

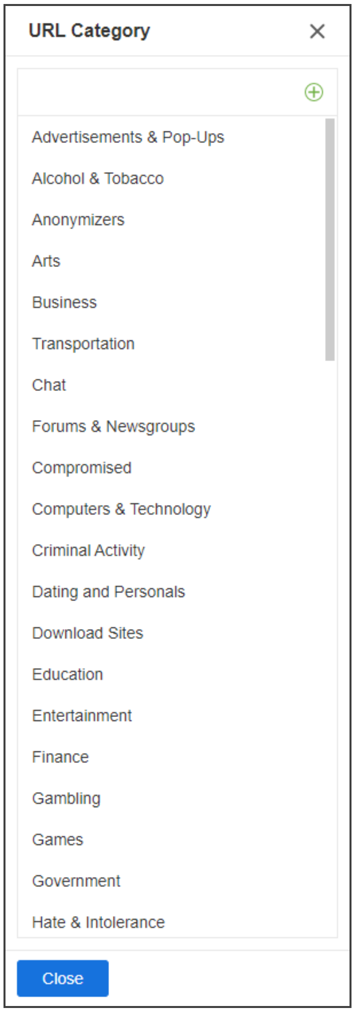
Configuring the URL Whitelist

To configure the URL whitelist, take the following steps:

1. Select **Object > URL Filtering > URL Blacklist/Whitelist**.

2. Select **URL Whitelist** tab to open the URL whitelist page, which displays all URL categories that have been added to the URL whitelist and the corresponding URL type and description.

3. Click "+" , and select the add the URL category needed to add to the URL white list.



4. The "URL category" on the left contains all URL categories that can be referenced (pre-defined URL DB and user-defined URL DB). You can also click ⊕ to create a new URL category. For specific steps, see Configuring User-defined URL DB.

5. If you need to delete the URL category entry in the URL whitelist, in the "URL whitelist" list on the right, select the URL category entry you want to delete and click ✕ .

6. Click **OK**.

Data Security

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The data security function allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs and content logs) on user network behavior.

Data security can audit and filter in the following network behaviors:

Function	Description
File filter	Checks the files transported through HTTP, FTP, SMTP, IMAP, POP3 protocols and control them according to the file filter rules.
Content filter	• Web content :Controls the network behavior of visiting the webpages that contain certain keywords, and log the actions. • Web posting: Controls the network behavior of posting on websites and posting specific keywords, and logs the posting action and posted content. • Email filter: Controls and audit SMTP mails : • Control and audit all the behaviors of sending emails; • Control and audit the behaviors of sending emails that contain specific sender, recipient, keyword or attachment. • Application behavior control: Controls and audits the actions of HTTP, FTP and TELNET applications:

Function	Description
	- FTP contents and methods, including Login, Get, and Put; - HTTP methods, including Connect, Get, Put, Head, Options, Post, and Trace; - Request content initiated by the TELNET client.
Network Behavior Record	Audits the IM applications behaviors and record log messages for the access actions.

Configuring Objects

Objects mean the items referenced during Content Filter rules. When using the data security function, you need to configure the following objects:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Category	Use the keyword category function to customize the keyword categories. You can use it to specify the keyword for the URL category/Web posting/email filter functions.
Warning Page	Enable or disable the warning page. • Block warning: When your network access is blocked, a warning page will prompt in the Web browser. • Audit warning: When your network access is audited, a warning page will prompt in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.

Predefined URL DB

The system contains a predefined URL database.

Notes: The predefined URL database is controlled by a license controlled. Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of Web content/Web posting. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category of a URL, the user-defined URL database has a higher priority than the predefined URL database.

Configuring Predefined URL Database Update Parameters

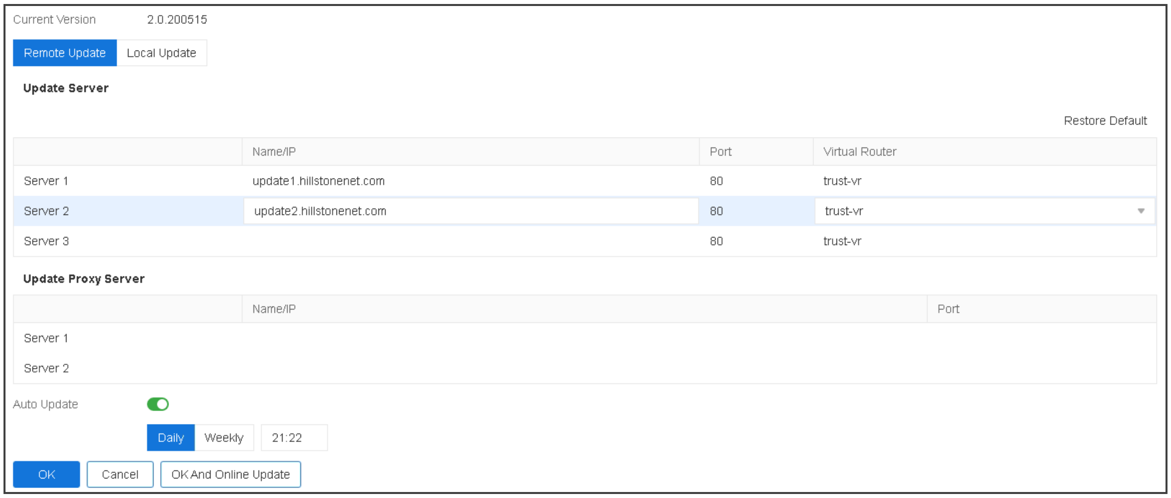
By default, the system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provides: https://update1.hillstonenet.com and https://update2.hillstonenet.com. Besides, you can update the predefined URL database from your local disk.

To change the update parameters:

1. Select **System > Upgrade Management > Signature Database Update**.

2. In the URL category database update section, you can view the current version of the database, perform the remote update, configure the remote update, and perform the local

update.



Current Version 2.0.200515

Update Server

	Name/IP	Port	Virtual Router
Server 1	update1.hillstonenet.com	80	trust-vr
Server 2	update2.hillstonenet.com	80	trust-vr
Server 3		80	trust-vr

Update Proxy Server

	Name/IP	Port
Server 1		
Server 2		

Auto Update ●

Daily Weekly 21:22

3. Click **Enable** button of **Auto Update**to enable the automatic update function. And then continue to specify the frequency and time. Click **OK** to save your settings.

4. Double click an entry of **Update Server** to configure the update server URL. Specify the URL or IP address of the update server, and select the virtual router that can connect to the server. To restore the URL settings to the default ones, click **Restore Default**.

5. Double click an entry of **Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup 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.

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

Upgrading Predefined URL Database Online

To upgrade the URL database online:

1. Select **System > Upgrade Management > Signature Database Update**.

2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local:

1. **System > Upgrade Management > Signature Database Update**

2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.

3. Click **Upload** to update the predefined URL database.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of Web content/Web posting. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL category.

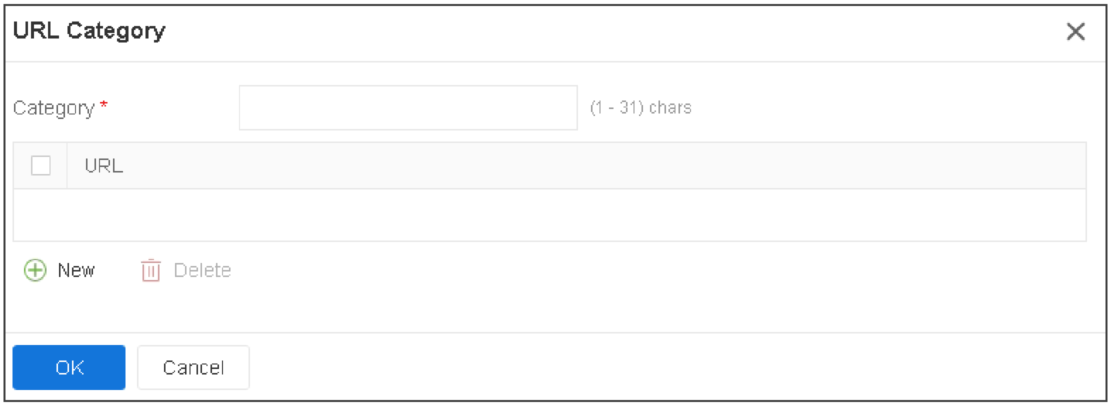
Configuring User-defined URL DB

To configure a user-defined URL category:

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

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.

3. Click **New**. The URL Category dialog appears.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.

5. Type a URL into the **URL http(s)://** box.

6. Click **Add** to add the URL and its category to the table.

7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.

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

Importing User-defined URL

System supports to batch import user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL:

1. Select **Object > URL Filter**.

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.

3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.

4. In the Batch Import URL dialog, click **Browse** button to select your local URL file. The file should be less than 1 M, and has at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.

5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear user-defined URL:

1. Select **Object > URL Filter**.

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.

3. Select one of the predefined URL category(custom1/2/3), and then click **Clear**, the URL in the custom 1/2/3 will be cleared from the system.

URL Lookup

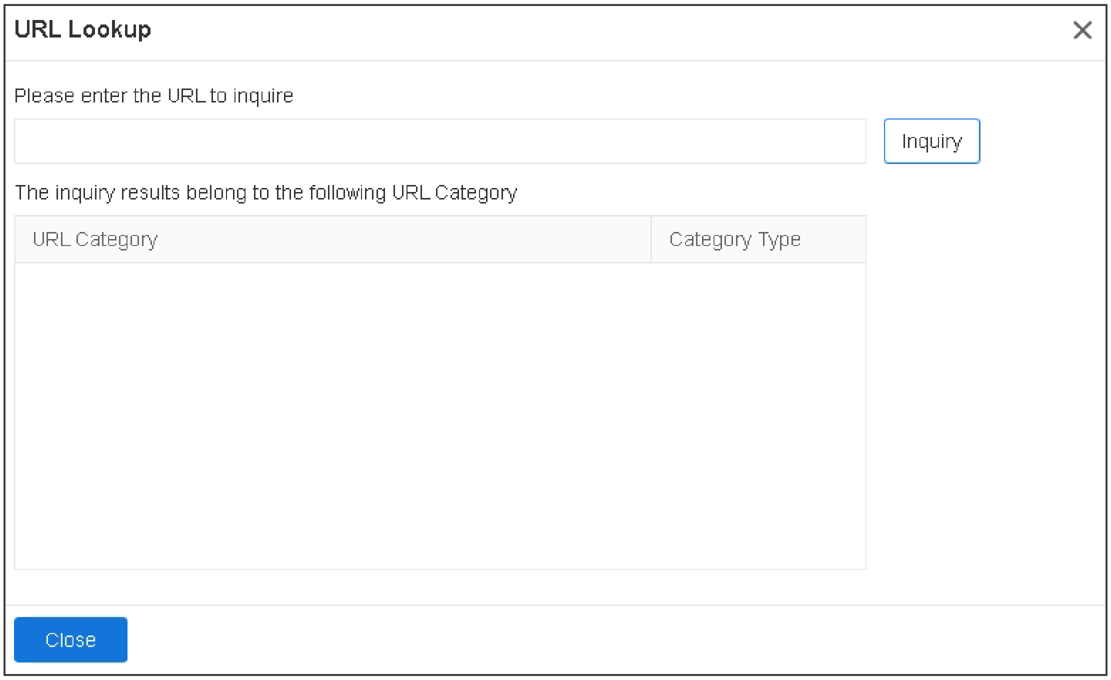
You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information:

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

2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog appears.



URL Lookup

Please enter the URL to inquire

The inquiry results belong to the following URL Category

URL Category	Category Type

3. Type the URL into the **Please enter the URL to inquire** box.

4. Click **Inquire**, and the results will be displayed at the bottom of the dialog.

Configuring URL Lookup Servers

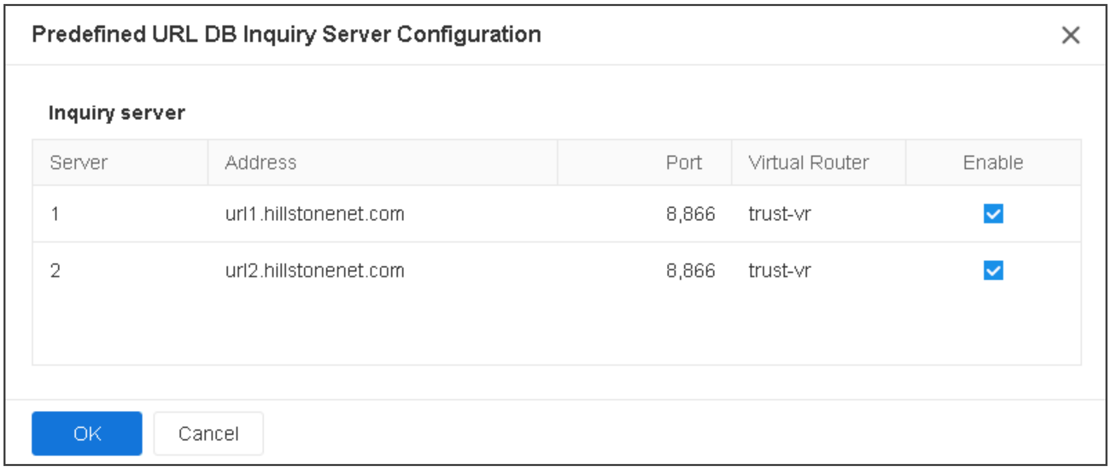
URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server:

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

2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog appears.

3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog appears.



Predefined URL DB Inquiry Server Configuration

Inquiry server

Server	Address	Port	Virtual Router	Enable
1	url1.hillstonenet.com	8,866	trust-vr	☑
2	url2.hillstonenet.com	8,866	trust-vr	☑

4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.

5. Select the check box in the **Enable** column to enable this URL lookup server.

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

Keyword Category

You can customize the keyword category and use it in the internet behavior control function.

After configuring a internet behavior control rule, the system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times* * *trust value* of each keyword that belongs to the category. Then the system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;

- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a web content rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

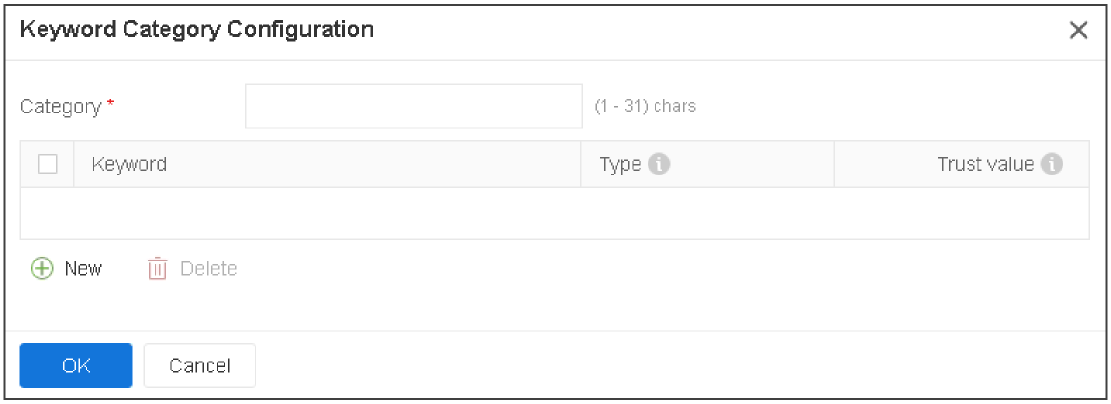
If the system detects 1 occurrence of K1 and K2 each on a web page, then C1 trust value is 20*1＋40*1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the web page access is permitted.

If the system detects 3 occurrences of K1 and 1 occurrence of K2 on a web page, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category:

1. Select **Object > URL Filtering> Profile**.
2. At the top-right corner, Select **Configuration > Keyword Category**. The Keyword Category dialog appears.
3. Click **New**. The **Keyword Category Configuration** dialog appears.



4. Type the category name.

5. Click **New**. In the slide area, specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).

6. Click **Add** to add the keyword to the list below.

7. Repeat the above steps to add more keywords.

8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.

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

Warning Page

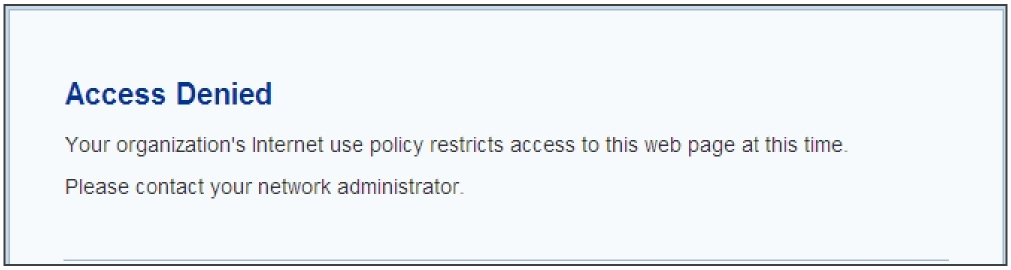
The warning page shows the user block information and user audit information. You can enable or disable the warning page as needed.

The warning page include predefined warning page and user-defined warning page.

- Predefined warning page: Displays the predefined warning information content, including prompt information and warning reasons.
- User-defined warning page: You can customize the warning page by custom warning information and pictures. For details, please refer to "Warning Page Management" on Page 1198..

Enabling/ Disabling the Block Warning

The block warning is disabled by default. If the internet behavior is blocked by the internet behavior control function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. The predefined warning page below:



Access Denied

Your organization's Internet use policy restricts access to this web page at this time.

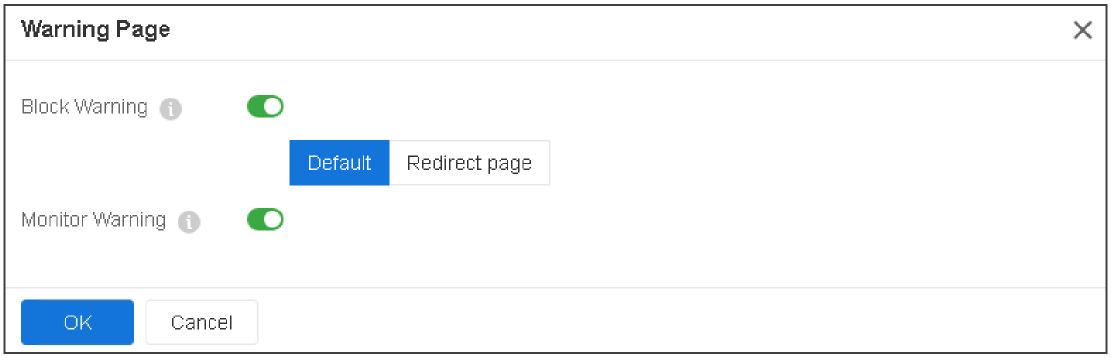
Please contact your network administrator.

After enabling the block warning function, block warning information will be shown in the browser when one of the following actions is blocked:

- Visiting the web page that contains a certain type of keyword category
- Posting information to a certain type of website or posting a certain type of keywords
- HTTP actions of Connect, Get, Put, Head, Options, Post, and Trace.

To enable or disable the block warning:

1. Click **Object > URL Filtering> Profile**.
2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.



Warning Page

Block Warning ●

Default | Redirect page

Monitor Warning ●

3. In the Block Warning section, select **Enable.**To disable this function, unselect the **Enable** check box.
   - If the user-defined warning page is not configured, the predefined warning page will be used.

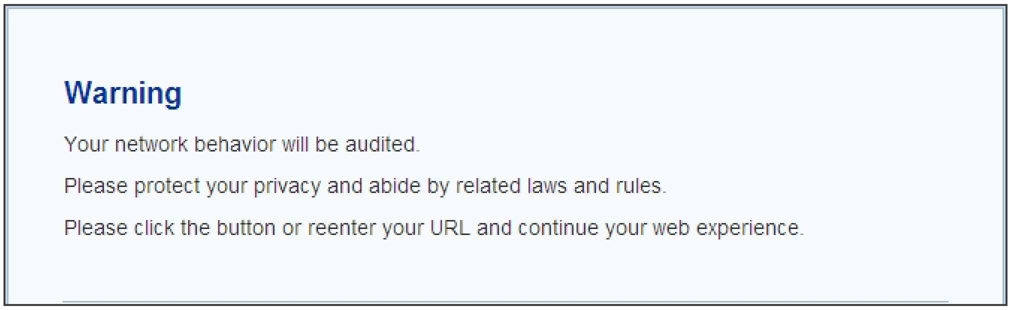
- If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

For details, please refer to "Warning Page Management" on Page 1198..

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

Enabling/ Disabling the Audit Warning

The audit warning function is disabled by default. After enabling the audit warning function, when your internet behavior matches the configured internet behavior rules, your HTTP request will be redirected to a warning page, on which the audit and privacy protection information is displayed. See the picture below:



Warning

Your network behavior will be audited.

Please protect your privacy and abide by related laws and rules.

Please click the button or reenter your URL and continue your web experience.

To enable or disable the audit warning function:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.
3. In the Audit Warning section, select **Enable**.To disable this function, unselect the **Enable** check box.
   - If the user-defined warning page is not configured, the predefined warning page will be used.

- If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

For details, please refer to "Warning Page Management" on Page 1198..

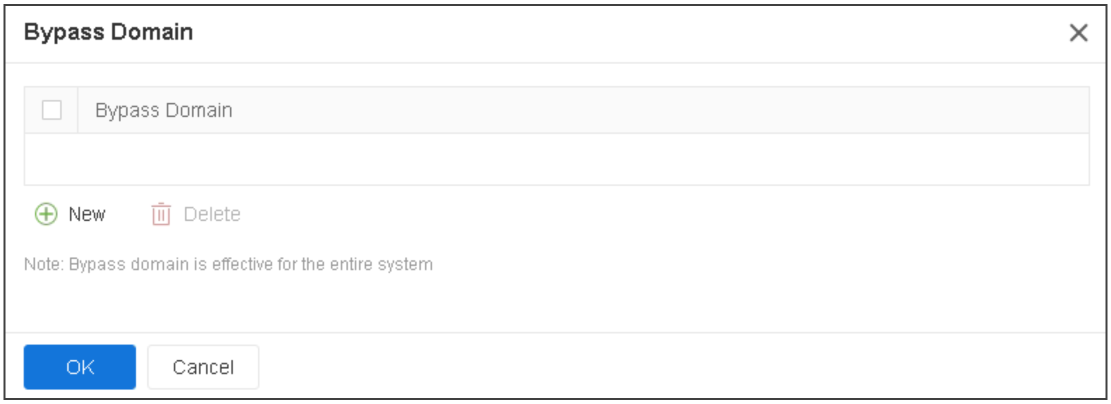
4. Click **OK** to save the settings.

Bypass Domain

Regardless of internet behavior control rules, requests to the specified bypass domains will be allowed unconditionally.

To configure a bypass domain:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Bypass Domain**. The Bypass Domain dialog appears.



Note: Bypass domain is effective for the entire system

3. Click **New**.In the text box, type the domain name. The domain name will be added to the system and displayed in the bypass domain list.
4. Click **OK** to save the settings.

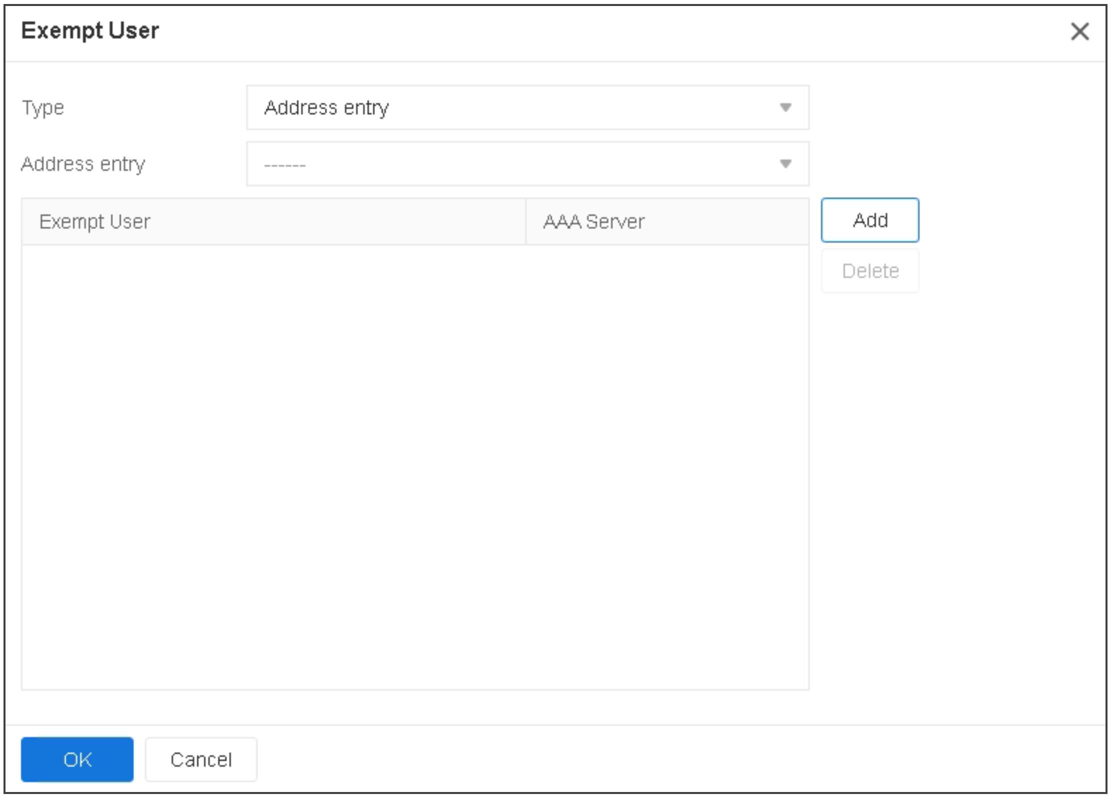
Exempt User

The Exempt User function is used to specify the users who will not be controlled by the internet behavior control rules. The system supports the following types of exempt user: IP, IP range, role, user, user group, and address entry.

To configure the user exception:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.

2. At the top-right corner, Select **Configuration > Exempt User**. The Exempt User dialog appears.



Exempt User

Type: Address entry

Address entry: -------

Exempt User	AAA Server

3. Select the type of the user from the **Type** drop-down list.

4. Configure the corresponding options.

5. Click **Add**. The user will be added to the system and displayed in the exempt user list.

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

File Filter

The file filter function checks the files transported through HTTP, FTP, SMTP, IMAP, POP3 protocols and control them according to the file filter rules.

- Be able to check and control the files transported through GET and POST methods of HTTP, FTP, SMTP, IMAP, and POP3.
- Support file type filter conditions.
- Support block, log, and permit actions.

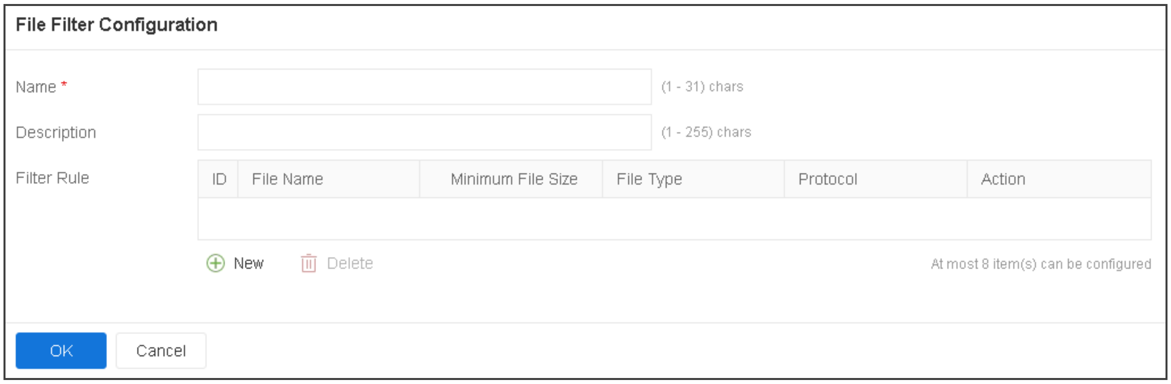
After you bind the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile.

Creating File Filter Rule

Use the file filter rule to specify the protocol that you want to check, the filter conditions, and the actions.

To create a file filter rule:

1. Select **Object** > **Data Security** > **File Filter**.
2. Click **New**.



File Filter Configuration

Name * (1 - 31) chars

Description (1 - 255) chars

Filter Rule

ID	File Name	Minimum File Size	File Type	Protocol	Action

3. **In the dialog box, enter values.**

Option	Description
Name	Specifies the name of the file filter rule.
Description	Specifies the description of the file filter rule.
Filter Rule	
ID	The ID of file filter rule item. There can be up to 8 items in each file filtering rule. Click the **+** button to add a file filter rule item. If one filter rule item is configured with the block action and the file happens to match this rule, then the system will block the uploading/downloading of this file.
Minimum File Size	When the size of the transported file reaches the specified file size, the system will trigger the actions. The range is from 1 to 512,000. The unit is KB.
File Type	Specify the file type. Click on the column's cells and select from the drop-down menu. You can specify more than one file types. To control the file type that not supported, you can use the UNKNOWN type. When the transmitted file is a particular type, the system will trigger the actions. The file filter function can identify the following file types: 7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV,

Option	Description
	MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, BZ2, UNKNOWN
Protocol	Specifies the protocols. http-get represents to check the files transported through the GET method of HTTP. http-post represents to check the files transported through the POST method of HTTP. ftp represents to check the files transported through FTP. smtp represents to check the files transported through SMTP. imap represents to check the files transported through IMAP. pop3 represents to check the files transported through POP3. You can specify more than one protocol types. This option is required.
Action	Specify the action to control the files that matches the filter conditions. You can specify block or log. This option is required.

4. Click **OK**.

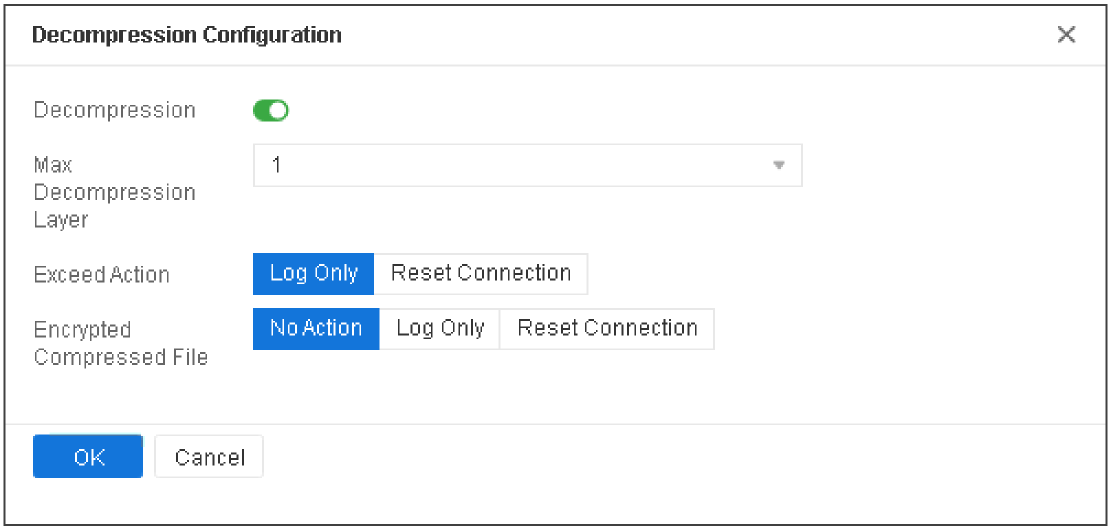
Configuring Decompression Control Function

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.

To configure the decompression control function, take the following steps:

1. Select **Object > Data Security > File Filter**.

2. At the top-right corner, click **Compression Configuration**.



Decompression Configuration

Decompression: On

Max Decompression Layer: 1

Exceed Action: Log Only [✓] | Reset Connection

Encrypted Compressed File: No Action [✓] | Log Only | Reset Connection

In the Compression Configuration dialog box, configure the following options.

Option	Description
Decompression	Select / clear the **Enable** check box to enable / disable the decompression function.
Max Decompression Layer	By default, StoneOS can check the files of up to 5 decompression layers. To specify a decompression layer, select a value from the drop-down list. The value range is 1 to 5.
Exceed Action	Specifies an action for the compressed files that exceed the max decompression layer. Select an action from the drop-down list: • Log Only - Only generates logs but will not check and control the files. This action is enabled by default. • Reset Connection - Resets connections for the files.
Encrypted Compressed File	Specifies an action for encrypted compressed files: • ------ - Will not take any actions against the files, but might further check and control the files according to the file filter rule. • Log Only - Only generates logs but will not check and control the files. • Reset Connection - Resets connections for the files.

3. Click **OK**.

Notes: For compressed files containing docx, pptx, xlsx, jar, and apk formats, when **Exceed Action** is specified as **Reset Connection**, the maximum compression layers should be added one more layer to prevent download failure.

Viewing File Filter Logs

To view the file filter logs, refer to "File Filter Log" on Page 1112.

Content Filter

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Includes :

- "Web Content" on Page 712: Controls the network behavior of visiting the webpages that contain certain keywords, and log the actions.
- "Web Posting" on Page 718: Controls the network behavior of posting on websites and posting specific keywords, and logs the posting action and posted content.
- "Email Filter" on Page 724: Controls and audit SMTP mails :
    - Control and audit all the behaviors of sending emails.
    - Control and audit the behaviors of sending emails that contain specific sender, recipient, keyword or attachment.
- "APP Behavior Control" on Page 730:Controls and audits the actions of HTTP and FTP applications:
    - FTP methods, including Login, Get, and Put.
    - HTTP methods, including Connect, Get, Put, Head, Options, Post, and Trace.

Web Content

The web content function is designed to control the network behavior of visiting the websites that contain certain keywords. For example, you can configure to block the access to website that contains the keyword "gamble", and record the access action and website information in the log.

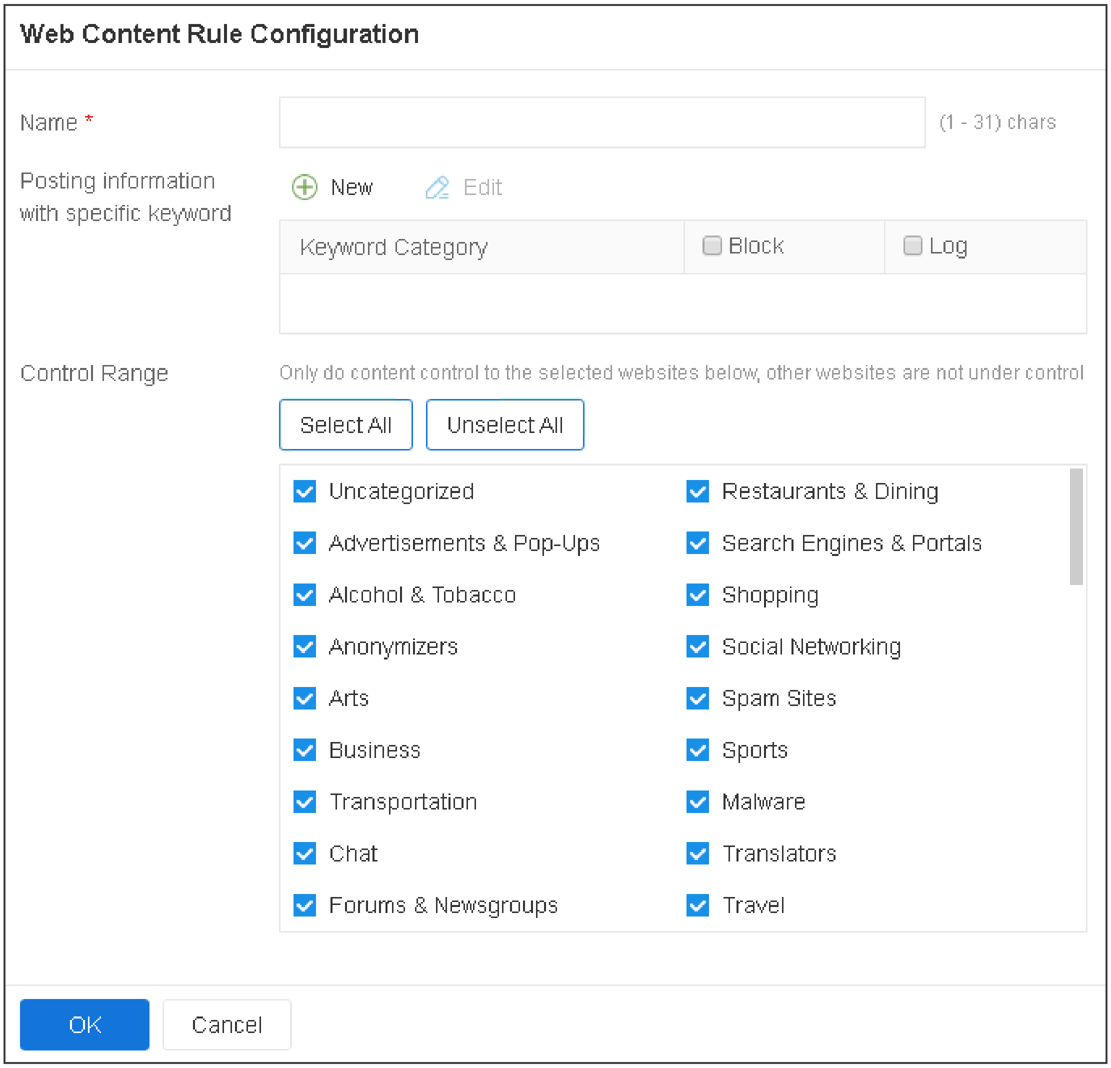
Configuring Web Content

Configuring Web Content contains two parts:

- Create a Web Content rule
- Bind a Web Content rule to a security zone or policy rule

Part 1: Creating a web content rule

1. Select **Object** > **Data Security** > **Content Filter** > **Web Content**.
2. Click **New**.



Web Content Rule Configuration

Name * [ ] (1 - 31) chars

Posting information with specific keyword

New Edit

Keyword Category	□ Block	□ Log

Control Range

Only do content control to the selected websites below, other websites are not under control

Select All Unselect All

☑ Uncategorized
☑ Advertisements & Pop-Ups
☑ Alcohol & Tobacco
☑ Anonymizers
☑ Arts
☑ Business
☑ Transportation
☑ Chat
☑ Forums & Newsgroups
☑ Restaurants & Dining
☑ Search Engines & Portals
☑ Shopping
☑ Social Networking
☑ Spam Sites
☑ Sports
☑ Malware
☑ Translators
☑ Travel

OK Cancel

In the Web Content Rule Configuration dialog box, enter values.

Option	Description
Name	Specifies the rule name.
Posting information with specific keyword	Defines the action when a keyword is matched. • New: Creates new keyword categories. For more information about keyword category, see "Configuring Objects" on Page 690.

Option	Description
	• Edit: Edits selected keyword category. • Keyword category: Shows the name of configured keyword categories. • Block: Select the check box to block the web pages containing the corresponding keywords. • Log: Select the check box to record log messages when visiting the web pages containing the corresponding keywords. • Record contents: Select the check box to record the keyword context. This option is available only when the device has a storage media (SD card, U disk, or storage module provided by Hillstone) with the NBC license installed.
Control Range	Specify the coverage of this rule. By default, the rule applies to all website. 1. Click **Control Range**. 2. Select or unselect the websites you want to monitor and control. 3. Click **OK**.

3. Click **OK**.

Part 2: Binding a Web Content rule to a security zone or security policy rule

The Web content configurations are based on security zones or policies.

- If a security zone is configured with the Web content function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the Web content function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the Web content configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based Web Content:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 74.
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a Web content rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a Web content rule, see Creating a Web content rule.
4. Click **OK** to save the settings.

To realize the policy-based Web content:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 769.
2. In the Data Security tab, select the **Enable** check box of Web Content.
3. From the **Profile** drop-down list, select a Web Content rule. You can also click **Add Profile** to create a new Web Content rule.
4. Click **OK** to save the settings.

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
User Exception	Users that are not controlled by the internet behavior control rules.

Notes:

- To enusre you have the latest URL database, it is better to update your database first. Refer to "Configuring Objects" on Page 690.

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1115.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Keyword Blocking in Web Content

If you have configured email filter with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > Web Content**, you will see the monitored results. For more about monitoring, refer to "Web Content" on Page 1058.

Viewing Logs of Keyword Blocking in Web Content

To see the system logs of keyword blocking in web content, please refer to the "Content Filter Log" on Page 1113.

Web Posting

The web posting function can control the network behavior of posting on websites and posting specific keywords, and can log the posting action and posting content. For example, forbid the users to post information containing the keyword X, and record the action log.

Configuring Web Posting

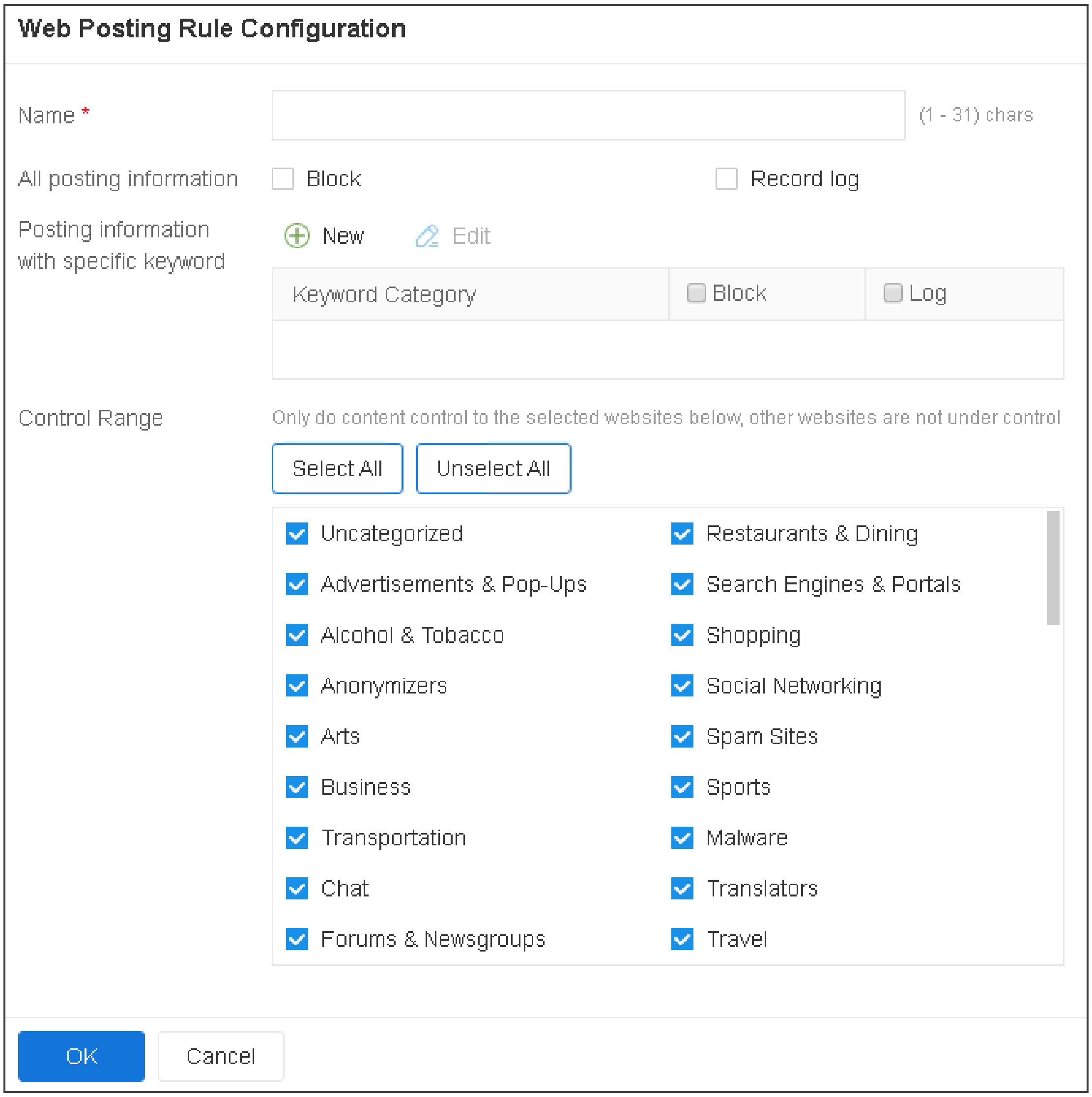
Configuring Web Posting contains two parts:

- Create a web posting rule
- Bind a web posting rule to a security zone or policy rule

Part 1: Creating a web posting rule

1. Select **Object > Data Security > Content Filter > Web Posting**.

2. Click **New**.



Web Posting Rule Configuration

Name * □ (1 - 31) chars

All posting information □ Block □ Record log

Posting information with specific keyword

Keyword Category	□ Block	□ Log

Control Range

Only do content control to the selected websites below, other websites are not under control

☑ Uncategorized
☑ Advertisements & Pop-Ups
☑ Alcohol & Tobacco
☑ Anonymizers
☑ Arts
☑ Business
☑ Transportation
☑ Chat
☑ Forums & Newsgroups
☑ Restaurants & Dining
☑ Search Engines & Portals
☑ Shopping
☑ Social Networking
☑ Spam Sites
☑ Sports
☑ Malware
☑ Translators
☑ Travel

In the Web Posting Rule Configuration dialog, enter values.

Option	Description
Name	Specifies the rule name.
All posting information	The action applies to all web posting content.

Option	Description
	- Block: Select to block all web posting behaviors. - Record Log: Select to record all logs about web posting.
Posting information with specific keyword	Controls the action of posting specific keywords. The options are: - New: Creates new keyword categories. For more information about keyword category, see "Keyword Category" on Page 697. - Edit: Edits selected keyword category. - Keyword category: Shows the name of configured keyword categories. - Block: Blocks the posting action of the corresponding keywords. - Log: Records log messages when posting the corresponding keywords.
Control Range	Specify the coverage of this rule. By default, the rule applies to all website. 1. Click **Control Range**. 2. Select or unselect the websites you want to monitor and control. 3. Click **OK**.

3. Click **OK**.

Part 2: Binding a Web Posting rule to a security zone or security policy rule

The web posting configurations are based on security zones or policies.

- If a security zone is configured with the web posting function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the web posting function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the web posting configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based web posting:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 74.
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a Web content rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a Web content rule, see Creating a web posting rule.
4. Click **OK** to save the settings.

To realize the policy-based web posting:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 769.
2. In the Data Security tab, select the **Enable** check box of web posting.
3. From the **Profile** drop-down list, select a web posting rule. You can also click **Add Profile** to create a new web posting rule.
4. Click **OK** to save the settings.

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	**Description**
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
User Exception	Users that are not controlled by the internet behavior control rules.

Notes:

- To enusre you have the latest URL database, it is better to update your database first. Refer to "Configuring Objects" on Page 690.

- If there is an action conflict between setting for "all websites" and "specific keywords", when a traffic matches both rules, the "deny" action shall prevail.
- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1115.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Keyword Blocking in Web Posts

If you have configured web posting rule with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor** > **Keyword Block** > **Web Posting**, you will see the monitored results. For more about monitoring, refer to "Keyword Block" on Page 1058.

Viewing Logs of Keyword Blocking in Web Posts

To see the system logs of keyword blocking in web posts, please refer to the "Content Filter Log" on Page 1113.

Email Filter

The email filter function is designed to control the email sending actions according to the sender, receiver, email content and attachment, and record the sending log messages. Both the SMTP emails and the web mails can be controlled.

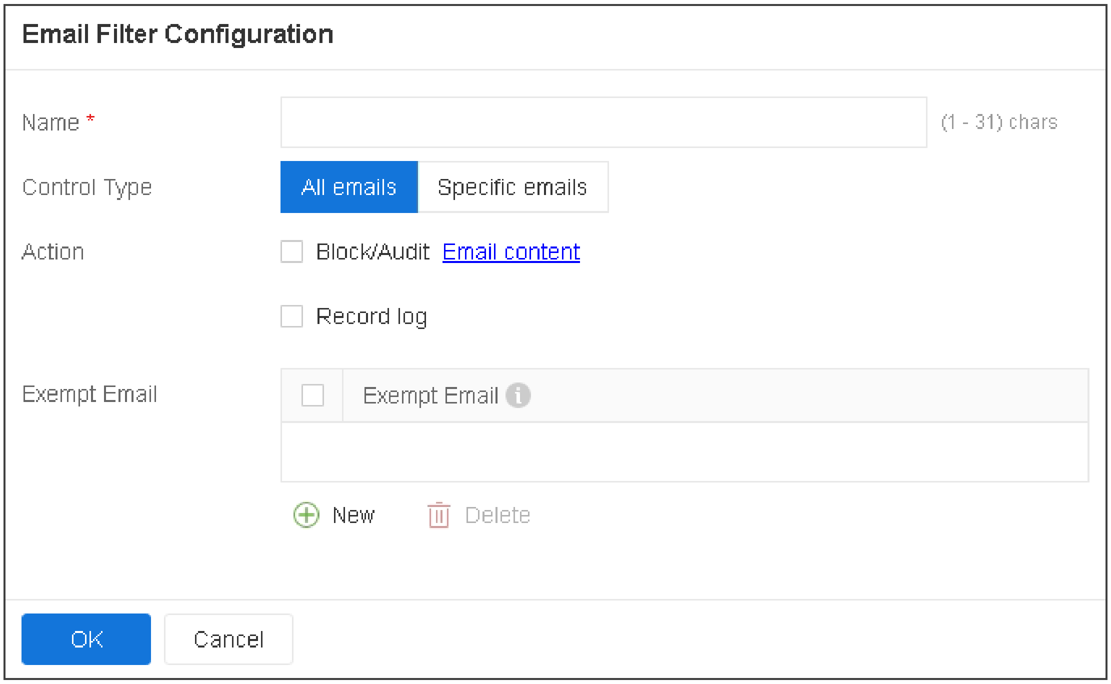
Configuring Email Filter

Configuring email filter contains two parts:

- Create an email filter rule
- Bind an email filter rule to a security zone or policy rule

Part 1: Creating an email filter rule

1. Select **Object** > **Data Security** > **Content Filter** > **Email Filtering Log**.
2. Click **New**.



In the dialog box, enter values.

Option	Description
Name	Specifies the rule name.
Control Type	All emails - This option applies to all the sending emails. - Record Log - Select this check box if you want all emails to be logged.
	Specific mail items - This option applies to specific mail items. To configure the email sender: 1. Click **Sender**. 2. In the prompt, enter sender's email address. 3. Click **Add**. 4. You may select to block the sender or keep a record. 5. Click **OK**. To configure the email receiver: 1. Click **Recipient**. 2. In the prompt, enter email receiver's email address. 3. Click **Add**. 4. You may select to block the receiver or keep a record. 5. Click **OK**.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<ol>
<li>Click <b>email content</b>.</li>
<li>In the prompt, click <b>Add</b>. See the Keyword Category part in "Configuring Objects" on Page 690.</li>
<li>You may select to block the email containing keywords or keep a record.</li>
</ol>
<table>
<tr><td><b>Other emails</b></td><td>Select an action for emails other than which are added above.</td></tr>
</table>
</td></tr>
<tr><td colspan="2"><b>Exempt Email</b></td></tr>
<tr><td>Exempt Email</td><td>To configure mail addresses that do not follow the regulations of email filter:
<ol>
<li>Click <b>Exempt Email</b>.</li>
<li>In the prompt, enter emails that do not obey email filter.</li>
<li>Click <b>Add</b>, and you can add more.</li>
<li>Click <b>OK</b>.</li>
</ol>
</td></tr>
</table>

Part 2: Binding an Email filter rule to a security zone or security policy rule

The email filter configurations are based on security zones or policies.

- If a security zone is configured with the email filter function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.

- If a policy rule is configured with the email filter function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the email filter configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based email filter:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 74.
2. In the Zone Configuration dialog, select Threat Protection tab.
3. Enable the threat protection you need, and select an email filter rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create an email filter rule, see Creating an email filter rule.
4. Click **OK** to save the settings.

To realize the policy-based email filter:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 769.
2. In the Protection tab, select the **Enable** check box of email filter.
3. From the **Profile** drop-down list, select an email filter rule. You can also click **Add Profile** to create a new email filter rule.
4. Click **OK** to save the settings.

If needed, you can also configure SSL proxy, keyword category, warning page, bypass domain and user exempt user.

To configure those features, click **Configuration** on the right top corner of the Email Filtering Log list page.

Option	Description
Keyword Category	Use the keyword category function to customize the keyword categories. You can use it to specify the keyword for the URL category/Web posting/email filter functions.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.

Notes:

- If an email filter rule has added all three of Audit/Block Sender, Receiver and email content, the rule will take effect when one of them is hit.
- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1115.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Email Keyword Blocking

If you have configured email filter with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > Email Content**, you will see the monitored results. For more about monitoring, refer to "Email Content" on Page 1059.

Viewing Logs of Emails Keyword Blocking

To see the system logs of email's keywords, please refer to the "Content Filter Log" on Page 1113.

APP Behavior Control

The APP behavior control function is designed to control and audit (record log messages) the actions of FTP, HTTP and TELNET applications, including:

- Controlling and auditing the FTP content and Login, Get, and Put actions;
- Controlling and auditing the Connect, Get, Put, Head, Options, Post, Trace, Delete actions of HTTP;
- Controlling and auditing the request content initiated by TELNET client.

Configuring APP Behavior Control

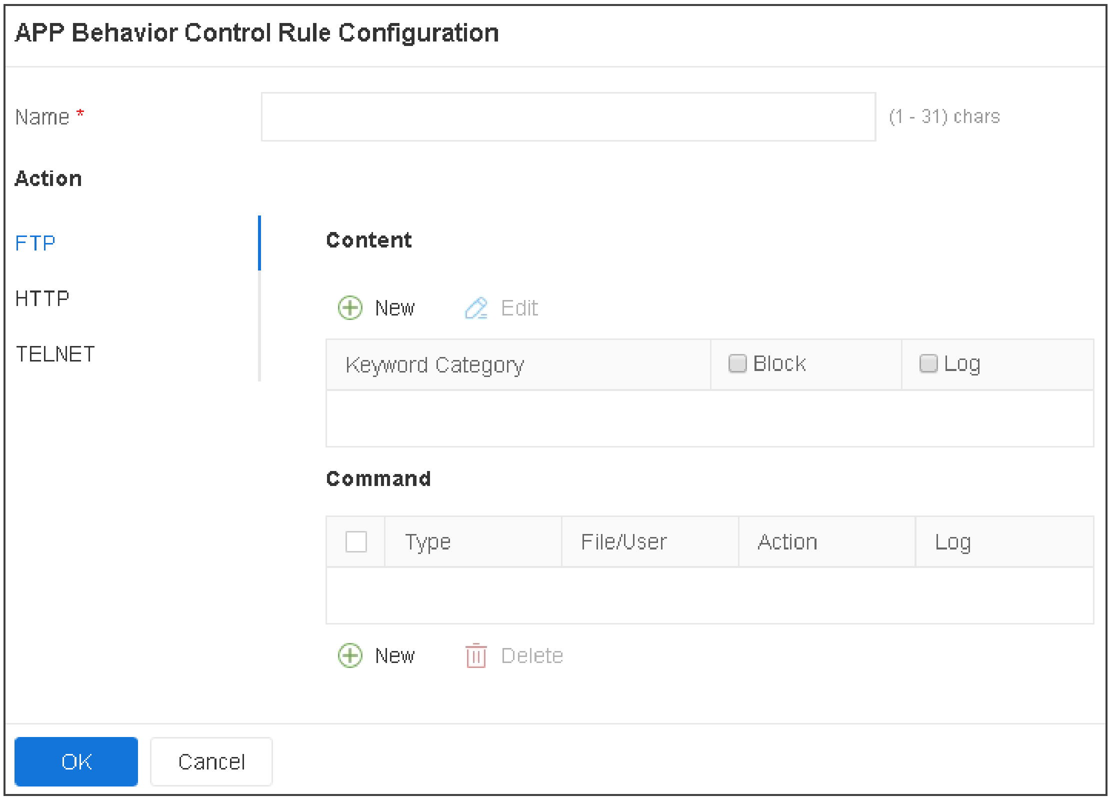
Configuring behavior control contains two parts:

- Creating an application behavior control rule
- Binding an application behavior control rule to a security zone or policy rule

Part 1: Creating an APP behavior control rule

1. Select **Object > Data Security > Content Filter > APP Behavior Control**.

2. Click **New**.



In the APP Control Rule Configuration dialog box, enter values.

Option	Description
Name	Specifies the rule name.
Action	
FTP	Content: Controls the FTP content. If the content matches the specified keyword categories, system will execute the specified action, including **Block** or **Log**. Expand the **Content**, and configure the control options. • **New**: Click the button to create a keyword category. For how to create the category, refer to the Keyword Category of Configuring Objects.

Option	Description
	- **Edit**: Select one keyword from the list and edit the category. - **Keyword Category**: Displays the keyword categories in system. - **Block**: Select the check box to block the FTP content matching the keyword category. - **Log**: Select the check box to record logs when the FTP content matches the keyword category. Command: Controls the FTP methods, including Login, Get, and Put. Expand the **Command**, and configure the control options. - From the first drop-down list, select the method to be controlled, it can be GET, PUT, or Login. - Type the file name (for the method of GET or PUT) or user name (for the method of Login) into the next box. - From the second drop-down list, select the action. It can be Block or Permit. - From the third drop-down list, specify whether to record the log messages. - Click **Add**. - Repeat Step 1 to 5 to add more control entries.

Option	Description
	To edit/delete a control entry, select the entry from the list, and then click **Edit** or **Delete**.
HTTP	Comment: Controls the HTTP methods, including Connect, GET, PUT, Head, Options, Post, Trace, and Delete. Expand HTTP, and configure the HTTP control options. • From the first drop-down list, select the method to be controlled, it can be Connect, GET, PUT, Head, Options, Post, Trace, or Delete. • Type the domain name into the next box. • From the second drop-down list, select the action. It can be Block or Permit. • From the third drop-down list, specify whether to record the log messages. • Click **Add**. • Repeat Step 1 to 5 to add more control entries. To edit/delete a control entry, select the entry from the list, and then click **Edit** or **Delete**.
TELNET	Content: Controls the request content initiated by the TELNET client. If the content matches the specified keyword categories, system will execute the specified action, including **Block** or **Log**. Expand the **Content**, and configure the control options.

Option	Description
	- **New**: Click the button to create a keyword category. For how to create the category, refer to the Keyword Category of Configuring Objects. - **Edit**: Select one keyword from the list and edit the category. - **Keyword Category**: Displays the keyword categories in system. - **Block**: Select the check box to block the request content matching the keyword category. - **Log**: Select the check box to record logs when the request content matches the keyword category.

3. Click **OK**.

Part 2: Binding an APP behavior control rule to a security zone or security policy rule

The APP behavior control configurations are based on security zones or policies.

- If a security zone is configured with the APP behavior control function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.

- If a policy rule is configured with the APP behavior control function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.

- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the APP behavior control configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based APP behavior control:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 74.

2. In the Zone Configuration dialog, select Data Security tab.

3. Enable the threat protection you need, and select an email filter rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create an APP behavior control rule, see Creating an APP behavior control rule.

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

To realize the policy-based APP behavior control:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 769.

2. In the Data Security tab, select the **Enable** check box of APP behavior control.

3. From the **Profile** drop-down list, select a APP behavior control rule. You can also click **Add Profile** to create a new APP behavior control rule.

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

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	**Description**
Predefined URL database	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL database	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.

Option	Description
URL lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword category	Customizes keyword categories as needed.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.

Notes:

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1115.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Logs of APP Behavior Control

To see the system logs of APP behavior control, please refer to the "Content Filter Log" on Page 1113.

Network Behavior Record

Network behavior record function audits the IM applications behaviors and record log messages for the access actions, includes:

- Audits the QQ, WeChat and sinaweibo user behaviors.
- Log the access behaviors.

Configuring Network Behavior Recording

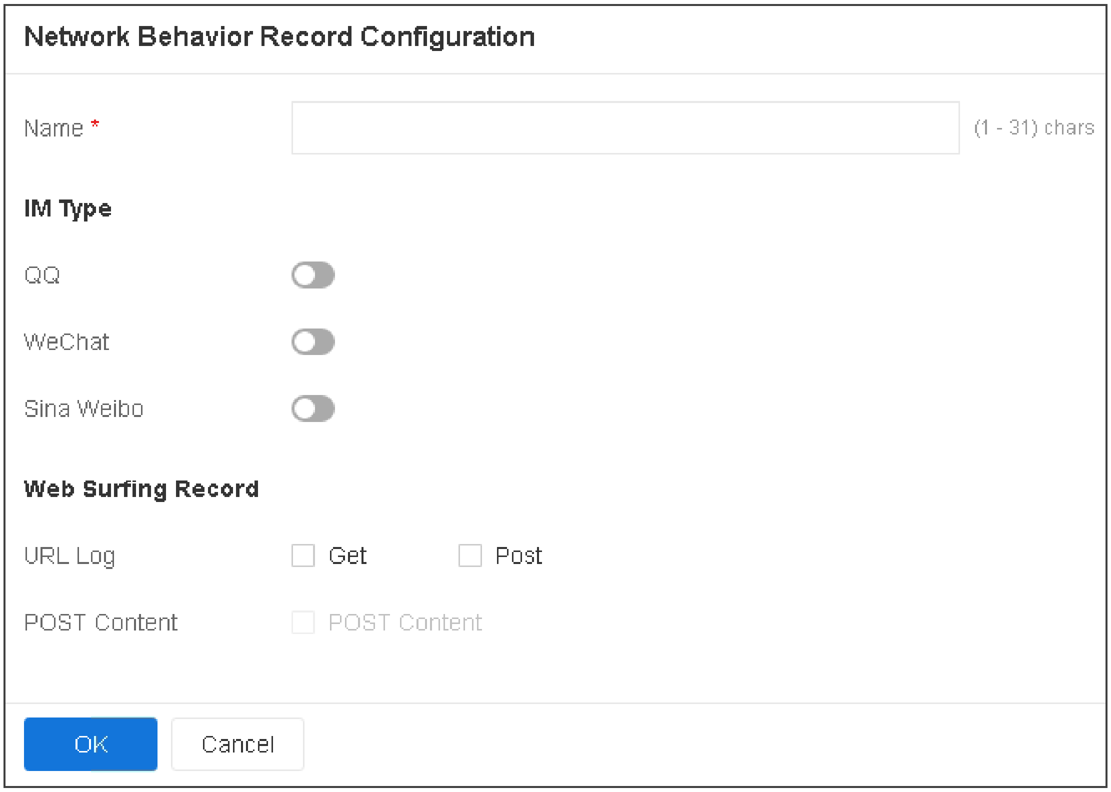
Configuring network behavior record contains two parts:

- Create a network behavior record rule
- Bind a network behavior record rule to a security zone or policy rule

Part 1: Creating a NBR rule

1. Select **Object > Data Security > Network Behavior Record**.

2. Click **New**.



Network Behavior Record Configuration

Name * (1 - 31) chars

IM Type

QQ

WeChat

Sina Weibo

Web Surfing Record

URL Log □ Get □ Post

POST Content □ POST Content

OK Cancel

In the Network Behavior Record Configuration dialog box, enter values.

Option	Description
Name	Specifies the rule name.
IM	
QQ	To audits the QQ behavior. 1. Select the **QQ** checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 10. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the

Option	Description
	timeout reaches, it will trigger new logs.
WeChat	To audits the WeChat behavior. 1. Select the **Wechat** checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Sina Weibo	To audits the sina weibo behavior. 1. Select the **Sina Weibo** checkbox 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Web Surfing Record	
URL Log	logs the GET and POST methods of HTTP. • Get: Records the logs when having GET methods. • Post: Records the logs when having POST methods.
POST Content	Post Content: Records the posted content.

3. Click **OK**.

Part 2: Binding a network behavior record rule to a security zone or security policy rule

The network behavior record configurations are based on security zones or policies.

- If a security zone is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the network behavior record configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based network behavior record:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 74.
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a network behavior record rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a network behavior record rule, see Creating a network behavior record rule.
4. Click **OK** to save the settings.

To realize the policy-based network behavior record:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 769.
2. In the Data Security tab, select the **Enable** check box of network behavior record.

3. From the **Profile** drop-down list, select a network behavior record rule. You can also click **Add Profile** to create a new network behavior record rule.

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

Notes:

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1115
- By default, a rule will immediately take effect after you click **OK** to complete configuration

Viewing Logs of Network Behavior Recording

To see the logs of network behavior recording, please refer to the "Network Behavior Record Log" on Page 1114.

NetFlow

NetFlow is a data exchange method, which records the source /destination address and port numbers of data packets in the network. It is an important method for network traffic statistics and analysis.

Hillstone NetFlow supports the NetFlow Version 9. With this function configured, the device can collect user's ingress traffic according to the NetFlow profile, and send it to the server with NetFlow data analysis tool, so as to detect, monitor and charge traffic.

Related Topics:

- "Configuring NetFlow" on Page 743

Configuring NetFlow

The NetFlow configurations are based on interfaces.

To configure the interface-based NetFlow, take the following steps:

1. Click **Object > NetFlow > Configuration**. Select **Enable** check box to enable the NetFlow function.

2. Click **Object > NetFlow > Profile** to create a NetFlow rule .

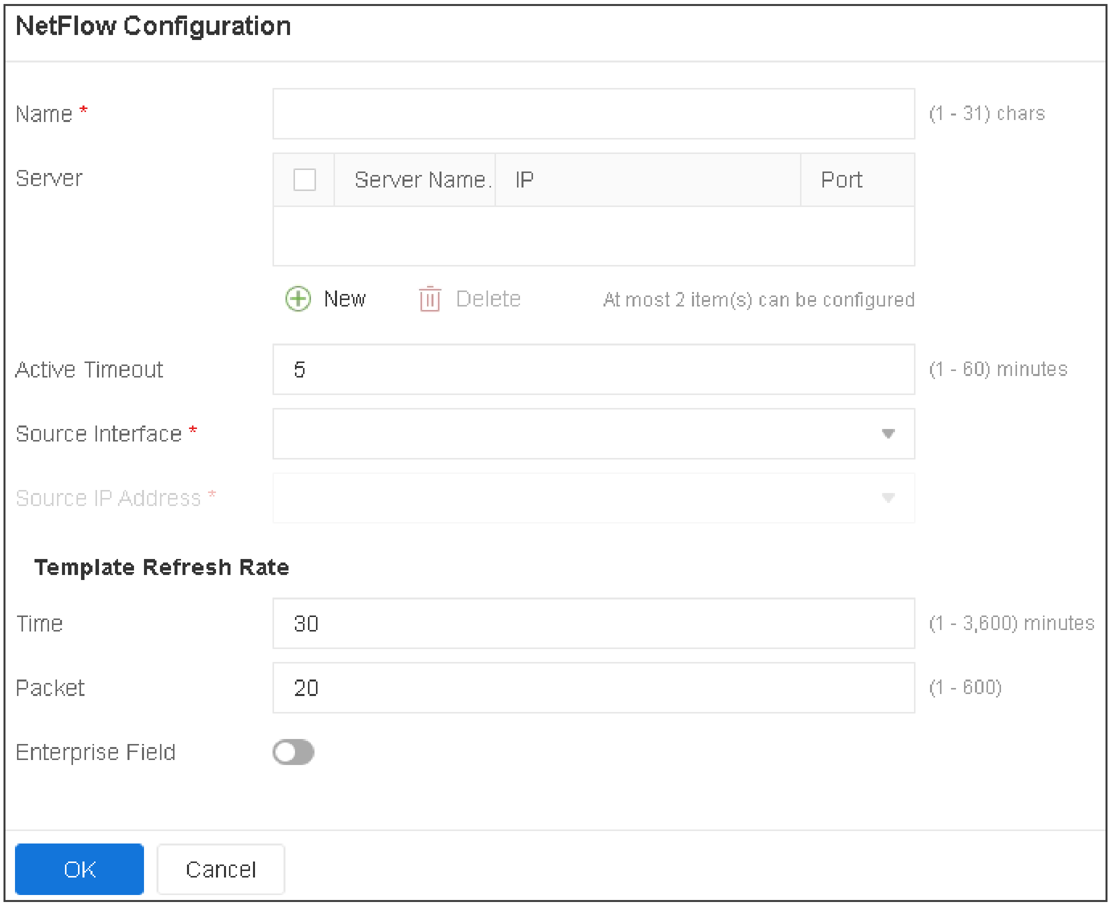
3. Bind the NetFlow rule to an interface. Click **Network > Interface**. Select the interface you want to bind or click **New** to create a new interface. In the Interface Configuration dialog box, select the **Basic** tab and then select a NetFlow rule from the **NetFlow configuration** drop-down list.

Configuring a NetFlow Rule

To configure the NetFlow rule, take the following steps:

1. Click **Object > NetFlow > Profile**.

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



NetFlow Configuration

Name * (1 - 31) chars

Server

☐	Server Name	IP	Port

At most 2 item(s) can be configured

Active Timeout: 5 (1 - 60) minutes

Source Interface *

Source IP Address *

Template Refresh Rate

Time: 30 (1 - 3,600) minutes

Packet: 20 (1 - 600)

Enterprise Field

In the NetFlow Configuration dialog box, configure the following options

Option	Description
Name	Enter the name of the NetFlow rule.
Server	To configure the NetFlow server, take the following steps: 1. Type the server name, IP address and port number into the **Server Name**, **IP** and **Port** box respectively. 2. Click **New** to add a NetFlow server which will be

Option	Description
	displayed in the list below. 3. Repeat the above steps to add more servers. You can add up to 2 servers. To delete a server, select the server check box you want to delete from the list and click **Delete**.
Active Timeout	The active timeout value is the time after which the device will send the collected NetFlow traffic information to the specified server once. Type the active timeout value into the **Active Timeout** box. The range is 1 to 60 minutes. The default value is 5 minutes.
Source Interface	Select the source interface for sending NetFlow traffic information in the **Source Interface** drop-down list.
Source IP Address	After specifying the source interface, the system will automatically acquire and display the management IP address or the secondary IP address of the source interface in the drop-down list.
Template Refresh Rate	You can configure the NetFlow template refresh rate by time or number of packets, after which system will refreshes the NetFlow rule. • Time: Specifies the time after which system refreshes the NetFlow rule. The range is 1 to 3600 minutes. The default value is 30 minutes. • Packets: Specifies the number of packets. When

Option	Description
	the number of NetFlow packets exceeds the specified value, system will refreshes the NetFlow rule. The range is 1 to 600. The default value is 20.
Enterprise Field	Select the **Enterprise Field** check box, and the collected NetFlow traffic information will contain enterprise field information.

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

NetFlow Global Configurations

To configure the NetFlow global configurations, take the following steps:

1. Select **Object > NetFlow > Configuration**.

2. Select the **Open NetFlow** check box of NetFlow to enable the NetFlow function. Clear the check box to disable the NetFlow function. The NetFlow function will take effect after rebooting.

End Point Protection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The endpoint security control center is used to monitor the security status of each access endpoint and the system information of the endpoint.

When the end point protection function is enabled, the device can obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.

Notes:

- At present, end point protection function only supports linkage with "JIANGMIN" endpoint security control center.
- End point protection is controlled by license. To use end point protection, apply and install the EPP license.

Related Topics:

- "Configuring End Point Protection" on Page 748
- "Configuring End Point Security Control Center Parameters" on Page 753
- "End Point Monitor" on Page 1030
- "EPP Log" on Page 1110

Configuring End Point Protection

This chapter includes the following sections:

- Preparation for configuring end point protection function.
- Configuring end point protection function.

Preparing

Before enabling end point protection, make the following preparations:

1. Make sure your system version supports end point protection.
2. Import an EPP license and reboot.

Configuring End Point Protection Function

The end point protection configurations are based on security zones or policies.

To realize the zone-based end point protection, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 74.
2. In the **Zone Configuration**page, select **End Point Protection** tab.
3. Enable the end point protection you need and select an end point protection rule from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list. To create an endpoint protection rule, see Configuring End Point Protection Rule.
4. Click **OK** to save the settings.

To realize the policy-based endpoint protection, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 768.
2. In the Policy Configuration page, expand Protection.

3. Select the **Enable** check box of **End Point Protection**. Then select an endpoint protection rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an end point protection rule. For more information, see Configuring End Point Protection Rule.

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

Notes: When the zone and policy bind the same end point protection rule, the priority is policy > zone.

Configuring End Point Protection Rule

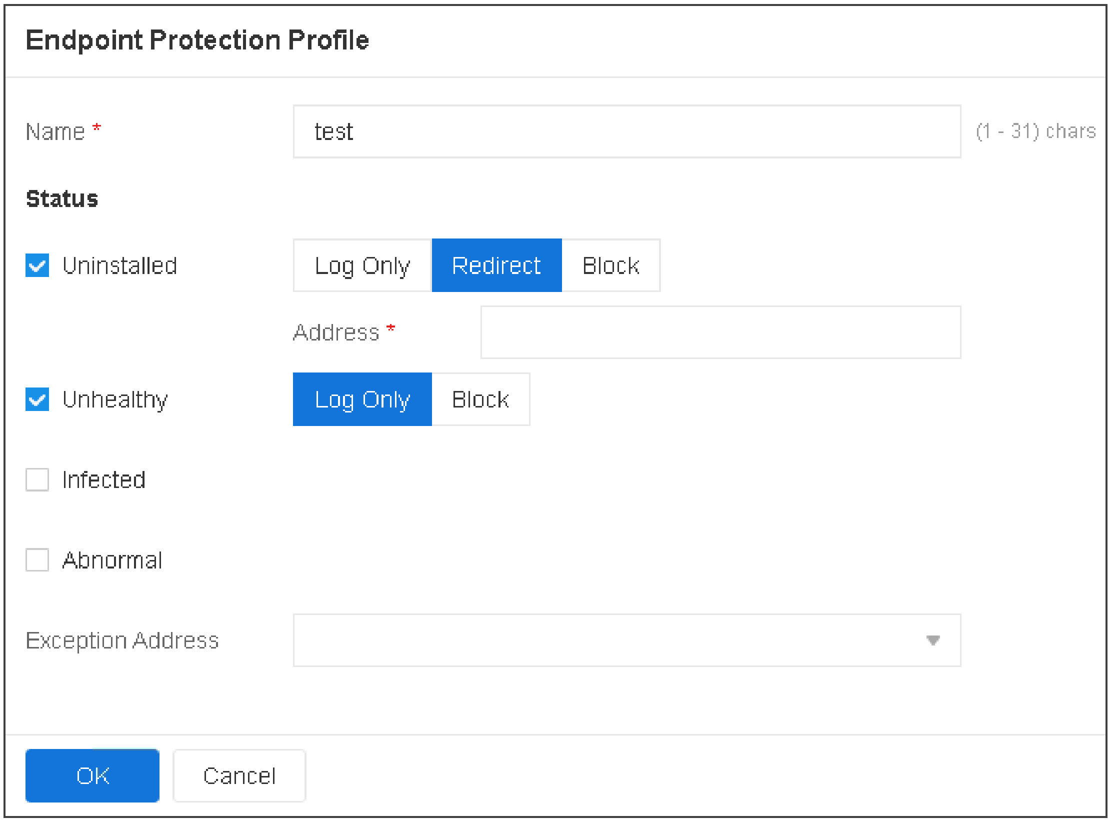
System has two default end point protection rules: **predef_epp** and **no_epp**.

- **predef_epp**: Execute the **Logonly** action for the endpoint whose status is "Uninstall" and "Unhealthy". Execute the **Block** action for the endpoint whose status is "Infected" and "Abnormal", and the block time is 60s.
- **no_epp**:No protective action is executed on all endpoints by default.

To configure an end point protection rule, take the following steps:

1. Click **Object**> **End Point Protection** > **Profile**.

2. Click **New**.



Endpoint Protection Profile

Name * test (1 - 31) chars

Status

☑ Uninstalled Log Only [✓ Redirect] Block

Address *

☑ Unhealthy [✓ Log Only] Block

□ Infected

□ Abnormal

Exception Address

In End Point Protection Rule page, enter the end point protection rule configurations.

Option	Description
Name	Specifies the rule name.
Status	Specifies the protection action corresponding to the end-point status. • Uninstalled: Specifies the protection action for the endpoint which doesn' t install an anti-virus client. Select the **Uninstalled** check box, and select the protection action in the drop-down list.

Option	Description
	- Redirect - Redirects the endpoint to the specified URL. Enter the URL in the **Address** text box. - Logonly - System will pass traffic and record logs only. - Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. • Unhealthy: Specifies the protection action for the unhealthy endpoint. Select the **Unhealthy** check box, and select the protection action in the drop-down list. - Logonly - System will pass traffic and record logs only. - Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. • Infected: Specifies the protection action for the infected endpoint. Select the **Infected** check box, and select the protection action in the drop-down list. - Logonly - System will pass traffic and record

Option	Description
	logs only. - Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. - Abnormal: Specifies the protection action for the abnormal endpoint. Select the **Abnormal** check box, and select the protection action in the drop-down list. - Logonly - System will pass traffic and record logs only. - Block - Block the endpoint connection, and specifies the block time in the **Block time** text box.
Exception Address	The exception address is not controlled by the end point protection rule. Select the address book name in the drop down list. **Notes:** Before selecting the exception address, you need to add the exception endpoint address to the address book. For configuration, see "Address" on Page 537.

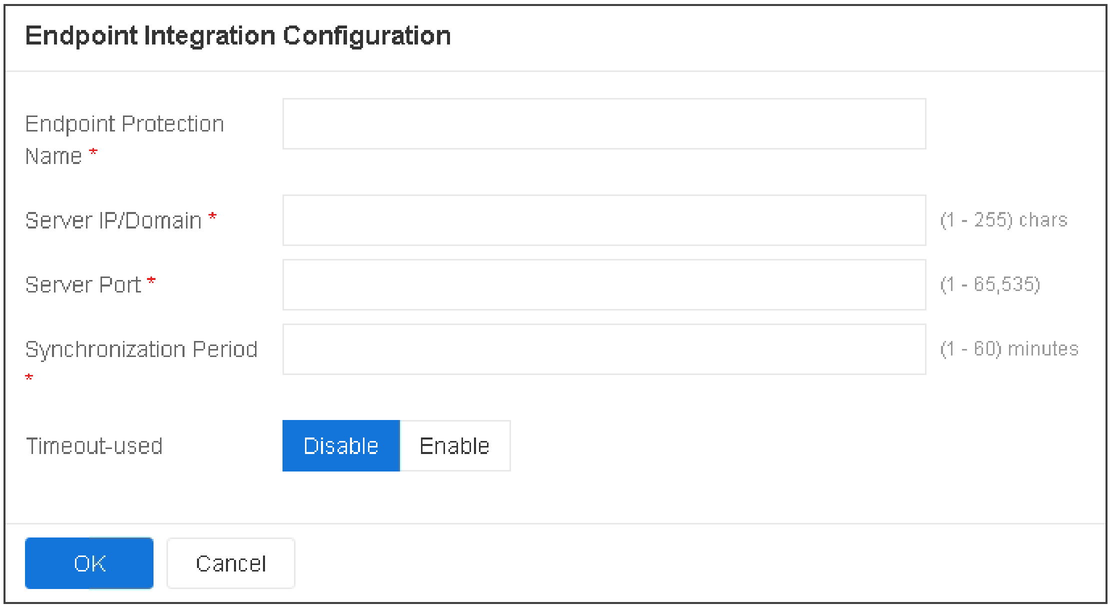
3. Click **OK** to save the settings.

Configuring End Point Security Control Center Parameters

To configure the endpoint security control center parameters, take the following steps:

1. Go to **System > Third Party Linkage**.

2. Click **New**.



Endpoint Integration Configuration

Endpoint Protection Name *		
Server IP/Domain *		(1 - 255) chars
Server Port *		(1 - 65,535)
Synchronization Period *		(1 - 60) minutes
Timeout-used	[✓ Disable] Enable	

In the End Point Linkage Configuration page, enter values.

Option	Description
Endpoint Prevention Name	Display the end point protection type as Jiangmin. Only one endpoint security control center server with the same type can be configured.
Server IP/Domain	Specifies the address or domain name of the endpoint security control center server. The range is 1 to 255 characters.
Server Port	Specifies the port of the endpoint security control center server. The range is 1 to 65535.
Synchronization Period	Specifies the synchronization period of endpoint data information. The range is 1 to 60 minutes. The default value is 10 minutes.
Timeout-used	• Disable: When the endpoint security control center is disconnected with the device and doesn't restore to connection in two synchronization periods, the synchronized endpoint data information will be cleared. By default, the timeout entry is disabled. • Enable: When the endpoint security control center is disconnected with the device and doesn't restore to connection in two synchronization periods, the endpoint data information that the system has been synchronized the last time continues to be used.

3. Click **OK**.

ACL

System supports ACL (Access Control List) based on MAC addresses. You can create access control profile based on MAC addresses and bind the profile to security policies to achieve access control of the specific MAC addresses. With the combination of security policy and ACL rules, system can achieve accurate access controlling.

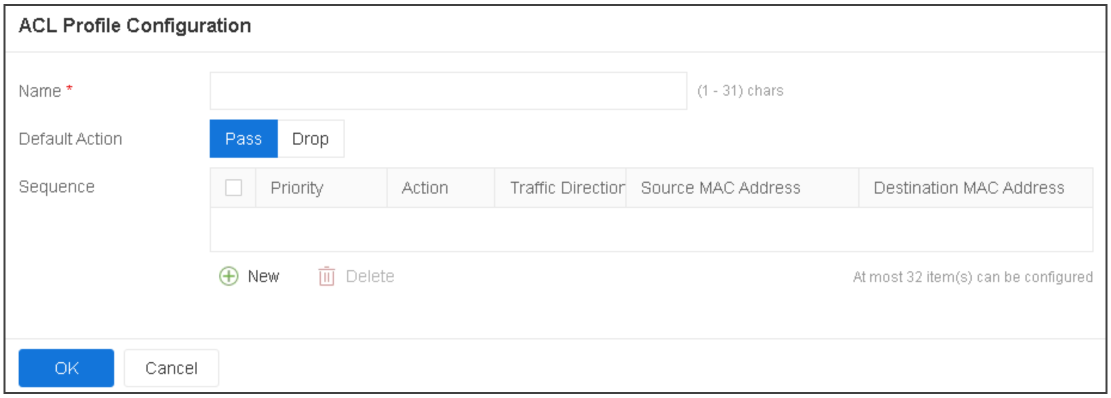
ACL Profile

The ACL profile consists of one or more access control rules. In the access rule, you can set the source MAC address and destination MAC address to filter the packets flowing through the device, and set access control action for the matched packets, pass or discard. The configured access control profiles will take effect only when they are bound to security policies.

To configure an ACL profile, take the following steps:

1. Select **Object** > **ACL** > **Profile**.

2. Click **New** and the ACL Profile Configuration dialog box will appear.

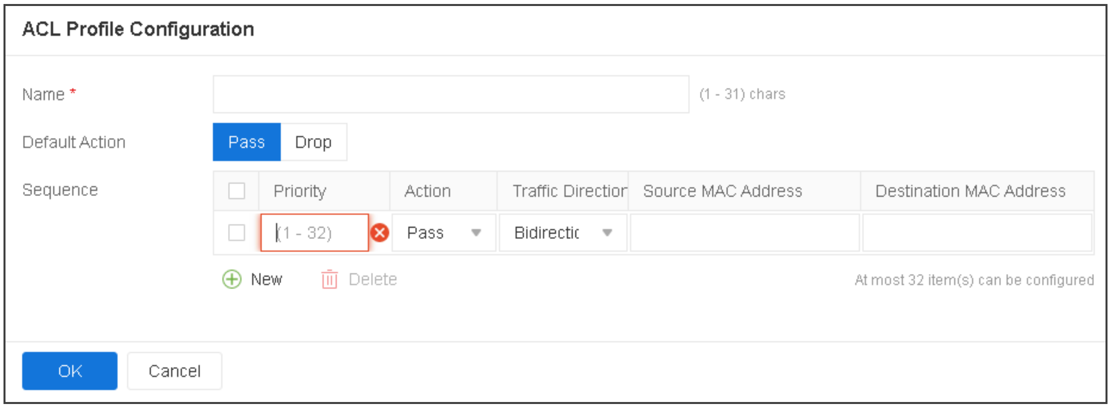


In the ACL Profile Configuration dialog, configure the corresponding options.

Option	Description
Name	Specify the name of the ACL profile.

Option	Description
Default Action	Specify the default action of access control. For the packets which match the access control rule in the list below, it will be processed according to the action set in the access control rule; for the packets which fail to match the access control rule, it will be processed according to the default action set here. Default control actions include: • Pass: By default, packets will be allowed to pass the detection of access control, but still need to be detected via IPS, Anti-virus and so on. • Block: By default, packets will be blocked directly and will not pass through the device.

3. Click New on the ACL Profile Configuration, and the ACL Rule Configuration dialog pops up.



ACL Profile Configuration

Name * (1 - 31) chars

Default Action: Pass | Drop

Sequence

□	Priority	Action	Traffic Directior	Source MAC Address	Destination MAC Address
□	(1 - 32)	Pass	Bidirectic		

In the <ACL Rule Configuration> dialog, configure the corresponding options.

Option	Description
Priority	Specify the priority of ACL rules to be matched, ranging from 1 to 32. The bigger the value, the higher the priority.
Action	Specify the action to be executed after the ACL rules have been matched, including: • Pass: Packets will be allowed to pass the detection of access control, but still need to be detected via IPS, Anti-virus and so on. • Block: Packets will be blocked directly and will not pass through the device.
Traffic Direction	Specify the traffic direction of the ACL rule. **Forward** indicates the traffic direction where the session is initiated. **Backward** indicates traffic direction where the session is responded. **Bidirectional** indicates the direction of both Forward and Backward. By default, system matches the bidirectional traffic.
Source MAC Address	Specify the source MAC address of packets to be matched.
Destination MAC Address	Specify the destination MAC address of packets to be matched.

4. Click **OK**.

IoT Policy

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

IoT, the abbreviation of Internet of Things, is the extension of Internet connectivity into physical devices and everyday objects.

The IoT policy in system can identify the network video monitoring devices, like IPC (IP Camera) and NVR (Network Video Recorder) via the flowing traffic, then monitor the identified devices and block illegal behaviors according to the configurations.

Notes:

- Only the IPC and NVR devices of Hikvision, Dahua and Uniview are supported currently.
- Only the network video monitoring devices are installed with the IoT licenses can the IoT policy be used.
- The network video monitoring devices in the NAT scenario cannot be identified with the IoT policy.

Links:

- Configuring IoT Policy
- Configuring Admittance List
- IoT Monitor
- IoT Log

Configuring IoT Policy

The chapter introduces the following topics:

- Preparations for IoT Policy Configuration
- Configuring IoT Policy

Preparations for IoT Policy Configuration

Before configuring the IoT policy, ensure the following conditions have been met.

1. The IoT Policy function is supported for the system version.
2. The IoT license has been installed and you log in to the device again.

Configuring IoT Policy

System supports the configuration of IoT policy based on the zone.

To configure the IoT policy based on the zone, take the following steps:

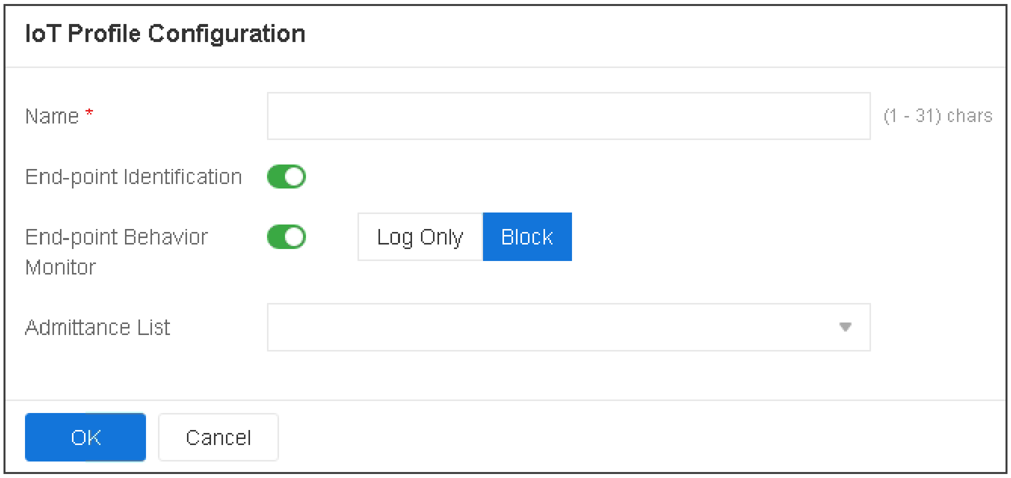
1. For how to create or edit the zone, refer to Zone.
2. In the **Zone Configuration** dialog, click the **IoT Monitor** tab.
3. Select the **Enable** check box. You can select a configured IoT profile from the **Profile** drop-down list, or click **Add Profile** in the drop-down list to create an IoT profile. For how to configure the IoT policy profile, refer to Configuring IoT Profile.
4. Click **OK** to save the configurations.

Configuring IoT Profile

To create an IoT profile, take the following steps:

1. Click **Object** > **IoT Policy** > **Profile**.

2. Click **New** and the **IoT Profile Configuration** dialog pops up.



IoT Profile Configuration

Name * (1 - 31) chars

End-point Identification

End-point Behavior Monitor

Admittance List

In the dialog, configure the options as follows:

Option	Description
Name	Specify the name of the IoT profile.
End-point Identification	Select the **Open** check box to enable the end-point identification. When the function is enabled, system will probe the end-point IP in the IoT monitoring list actively, and identify the information of manufacturer and model of the network video monitoring devices according to the returned packets. Then the information will be displayed in the IoT monitoring list. The end-point identification will be triggered • when a new end-point IP adds into the IoT monitoring list. • when the network video monitoring device logs in

Option	Description
	again. - when the network video monitoring device has been online, and the function will be triggered every 5 minutes.
End-point Behavior Monitor	Select the **Open** check box to enable the end-point behavior monitoring. When the function is enabled, system can check whether the devices behaviors are illegal. If illegal behaviors are detected, you can execute the following operation: - Log Only: System will let the traffic flowing through the end-point device pass and record logs. - Block: System will block the traffic flowing through the end-point device.
Admittance List	You can select a configured admittance list profile from the drop-down list, or click **Add Profile** in the drop-down list to Configure Admittance List.

3. Click **OK** to save the configurations.

Notes: To ensure the normal performance of IoT policy, the network video monitoring devices should:

- enable ONVIF service and multi-cast detection function.
- communicate with the Hillstone devices.

Configuring Admittance List

For the traffic flowing through the zone bound with the IoT policy profile, systems supports to control it by configuring the admittance list of the IP, MAC and IP/MAC types, that is, only the traffic matches the type in the admittance list is allowed to pass. By default, all the traffic flowing through the zone bound with the IoT policy profile is allowed to pass.

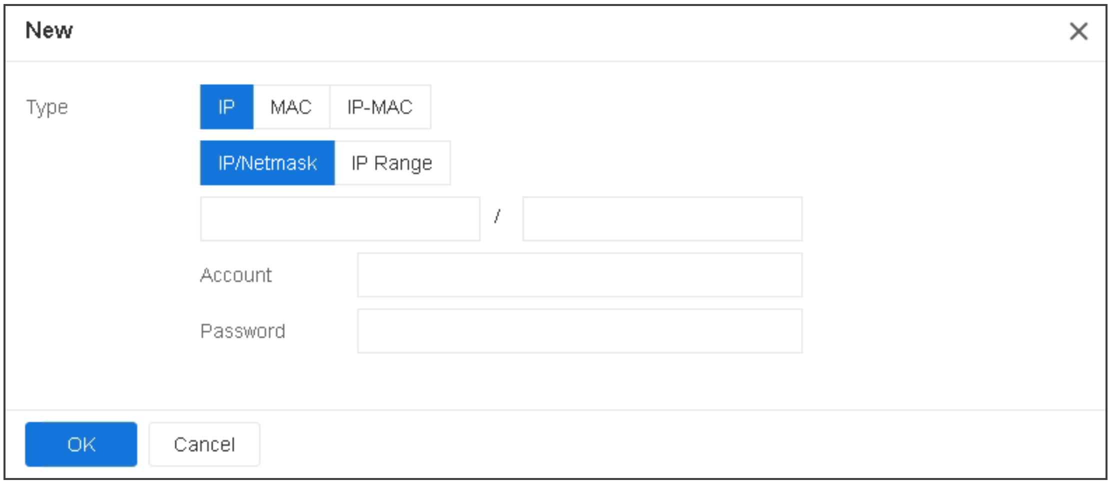
When the admittance lists of the IP/MAC, IP and MAC types are all configured, traffic matches the admittance lists in the sequence of IP/MAC > IP > MAC. Traffic can pass in the following conditions.

- Traffic first matches the admittance list of IP/MAC type, and both the IP and MAC types are matched.
- Traffic first matches the admittance list of IP/MAC type, while only the IP type is matched. Then traffic tries to match the admittance list of IP and MAC type in order, and both the IP and MAC types are matched.

You can configure the admittance list with the following methods:

Creating Admittance List Profile

1. Click **Object** > **IoT Policy** > **Admittance List**.
2. Click **New**, and the **Admittance List Configuration** dialog pops up. Enter the name of the admittance list into the **Name** text box. Click **Add** and the **Add** dialog pops up.



Configure the options as follows:

Option	Description
Mode	Specify the type of the admittance list, including IP, MAC and IP-MAC. Note: When the network video monitoring devices and the Hillstone devices are not in the same broadcast domain, the obtained MAC address in the packets may not be true. Then the network video monitoring devices cannot match the admittance list. Therefore, you're suggested to configure the admittance list of IP type.
IP	Specify the type of admittance list as IP and configure the following items: • IP/Netmask: Enter the IP address and netmask. • IP Range: Enter the start IP and end IP address. • Account (Optional): Enter the admin name of the

Option	Description
	network video monitoring device. • Password (Optional): Enter the password of the account.
MAC	Specify the type of admittance list as MAC and configure the MAC address of the network video monitoring device.
IP-MAC	Specify the type of admittance list as IP/MAC and configure the following items: • IP: Enter the IP address into the text box. • MAC: Enter the MAC address into the text box. • Account (Optional): Enter the admin name of the network video monitoring device. • Password (Optional): Enter the password of the account.

3. Click **Add** to save the configurations.

Notes: The admittance list of the specified type in one profile cannot be repeated, otherwise, an error will pop up. The repeat conditions for different types include:

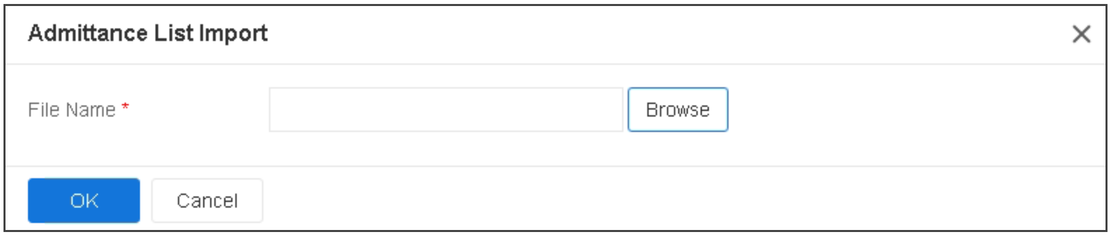
- IP-MAC: The IP address and MAC address are the same.
- IP: There're repeated IP addresses in the IP/netmask or IP range.
- MAC: The MAC addresses are repeated.

Importing Admittance List

1. Click **Object** > **IoT Policy** > **Admittance List**.

2. (Optional) Click **Admittance List Template** and download the template in local.

3. Select an admittance list and click **Import**.



Admittance List Import

File Name *

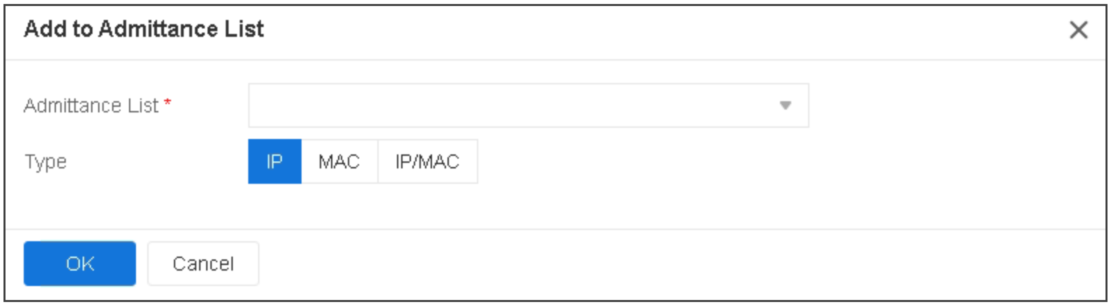
4. In the **Admittance List Import** dialog, click **Browse** and upload the admittance list in the local.

5. Click **OK**.

Adding to Admittance List

1. Click **Monitor** > **IoT Monitor** > **Details**.

2. Select the check box and click **Add to Admittance List**.



Add to Admittance List

Admittance List *

Type: IP

In the pop-up dialog, configure the options as follows.

Option	Description
Admittance List	Select the admittance list profile from the drop-down list that the selected item will be added to.
Type	Specify the type of the selected item that will be added as IP, MAC or IP/MAC.

3. Click **OK** to save the configurations.

Chapter 10 Policy

The Policy module provides the following functions:

- Security policy: Security policy the basic function of devices that are designed to control the traffic forwarding between security zones/segments. By default all traffic between security zones/segments will be denied.
- NAT: When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets.
- QoS: QoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. QoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.
- Session limit: The session limit function limits the number of sessions and controls the session rate to the source IP address, destination IP address, specified IP address, service, or role/user/user group, thereby protecting from DoS attacks and control the bandwidth of applications, such as IM or P2P.
- Internet behavior control: The Internet behavior control allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs and content logs) on user network behavior.
- Global blacklist: After adding the IP addresses or services to the global blacklist, system will perform the block action to the IP address and service until the block duration ends.

Security Policy

Security policy is the basic function of devices that is designed to control the traffic forwarding between security zones/segments. Without security policy rules, the devices will deny all traffic between security zones/segments by default. After configuring the security policy rule, the device can identify what traffic between security zones or segments will be permitted, and the others will be denied.

The basic elements of policy rules:

- The source zone and address of the traffic
- The destination zone and address of the traffic
- The service type of the traffic
- Actions that the devices will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server.

Generally a security policy rule consists of two parts: filtering conditions and actions. You can set the filtering conditions by specifying traffic's source zone/address, destination zone/address, service type, and user. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in system are arranged in a specific order. When traffic flows into a device, the device will query for policy rules by turn, and processes the traffic according to the first matched rule.

The max global security policy rule numbers may vary in different models.

Security policy supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the policy rule.

This section contains the following contents:

- Configure a security policy rule

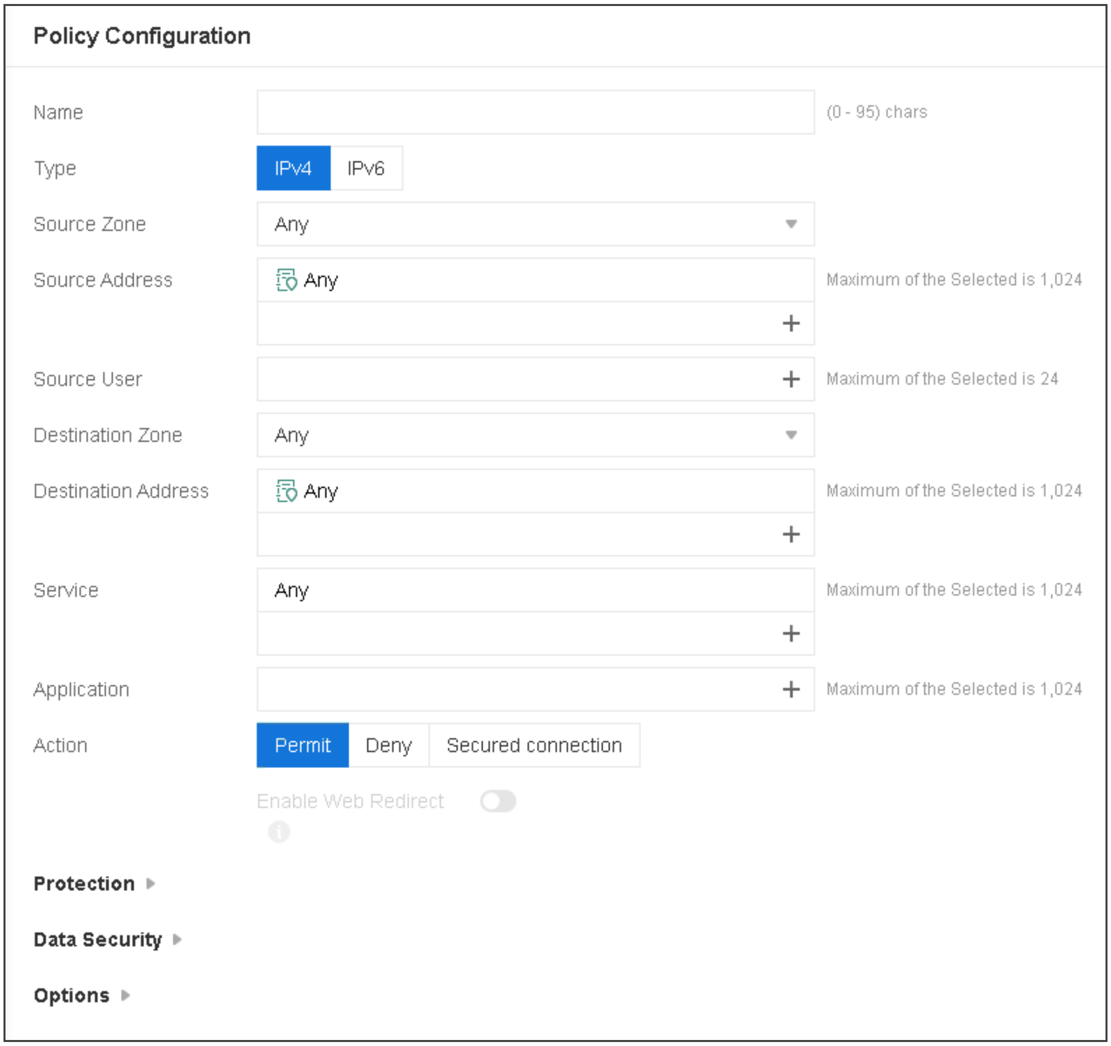
- Manage the security policy rules: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check, and rule redundancy check.
- Configure a security policy group
- View and search the security policy rules/ security policy groups
- Configure the policy assistant

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.



Policy Configuration

Name (0 - 95) chars

Type: IPv4 | IPv6

Source Zone: Any

Source Address: Any — Maximum of the Selected is 1,024

Source User — Maximum of the Selected is 24

Destination Zone: Any

Destination Address: Any — Maximum of the Selected is 1,024

Service: Any — Maximum of the Selected is 1,024

Application — Maximum of the Selected is 1,024

Action: Permit | Deny | Secured connection

Enable Web Redirect

Protection ▸

Data Security ▸

Options ▸

Configure the corresponding options.

Option	Description
Name	Type the name of the security policy.
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 address-book should be configured in the IPv6 format.

Option	Description
Source Information	
Zone	Specifies a source zone.
Address	Specifies the source addresses. 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 ⊕ icon to create a new address entry. - The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
User	Specifies a role, user or user group for the security policy rule. 1. From the **User** drop-down menu, select the AAA server where the users and user groups reside. To specify a role, select **Role** from the

Option	Description
	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.
Destination	
Zone	Specifies a destination zone.
Address	Specifies the destination addresses. 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:

Option	Description
	• When selecting the **Address Book** type, you can click ⊕ icon to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
Other Information	
Service	Specifies a service or service group. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 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 **User-defined** from the **Predefined** drop-down menu, and click ⊕ icon. • The default service configuration is any. To

Option	Description
	restore the configuration to this default one, select the **any** check box. 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 options include TCP, UDP, ICMP 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:

Option	Description
	• 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. **Notes:** • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional.

Option	Description
	• 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, the default value is

Option	Description
	: 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）, 100 （Private experimentation）, 101 （Private experimentation）, 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 Advert-

Option	Description
	isement）, 135（Neighbor Solicitation）, 136（Neighbor 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

Option	Description
	• 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. **ALL**: • Protocol: Specifies a protocol name for the service rule. If it is a unknown protocol, you can directly 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

Option	Description
	filters. 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 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: • 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.
Action	
Action	Specifies an action for the traffic that is matched to the

Option	Description
	policy rule, including: • Permit - Select **Permit** to permit the traffic to pass through. • Deny - Select **Deny** to deny the traffic. • 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 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. • Portal server - Performs portal authentication on

Option	Description
	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 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" on Page 824.

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 and IPS profile enables the devices to implement fine-grained application layer policy control.
URL Fil-	Specifies a URL filter profile. The combination of security

Option	Description
tering	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.
Content Filter	• 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

Option	Description
	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. • HTTP/FTP Control: Specifies a HTTP/FTP control profile. The combination of security policy rule and HTTP/FTP 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** drop-down list. 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.
Log	You can log policy rule matching in the system logs according to your needs.

Option	Description
	• 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. • 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 expect-

Option	Description
	ations 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 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.

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

Managing Security Policy Rules

Managing security policy rules include the following matters: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check, and rule redundancy check.

Enabling/Disabling a Policy Rule

By default the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Select the security policy rule that you want to enable/disable.
3. Click ⋮ icon , and then select **Enable** or **Disable** to enable or disable the rule.

The disabled rule will not display in the list. Click ⋮ icon , and then select **Show Disabled Policies** to show them.

Cloning a Policy Rule

When there are a large number of policy rules in system, to create a policy rule which is similar to an configured policy rule easily, you can copy the policy rule and paste it to the specified location.

To clone a policy rule, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Select the security policy rule that you want to clone and click **Copy**.
3. Click **Paste**. In the drop-down list, select the desired position. Then the rule will be cloned to the desired position.

Adjusting Security Policy Rule Position

To adjust the rule position, take the following steps:

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.

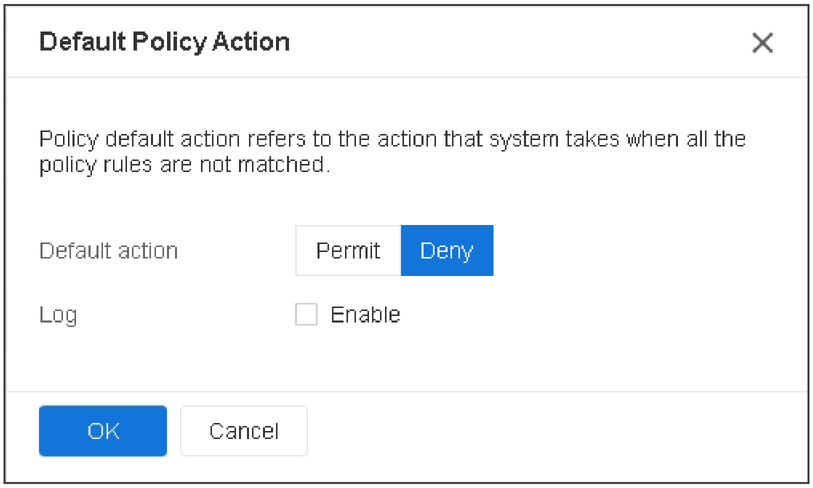
Configuring Default Action

You can specify a default action for the traffic that is not matched with any configured policy rule. System will process the traffic according to the specified default action. By default system will deny such traffic.

To specify a default policy action, take the following steps:

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

2. Click ⋮ icon and select **Default Policy Action**.



Default Policy Action

Policy default action refers to the action that system takes when all the policy rules are not matched.

Default action: Permit [✓ Deny]

Log: □ Enable

Configure the following options.

Option	Description
Default action	Specify a default action for the traffic that is not matched with any configured policy rule. • Click **Permit** to permit the traffic to pass through. • Click **Deny** to deny the traffic.
Log	Configure to generate logs for the traffic that is not matched with any configured policy rule. By default system will not generate logs for such traffic. To enable log, click the **Enable** button, and system will generate logs for such traffic.

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

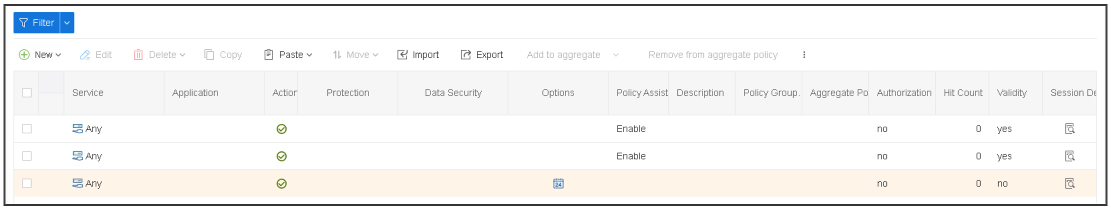
Schedule Validity Check

In order to make sure that the policies based on schedule are effective, system provides a method to check the validity of policies. After checking the policy, the invalid policies based on schedule will be highlighted by yellow.

To check schedule validity:

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

2. Click ⋮ icon and select **Schedule Validity Check**. After check, system will highlight the invalid policy based on schedule by yellow. Meanwhile, you can view the validity status in the policy list.



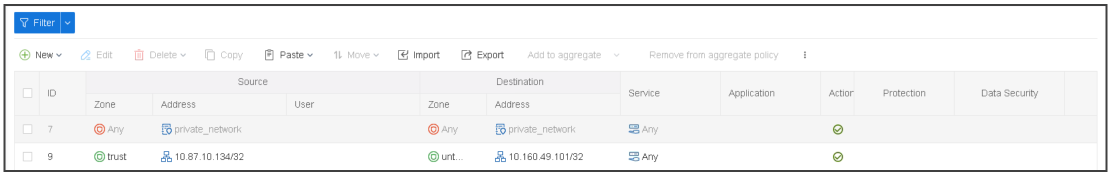
□		Service	Application	Actior	Protection	Data Security	Options	Policy Assist	Description	Policy Group.	Aggregate Po	Authorization	Hit Count	Validity	Session De
□		Any		✓				Enable				no	0	yes	
□		Any		✓				Enable				no	0	yes	
□		Any		✓			24					no	0	no	

Showing Disabled Policies

To show disabled policies:

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

2. Click ⋮ icon and select **Show Disabled Policies**. The disabled policies will be highlighted by gray in the policy list.



□	ID	Source			Destination		Service	Application	Actior	Protection	Data Security
		Zone	Address	User	Zone	Address					
□	7	Any	private_network		Any	private_network	Any		✓		
□	9	trust	10.87.10.134/32		unt...	10.160.49.101/32	Any		✓		

Notes:

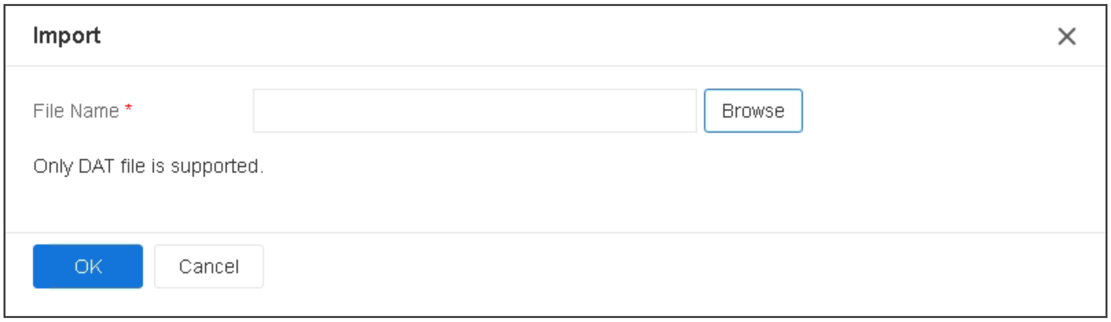
- By default(the "Schedule Validity Check" and "Show Disabled Policies" are not selected), the policy list only displays the enabled policies which are not highlighted.
- When you select both "Schedule Validity Check" and "Show Disabled Policies", the policy is managed as follows:
  - The policy list will display the "Validity" column, which shows the validity status of policies.
  - The invalid policy based on schedule will be highlighted by yellow no matter if the policy is disabled or not.
  - If the valid policy based on schedule is disabled, it will be highlighted by gray.

Importing Policy Rule

You can import the configuration file of the local policy rules into the device to avoid creating policy rules manually. Only the DAT format file is supported currently.

To import the configuration file of policy rules, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Click the **Import** button to open the **Import** page.



Import

File Name *

Only DAT file is supported.

3. Click **Browse** and select the local configuration file of policy rule to upload.
4. Click **OK**, and the imported policy rule will be displayed in the list.

Notes:

- If there's an error during import, system will stop importing immediately and roll back configurations automatically.
- The imported policy will be displayed on the bottom of the policy list.

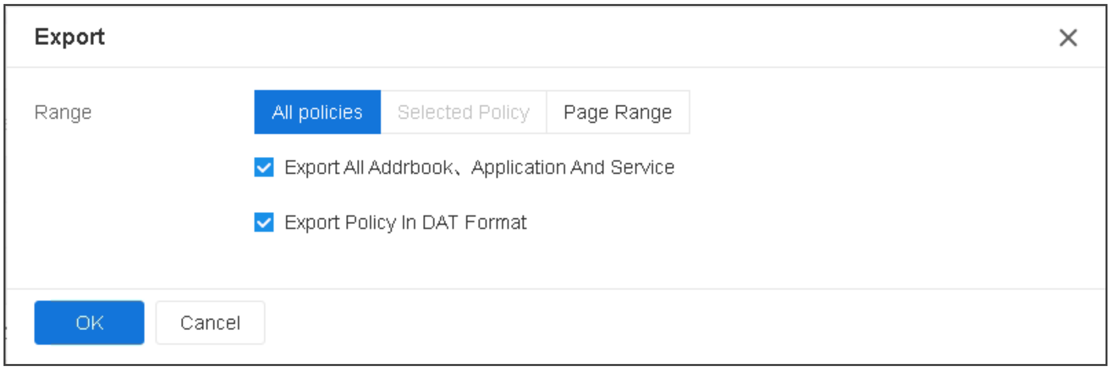
Exporting Policy Rule

You can export the policy rules existing on the device to the local in the format of HTML or DAT formats. At the same time, all the custom objects such as address book, service book and application can be exported.

To export the policy rules, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Click **Export** to open the **Export** page.



Export

Range: [All policies] Selected Policy | Page Range

☑ Export All Addrbook、Application And Service

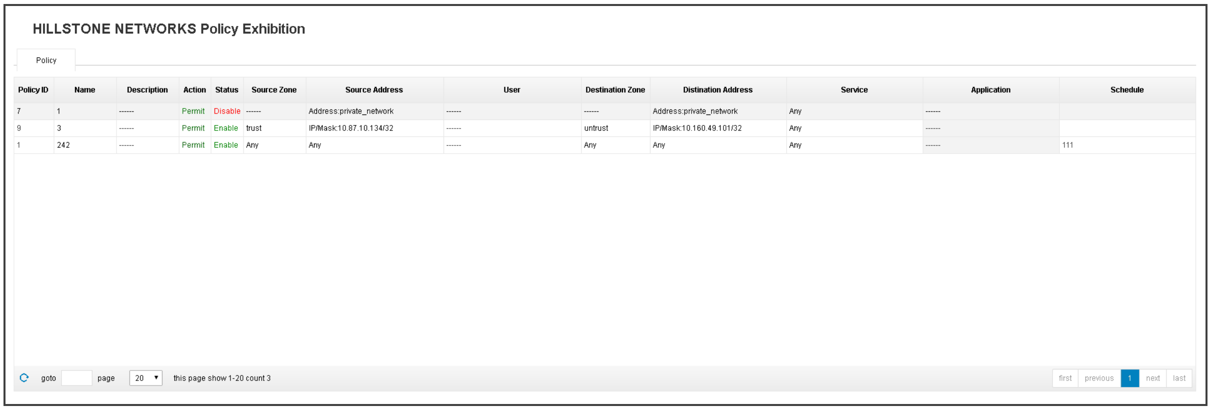
☑ Export Policy In DAT Format

Configure the options as follows:

Option	Description
Range	Specify the range of policy rules to be exported. • All Policy: Select the radio button and export all policy rules on the device. • Selected Policy: In the policy list, select the policy to be exported, and then click **Export** > **Selected Policy**. • Page Range: Select the radio button, and enter the page number or page range of the policy list to be exported. **Note**: Separate the page number or range with semicolons, e.g. "3;5-8".
Export Address, Service, APP Book	Select the check box to export all the custom objects including address book, service book and application book, and a Zip file named "book+-exported time" will be generated.
Export Policy in DAT Format	Select the check box to export the policy configurations in the format of DAT.

3. Click **OK** to download the exported files. There're four kinds of files: policyExport.html, " policy+exported time.zip", "book+exported time.zip" and the policy configurations in the DAT format.

4. Double-click the policyExport.html, click **Import File** and import the " policy+exported time.zip" to view the table of exported policies.

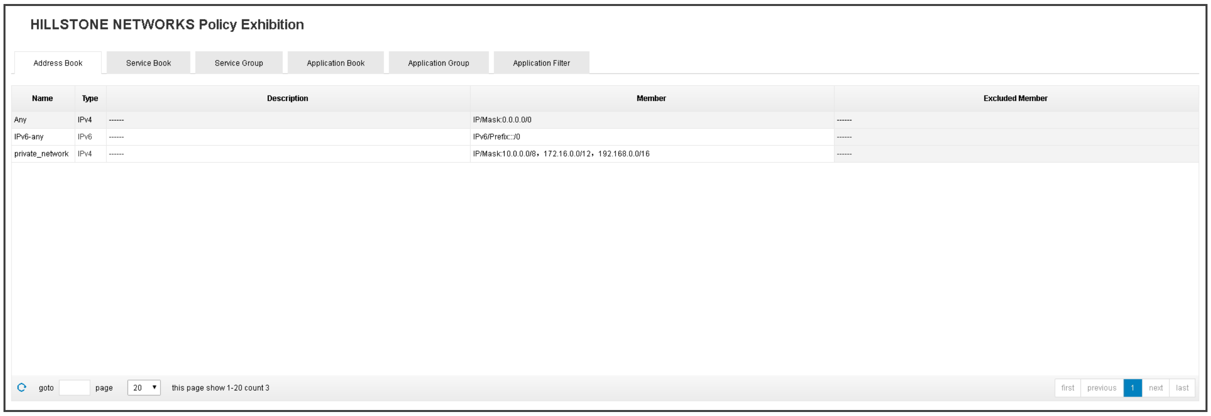


HILLSTONE NETWORKS Policy Exhibition

Policy ID	Name	Description	Action	Status	Source Zone	Source Address	User	Destination Zone	Distination Address	Service	Application	Schedule
7	1	------	Permit	Disable	------	Address:private_network	------	------	Address:private_network	Any	------	
9	3	------	Permit	Enable	trust	IP/Mask:10.87.10.134/32	------	untrust	IP/Mask:10.160.49.101/32	Any	------	
1	242	------	Permit	Enable	Any	Any	------	Any	Any	Any	------	111

this page show 1-20 count 3

5. Double-click the policyExport.html, click **Import File** and import the "book+exported time.zip" to view the table of object configurations.



HILLSTONE NETWORKS Policy Exhibition

Name	Type	Description	Member	Excluded Member
Any	IPv4	------	IP/Mask:0.0.0.0/0	------
IPv6-any	IPv6	------	IPv6/Prefix:::/0	------
private_network	IPv4	------	IP/Mask:10.0.0.0/8，172.16.0.0/12，192.168.0.0/16	------

this page show 1-20 count 3

Configuring an Aggregate Policy

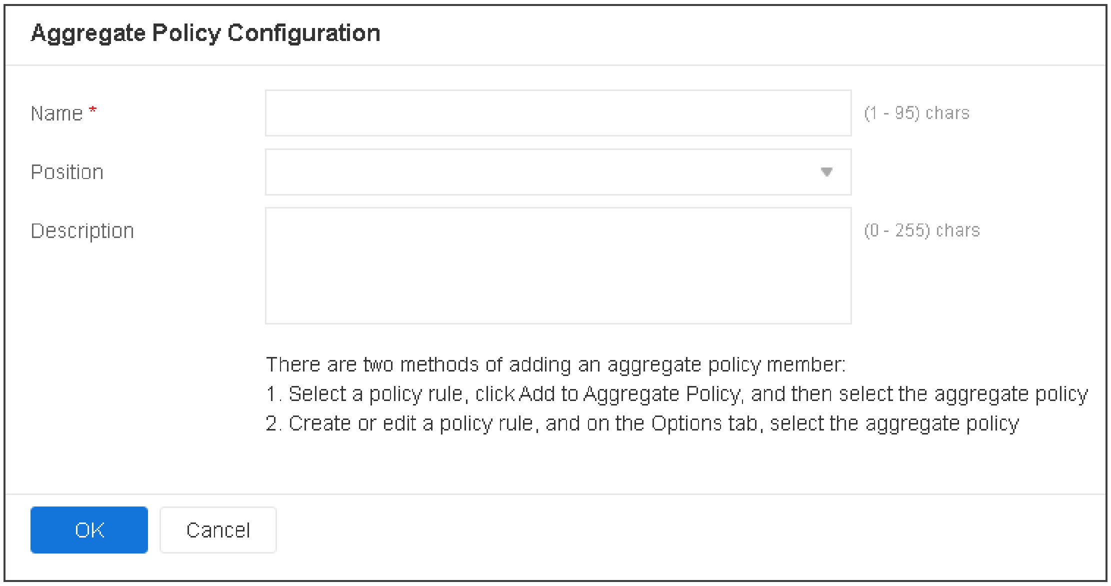
According to the needs of different scenarios, you can create an aggregate policy, and add some policy rules with the same effect or the same attributes to the aggregation policy. If the administrator adjusts the position of an aggregate policy, the positions of all its members will be adjusted accordingly, so as to manage policy rules in bulk.

Configuring an aggregate policy includes: creating an aggregate policy, adding an aggregate policy member, removing an aggregate policy member, deleting an aggregate policy, adjusting the position of an aggregate policy, and enabling/disabling an aggregate policy.

Creating an Aggregate Policy

To create an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Click the **New** drop-down list, and select **Aggregate Policy** to open the **Aggregate Policy Configuration** page .



Aggregate Policy Configuration

Name * (1 - 95) chars

Position

Description (0 - 255) chars

There are two methods of adding an aggregate policy member:
1. Select a policy rule, click Add to Aggregate Policy, and then select the aggregate policy
2. Create or edit a policy rule, and on the Options tab, select the aggregate policy

On the Aggregate Policy Configuration tab, complete the basic configuration information.

Option	Description
Name	Specifies the name of an aggregate policy. The range is 1 to 95 characters.

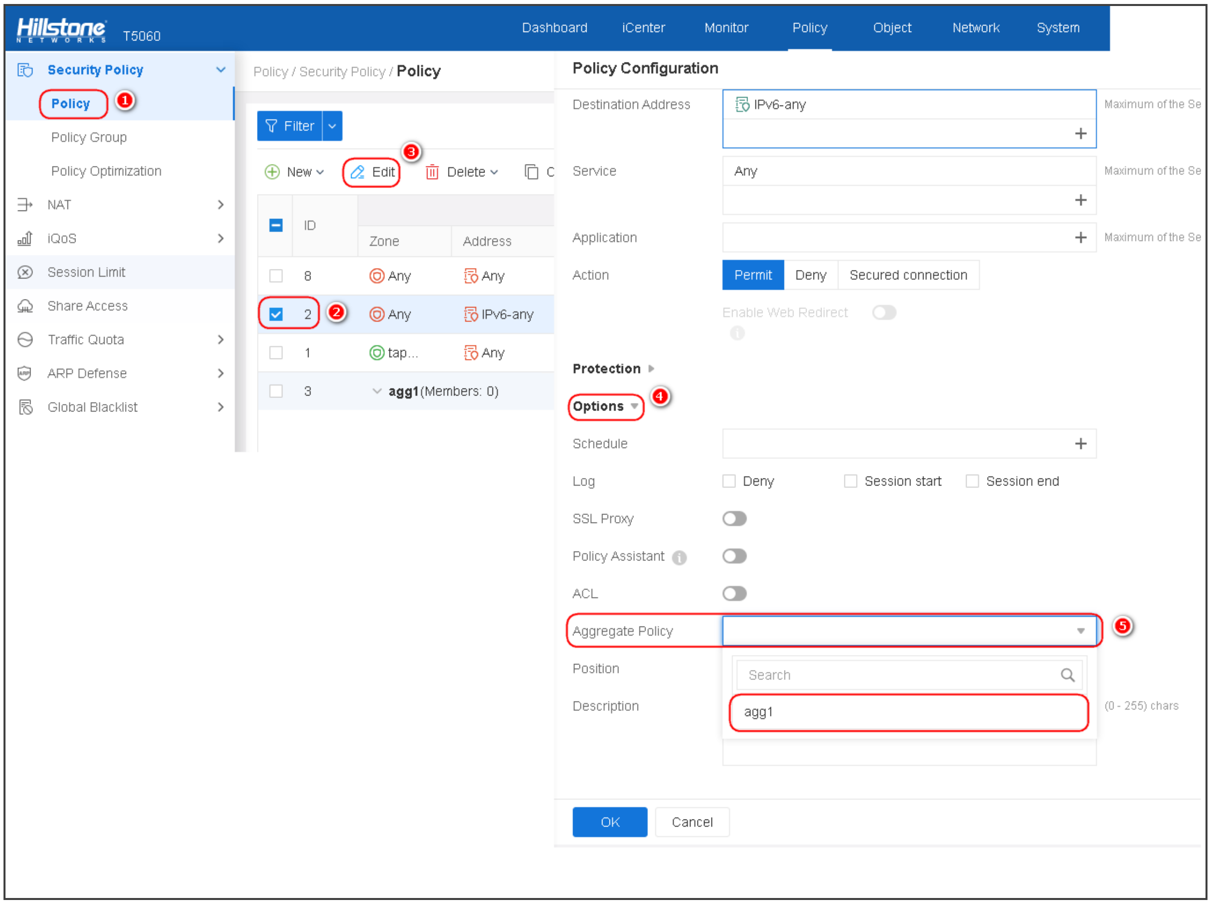
Option	Description
Position	The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. In the **Position** drop-down list, you can select a position for the aggregate policy.
Description	Type descriptions into the **Description** box.

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

Adding an Aggregate Policy Member

After creating an aggregate policy, the administrator can add a policy rule to the aggregate policy to be an aggregate policy member. There are two methods for adding an aggregate policy member.

- **Editing the policy configuration:**



As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Select the policy rule that you want to add to an aggregate policy from the list.

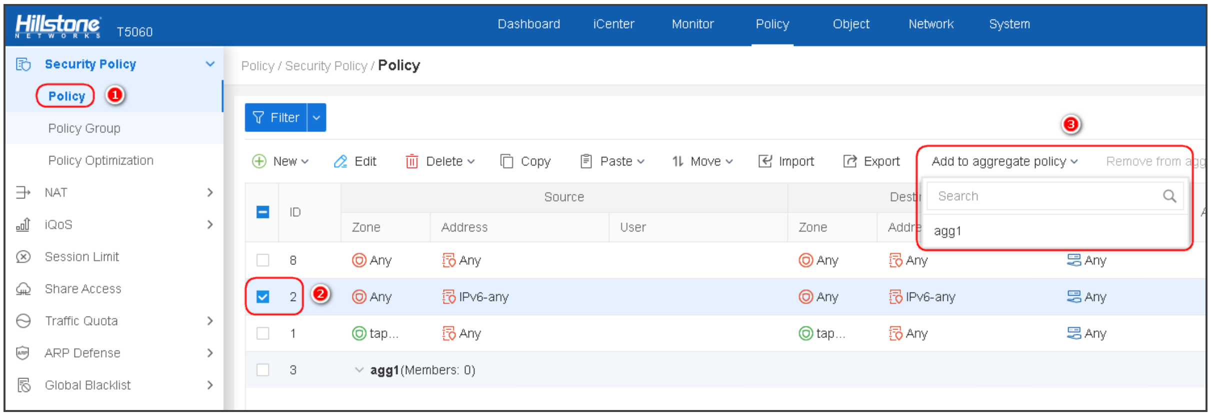
3. Click **Edit** to open the **Policy Configuration** page.

4. Click **Options** to expand the relevant configuration items.

5. 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.

6. Click **OK**.

- **Selecting a policy rule you want to add**:



ID	Source			Desti		
	Zone	Address	User	Zone	Addre	
□ 8	Any	Any		Any	Any	Any
☑ 2	Any	IPv6-any		Any	IPv6-any	Any
□ 1	tap...	Any		tap...	Any	Any
□ 3	agg1(Members: 0)					

As shown above, take the following steps:

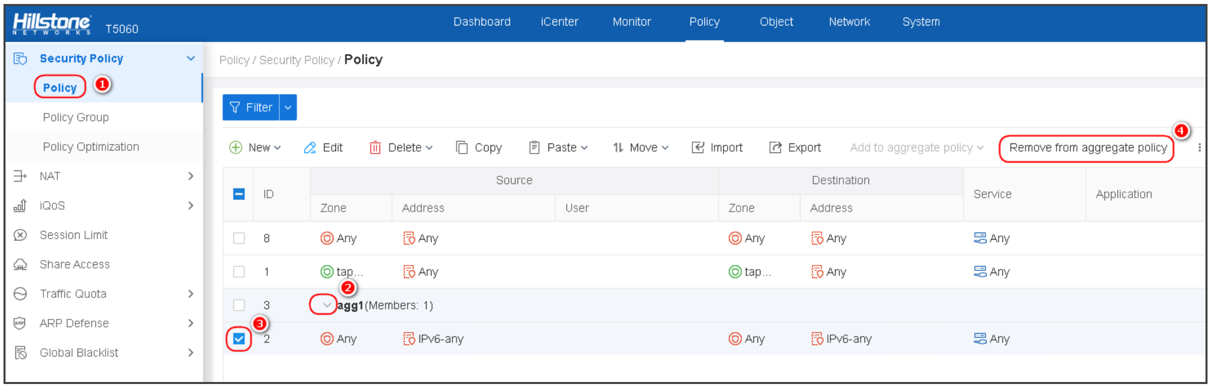
1. Click **Policy** > **Security Policy** > **Policy**.

2. Select the policy rule that you want to add to an aggregate policy from the list. You can select multiple policy rules at a time

3. Click the **Add to aggregate policy** drop-down list, and select the aggregate policy to which you want to add.

Removing an Aggregate Policy Member

To remove a member from an aggregate policy, take the following steps:



ID	Source			Destination		Service	Application
	Zone	Address	User	Zone	Address		
□ 8	Any	Any		Any	Any	Any	
□ 1	tap...	Any		tap...	Any	Any	
□ 3	agg1(Members: 1)						
☑ 2	Any	IPv6-any		Any	IPv6-any	Any	

1. Click **Policy** > **Security Policy** > **Policy**.

2. In the list, click the arrow before an aggregate policy to expand it

3. Select the aggregate policy member that you want to remove. You can select multiple policy rules at a time.

4. Click the **Move out from aggregate policy** button.

Notes:

- If the member at the top position is removed from an aggregate policy, the removed member will be put before the aggregate policy.

- If a member at a non-top position is removed from an aggregate policy, the removed member will be put after the aggregate policy.

- If several aggregate policy members (including the member at the top position) in consecutive order are removed, they will be put before the policy all together.

Deleting an Aggregate Policy

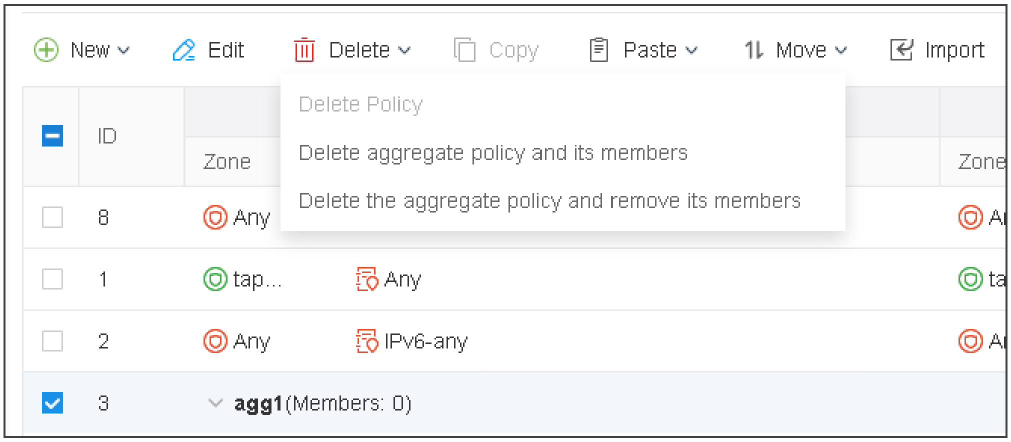
To delete an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Select the aggregate policy that you want to delete from the list.

3. Click **Delete**.

4. Select a deletion method from the drop-down list.


New
Edit
Delete
Copy
Paste
Move
Import
Delete Policy
Delete aggregate policy and its members
Delete the aggregate policy and remove its members

⊟	ID	Zone		Zone
☐	8	Any		A
☐	1	tap...	Any	ta
☐	2	Any	IPv6-any	A
☑	3	**agg1**(Members: 0)		

- Delete aggregate policy and members: When deleting an aggregate policy, the members in it will also be deleted.

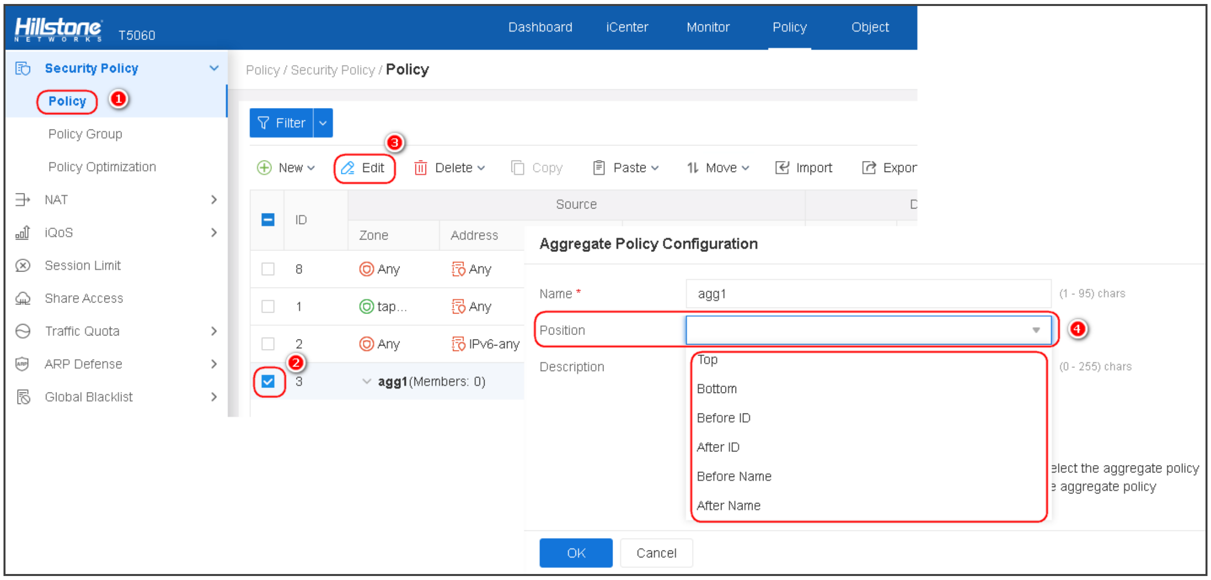
- Delete aggregate policy, unbind members: When deleting an aggregate policy, all members in it will be removed.

5. Click **OK**.

Adjusting Position of an Aggregate Policy

The administrator can adjust the position of an aggregate policy by the following two methods. After the adjustment, the positions of all its members will be adjusted accordingly.

- **Editing the aggregate policy configuration:**



As shown above, take the following steps:

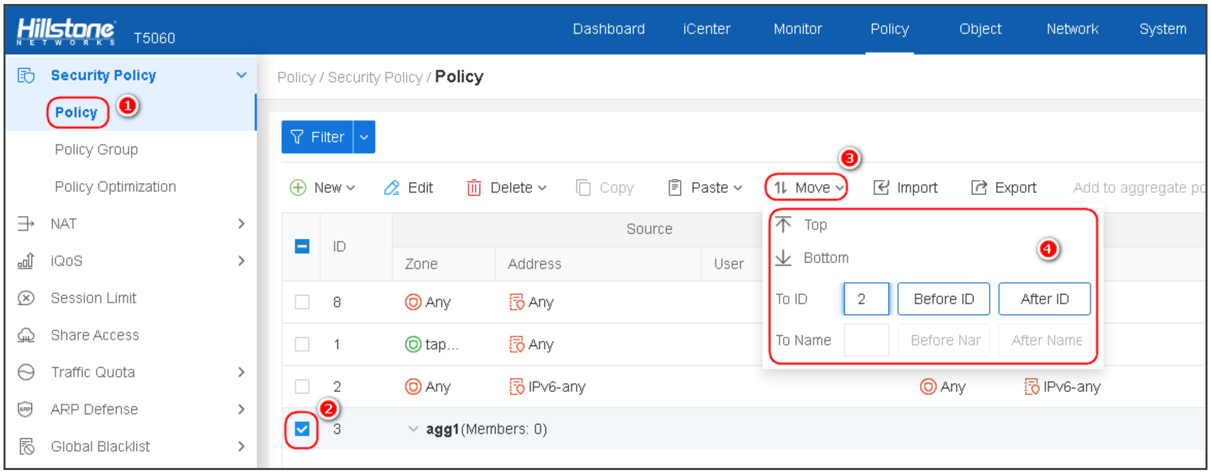
1. Click **Policy** > **Security Policy** > **Policy**.

2. Select the aggregate policy whose position that you want to adjust from the list.

3. Click **Edit** to open the **Aggregate Policy Configuration**page.

4. Click the **Position** drop-down list, select a position for the aggregate policy.

- **Adjust directly in the policy list**:



As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy whose position that you want to adjust from the list.
3. Click **Move**.
4. In the pop-up menu, click **Top**, **Bottom** or type the rule ID /name , and click **Before ID** , **After ID** , **Before Name** or **After Name**. Then the rule will be moved before or after the specified ID or name.

Notes:

- The method for adjusting the position of an aggregate policy member is the same as the method for adjusting the position of an aggregate policy.
- The position adjustment for an aggregate policy member can only be performed in the aggregate policy to which it belongs.
- It is not supported to add a policy rule to or remove a policy rule from an aggregate policy by adjusting the position of the policy rule.

Enabling/Disabling an Aggregate Policy

By default, the configured aggregate policy will take effect immediately. By disabling an aggregate policy, the administrator can terminate its control over the traffic.

To enable/disable an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy that you want to enable/disable from the list.
3. Click ⋮ , and then select **Enable** or **Disable** to enable or disable the aggregate policy.

The disabled rule will not display in the list. Click ⋮ , and then select **Show Disabled Policies** to show them.

Notes:

- After disabling an aggregate policy, its members will be disabled too.
- After enabling an aggregate policy, the original status (enabled/disabled) of its members will remain unchanged. For example, if the original status of an aggregate policy member is "disabled", the status will remain unchanged after the policy to which it belongs is enabled.

Configuring a Policy Group

You can organize some policy rules together to form a policy group, and configure the policy group directly.

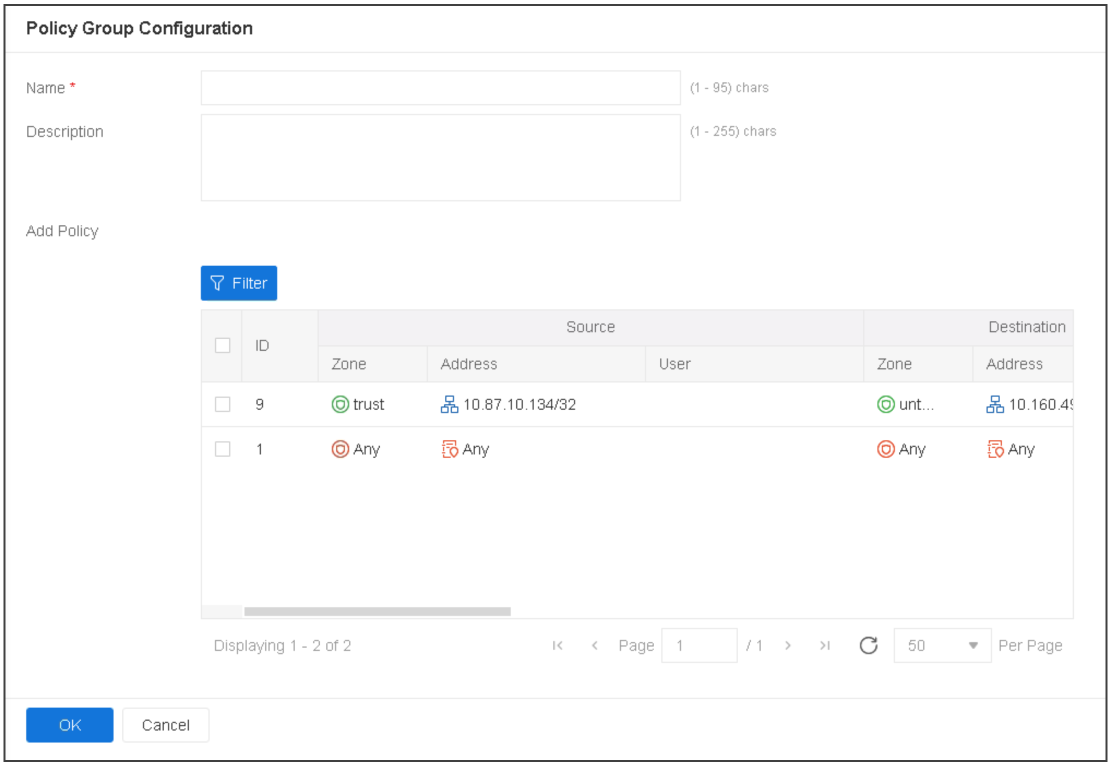
Configuring a security policy group include the following matters: creating a policy group, deleting a policy group, enable/disable a policy group, add/delete a policy rule member, edit a policy group and show disabled policy group.

Creating a Policy Group

To create a policy group, take the following steps:

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

2. Click **New** to open the **Policy Group Configuration** page.



Policy Group Configuration

Name * (1 - 95) chars

Description (1 - 255) chars

Add Policy

Filter

□	ID	Source			Destination	
		Zone	Address	User	Zone	Address
□	9	trust	10.87.10.134/32		unt...	10.160.4
□	1	Any	Any		Any	Any

Displaying 1 - 2 of 2 Page 1 / 1 50 Per Page

OK Cancel

Configure the corresponding options.

Option	Description
Name	Specifies the name of the policy group. The length is 1 to 95 characters.
Description	Specifies the new description. You can enter at most 255 characters.
Add Policy	In the policy rules list, select the security policy rule that you want to add to the policy group.

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

Deleting a Policy Group

To delete a policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. Select the check box of the policy group that you want to delete, and click **Delete**.

Enabling/Disabling a Policy Group

By default the configured policy group will take effect immediately.

To enable/disable a policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. Select the check box of the policy group that you want to enable or disable, and click the enable button under **Status** column. The enabled state is displayed as ● , and the disabled state is displayed as ○ .

Adding/Deleting a Policy Rule Member

To add a policy rule member to the policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
3. Click **Add Members** button to open the **Policy Group-Add policy** page, which displays the list of policy rules that are not added to policy group.

4. Select the check box of the policy rules that you want to add to the policy group.
5. Click **OK** to save your settings.

> **Notes:** A policy rule only can be added to a policy group.

To delete a policy rule member to the policy group, take the following steps:

1. Select **Policy** > **Security Policy** .
2. At the top-right corner of list, click **Policy Group** to enter the **Security Policy Group** page.
3. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
4. Select the check box of the policy group that needs to be deleted, and click **Delete**.

Editing a Policy Group

To modify the name or description of policy group, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy Group** .
2. Select the check box of the policy group that you want to edit, and click **Edit**.
3. Modify the name or description of policy group in the **Policy Group Configuration** page.

Showing Disabled Policy Group

To show disabled policy groups, take the following steps:

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

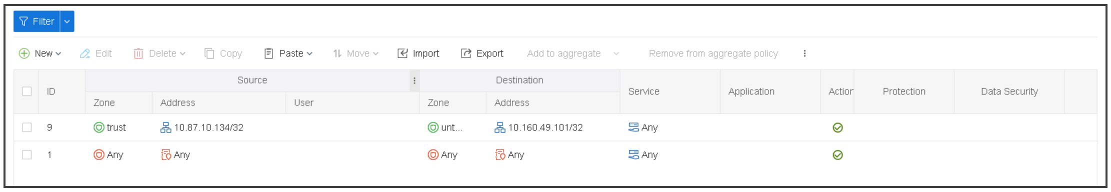
2. Select the check box of **Show Disabled Policy Group**. The disabled policy group will be displayed in the policy group list, otherwise the policy group list will show only the enabled policy group.

Viewing and Searching Security Policy Rules/ Policy Groups

You can view and search the policy rules or policy groups in the policy/ policy group list.

Viewing the Policy/ Policy Group

View the security policy rules in the policy rule list.

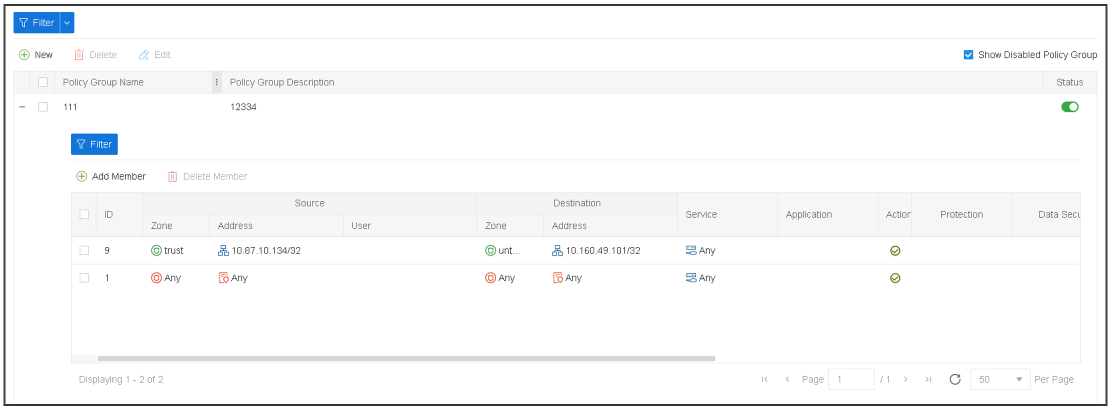


□	ID	Source			Destination		Service	Application	Action	Protection	Data Security
		Zone	Address	User	Zone	Address					
□	9	trust	10.87.10.134/32		unt...	10.160.49.101/32	Any		✓		
□	1	Any	Any		Any	Any	Any		✓		

- 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.
- 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.
- 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.

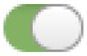
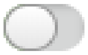
View the policy groups in the policy group list.



□	Policy Group Name	Policy Group Description	Status
− □	111	12334	●

□	ID	Source			Destination		Service	Application	Actior	Protection	Data Secu
		Zone	Address	User	Zone	Address					
□	9	trust	10.87.10.134/32		unt...	10.160.49.101/32	Any		✓		
□	1	Any	Any		Any	Any	Any		✓		

Displaying 1 - 2 of 2

- 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  .

Searching Security Policy Rules/ Policy Groups

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

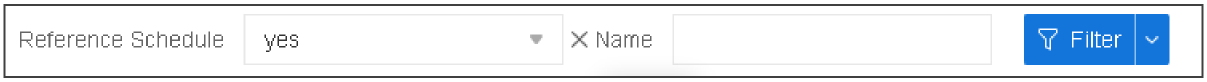
1. Click **Policy** > **Security Policy** > **Policy** or **Policy** > **Security Policy** > **Policy Group**.
2. At the top-right corner of the **Security Policy/ Security Policy Group** page, click **Filter**. Then a new row appears at the top.

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.



Reference Schedule yes × Name Filter

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.

Policy Optimization

If you want to clear up the rules which haven't been used for a long time, it is hard to determine which policy rules need to be deleted when there are a large number of policy rules on the device. The system supports to operate the Policy Hit Analysis, operate the Rule Redundancy Check, and configure the Policy Assistant.

Policy Hit Analysis

Policy Hit Analysis is a process to check the policy rule hit counts, that is, when traffic matches a certain policy rule, the hit count will increase by 1 automatically. With the statistics of the first hit time, the last hit time, and the days since last hit, you can identify the policy rule that need to be cleared. You can view the specified policy rules by setting up filters.

To check the hit counts, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Policy Hit Analysis** tab.

2. Select filter conditions from the **Filter** drop-down list, and configure filter conditions as needed.

   Configure the options as follows.

Option	Description
Days Since First Hit>	Specify the day after the first hit. Then the policy rules which were hit before the specified day will be displayed.
Days Since Last Hit>	Specify the day after the last hit. Then the policies rules before the specified day will be displayed.
Days Since Policy Created>	Specify the day after the policy is created. Then the policy rules before the specified day will be displayed.

3. Click the **Export** button, and the analysis of the filtered policy rules will be exported in the format of CSV.

4. Click **Enter** or any blank space on the page to view the latest result of Policy Optimization.

5. Click + icon in front of policy ID to view the details of the policy rule.

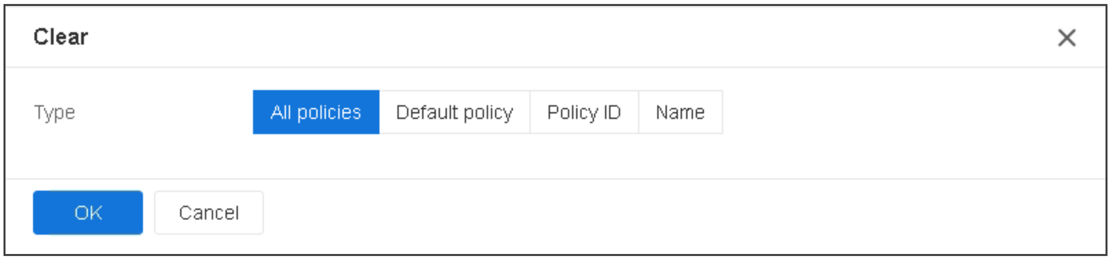
6. Click ⌄ icon on the right side of Filter ⌄ to save the selected filters. Click **Save Filters**, type the name of the filters and click Save. After saved, the combined filters can be selected directly in the drop-down list.

7. To delete a filter condition, hover your mouse on that condition and then click × icon. To delete all filter conditions, click ×Remove All icon on the right side of the row.

To clear a policy hit count, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Policy Hit Analysis** tab.

2. Click **Clear** to open the **Clear** page.



Configure the following options.

Option	Description
All policies	Clears the hit counts of all policy rules.
Default policy	Clears the hit counts of the default action policy rules.

Option	Description
Policy ID	Clears the hit counts of a specified ID policy rule.
Name	Clears the hit counts of a specified name policy rule.

3. Click **OK**.

You can also perform other operations:

- Click 🗑 icon to delete the policy rule.
- Click ⏻ icon to disable the policy rule.

Rule Redundancy Check

In order to make the rules in the policy effective, system provides a method to check the conflicts among rules in a policy. With this method, administrators can check whether the rules overshadow each other.

To start a rule redundancy check, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy Optimization**, and select the **Redundancy Check** tab.
2. Select **Redundancy Check**. After the check, system will list the policy rule which is overshadowed.

Notes: Status will be shown below the policy list when redundancy check is started. It is not recommended to edit a policy rule during the redundancy check. You can click ✖ to stop the check manually.

Configuring the Policy Assistant

The policy assistant can help users generate targeted policies more quickly and accurately. With the function, system can analyze the traffic of a specified policy ID, generate service on the basis of the traffic, optimize the traffic via setting replacement conditions and aggregation conditions, and then generate the target policies.

Click **Policy** > **Security Policy** > **Policy Optimization**, and select the **Policy Assistant** tab. In the **Policy Assistant** tab, generate target policies as the wizard:

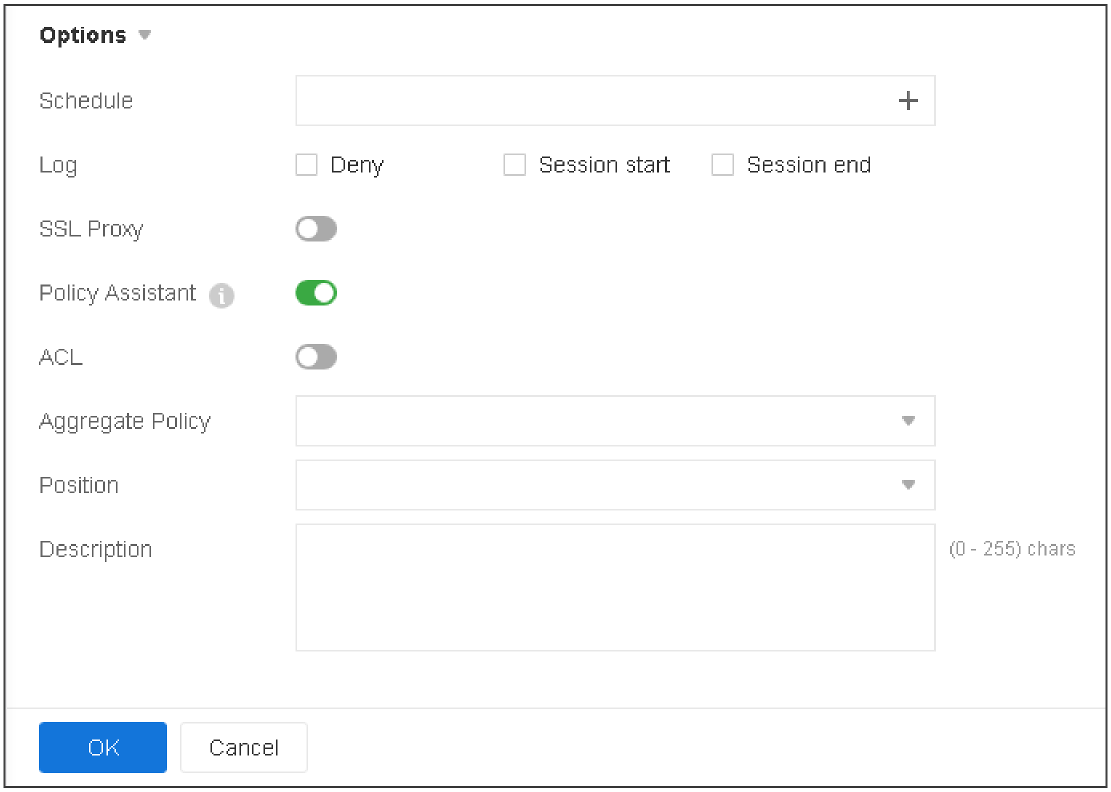
Display Traffic ->Generate Service ->Replace Policy ->Aggregate Policy -> Generate Policy

Enabling the Policy Assistant

Before configuring policy assistant related function, please enable the function first.

1. Select **Policy** > **Security Policy** > **Policy**.
2. Create a rule or select an existing rule which needs to enable the policy assistant function and click **Edit** to open the **Policy Configuration** page.

3. Expand **Options**, and click the **Policy Assistant** button to enable the function.



Options ▾

Schedule

Log □ Deny □ Session start □ Session end

SSL Proxy ○

Policy Assistant ●

ACL ○

Aggregate Policy

Position

Description (0 - 255) chars

OK Cancel

Notes: For the root VSYS, at most 4 policies are allowed to enable the policy assistant function, while for the non-root VSYS, only 1 policy can enable the function.

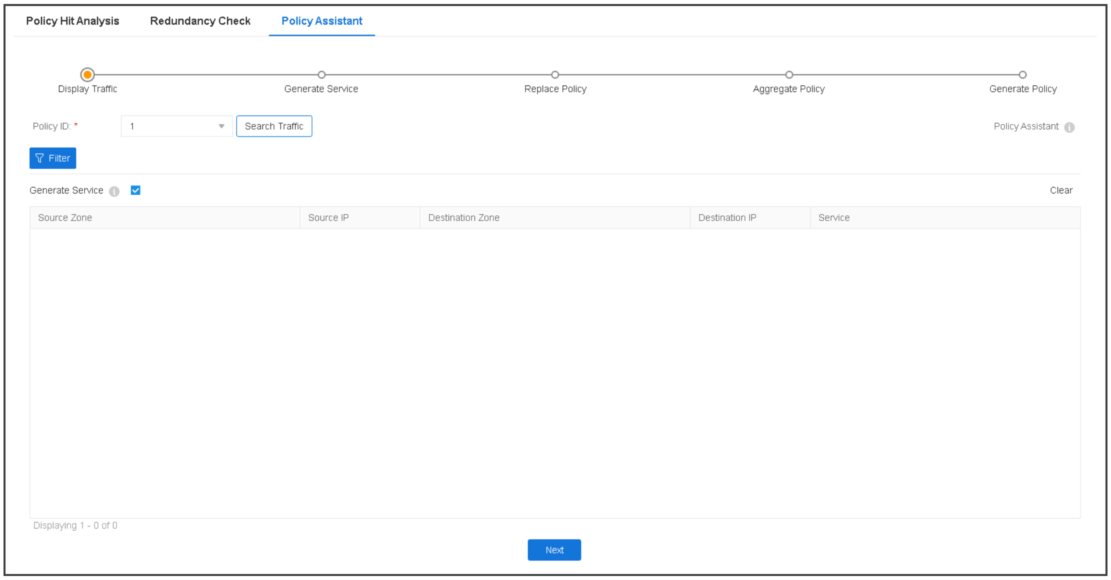
Displaying Traffic

On the Display Traffic page, the source zone, source IP, destination zone, destination IP and service of traffic hit the selected policy ID will be displayed.

To display the traffic data, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy Optimization**, and select the **Policy Assistant** tab.

2. Click **Display Traffic** on the configuration wizard.



Configure the options as follows:

Option	Description
Policy ID	Select the ID of policy which has enabled the policy assistant function from the **Policy ID** drop-down list, click **Search Traffic** and the traffic hit the policy will be displayed in the following list. **Note:** • At most 1,000 traffic data can be displayed in the list. If the traffic data exceeds 1,000, the oldest traffic data will be covered. • If the selected policy is edited, or the policy assistant function is disabled or the device is rebooted, the traffic data will be cleared.

Option	Description
Filter	Click the Filter button to add filtering conditions, and the filtered traffic data will be displayed in the list.
Policy Assistant	Hove the mouse over the ⓘ button to view the help information.
Generate Service	Click the **Generate Service** button to enable the step of Generate Service in the configuration wizard, otherwise, the step will be skipped automatically. For the configurations about Generate Service, refer to Generate Service.
Clear	Click the **Clear** button to delete the searched traffic data in the list. **Note**: Make sure the searched traffic has been analyzed before clearing.

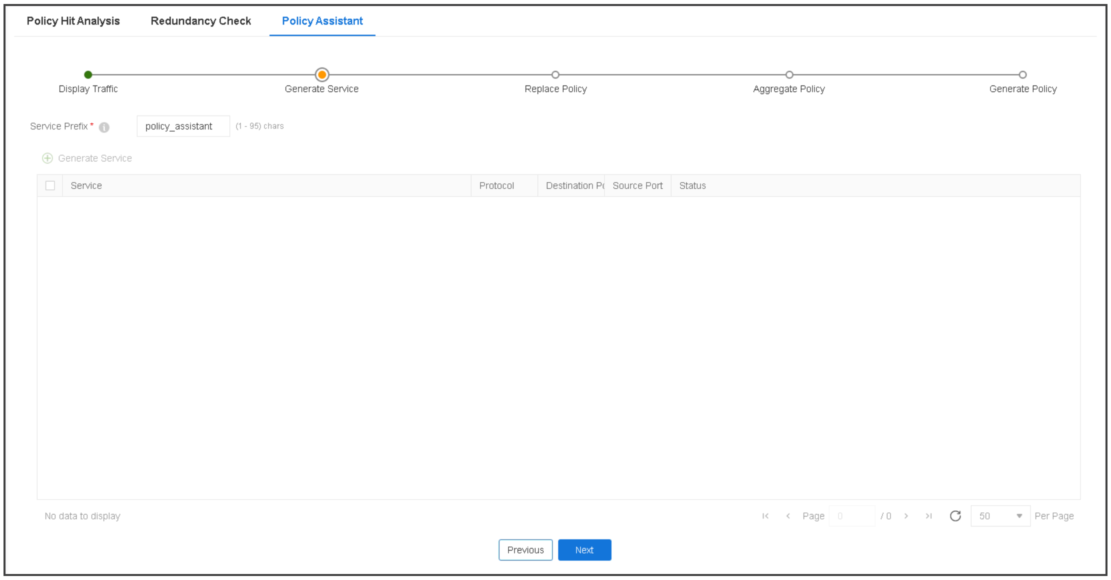
3. Click **Next** to enter into the next configurations.

Generating Service

The searched traffic data can display the protocol and port, and you can generate corresponding service based on the protocol and service, as well as add the service to the service book, so as to deliver the generated policies more accurately.

To generate service, take the following steps:

1. Click **Generate Service** on the configuration wizard. The Generate Service page display items of all services, including the protocol, destination/source port and service status.



Service Prefix * policy_assistant (1 - 95) chars

Page 0 / 0 50 Per Page

Configure the options as follows:

Option	Description
Service Prefix	Specify the prefix for the service in the list. The range is 1 -95 characters. The default prefix is "policy_assistant". When the prefix is specified, the name pf service in the list will change to "the specified prefix + protocol configurations".
Generate Service	Select the check box before the service item, click **Generate Service**, and the corresponded service will be generated and added to the service book. You can also view the generated service in **Object** > **Service Book** > **Service**.After a service is generated, the column of Status will turn Generated.

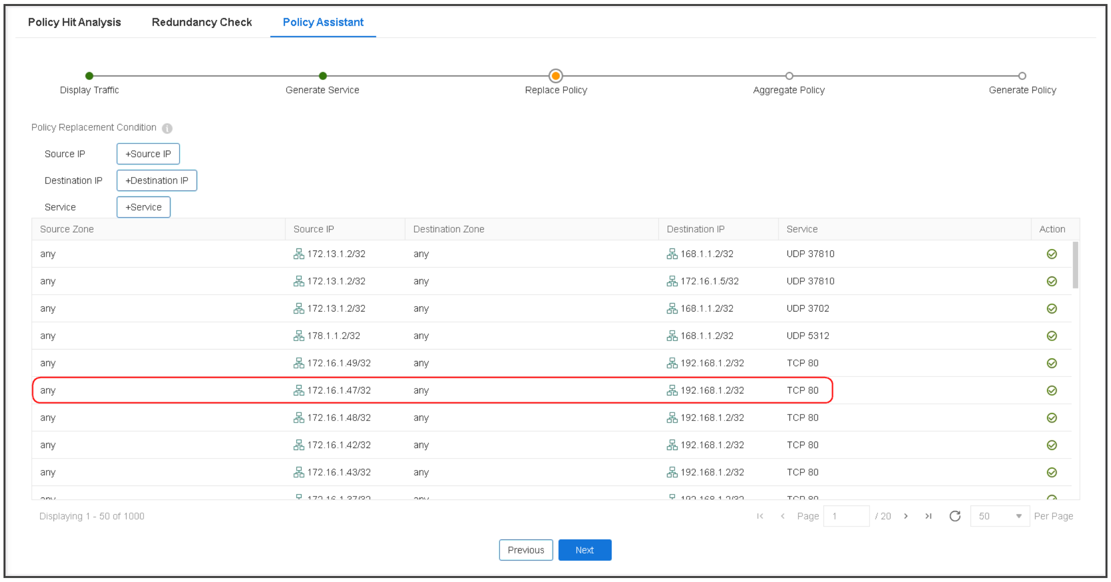
2. Click **Next** to enter into the next configurations.

Replacing Policy

You can set the condition of source IP, destination IP or service. When the items of policies meet the condition, the items will be replaced with the condition.

Application Scenario Example

For example, when the admin get some traffic data originating form 172.16.1.47. After the analysis of the traffic data, the source IP is judged as normal. What's more, all IP address of 172.16.1.0/24 is judged as normal too. To enlarge the source IP range to 172.16.1.0/24, the admin can set the 172.16.1.0/24 as the replacement condition on the Replace Policy page, then the source IP of the searched traffic which is within the IP range will be changed to 172.16.1.0/24.



Policy Replacement Condition

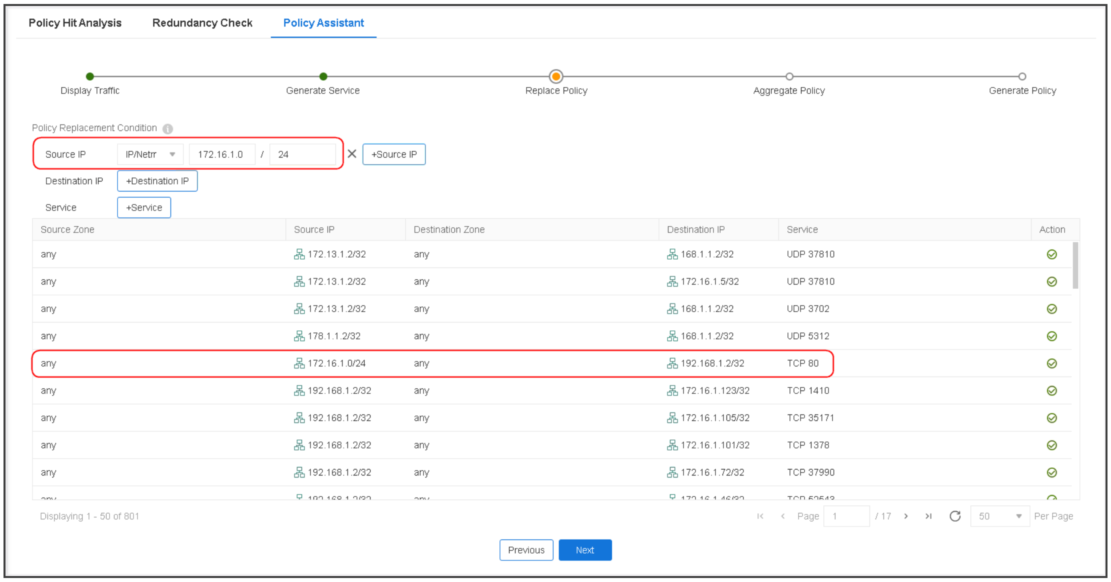
Source IP

Destination IP

Service

Source Zone	Source IP	Destination Zone	Destination IP	Service	Action
any	172.13.1.2/32	any	168.1.1.2/32	UDP 37810	✓
any	172.13.1.2/32	any	172.16.1.5/32	UDP 37810	✓
any	172.13.1.2/32	any	168.1.1.2/32	UDP 3702	✓
any	178.1.1.2/32	any	168.1.1.2/32	UDP 5312	✓
any	172.16.1.49/32	any	192.168.1.2/32	TCP 80	✓
any	172.16.1.47/32	any	192.168.1.2/32	TCP 80	✓
any	172.16.1.48/32	any	192.168.1.2/32	TCP 80	✓
any	172.16.1.42/32	any	192.168.1.2/32	TCP 80	✓
any	172.16.1.43/32	any	192.168.1.2/32	TCP 80	✓
any	172.16.1.37/32	any	192.168.1.2/32	TCP 80	✓

Displaying 1 - 50 of 1000 Page 1 / 20 50 Per Page



Policy Replacement Condition

Source IP IP/Netm 172.16.1.0 / 24

Destination IP

Service

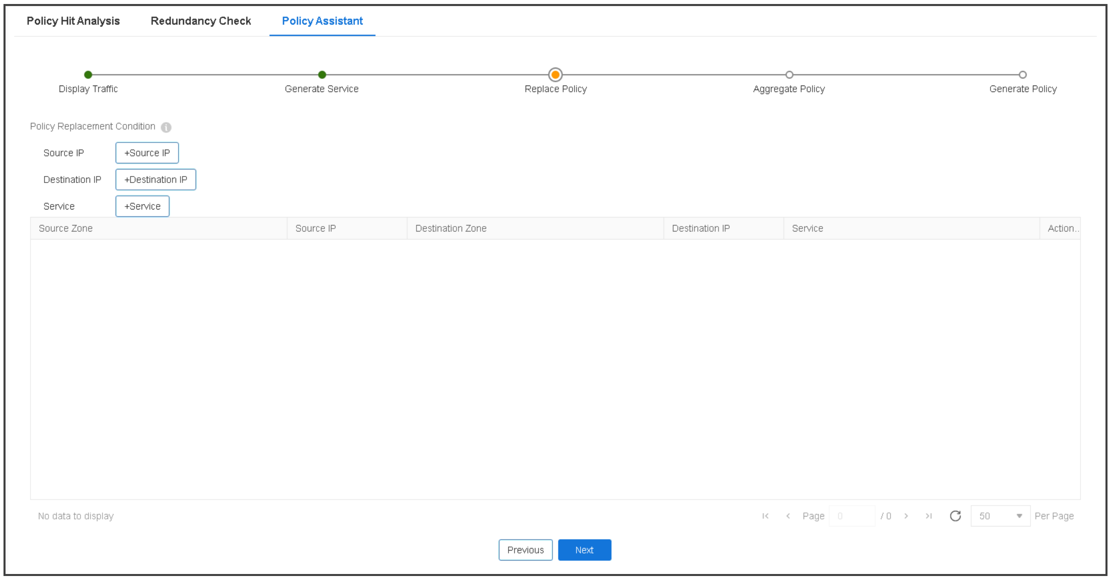
Source Zone	Source IP	Destination Zone	Destination IP	Service	Action
any	172.13.1.2/32	any	168.1.1.2/32	UDP 37810	✓
any	172.13.1.2/32	any	172.16.1.5/32	UDP 37810	✓
any	172.13.1.2/32	any	168.1.1.2/32	UDP 3702	✓
any	178.1.1.2/32	any	168.1.1.2/32	UDP 5312	✓
any	172.16.1.0/24	any	192.168.1.2/32	TCP 80	✓
any	192.168.1.2/32	any	172.16.1.123/32	TCP 1410	✓
any	192.168.1.2/32	any	172.16.1.105/32	TCP 35171	✓
any	192.168.1.2/32	any	172.16.1.101/32	TCP 1378	✓
any	192.168.1.2/32	any	172.16.1.72/32	TCP 37990	✓
any	192.168.1.2/32	any	172.16.1.46/32	TCP 52643	✓

Displaying 1 - 50 of 801 Page 1 / 17 50 Per Page

Configuring Replacement Conditions

To configure replacement conditions for the policy items, take the following steps:

1. Click **Replace Policy** on the configuration wizard.



Configure the options as follows:

Option	Description
Source IP	Specify the replacement condition of source IP. At most 3 conditions can be set for the source IP. 1. Click the +Source IP button. 2. Select IP/Netmask or IP Range from the drop down list and set the replacement conditions as needed.
Destination IP	Specify the replacement condition of destination IP. At most 3 conditions can be set for the destination IP.

Option	Description
	1. Click the +Destination IP button. 2. Select IP/Netmask or IP Range from the drop down list and set the replacement conditions as needed.
Service	Specify the replacement condition of service. At most 3 conditions can be set for the service. 1. Click the +Service button. 2. Specify the protocol from the drop-down list and set the port range as needed.

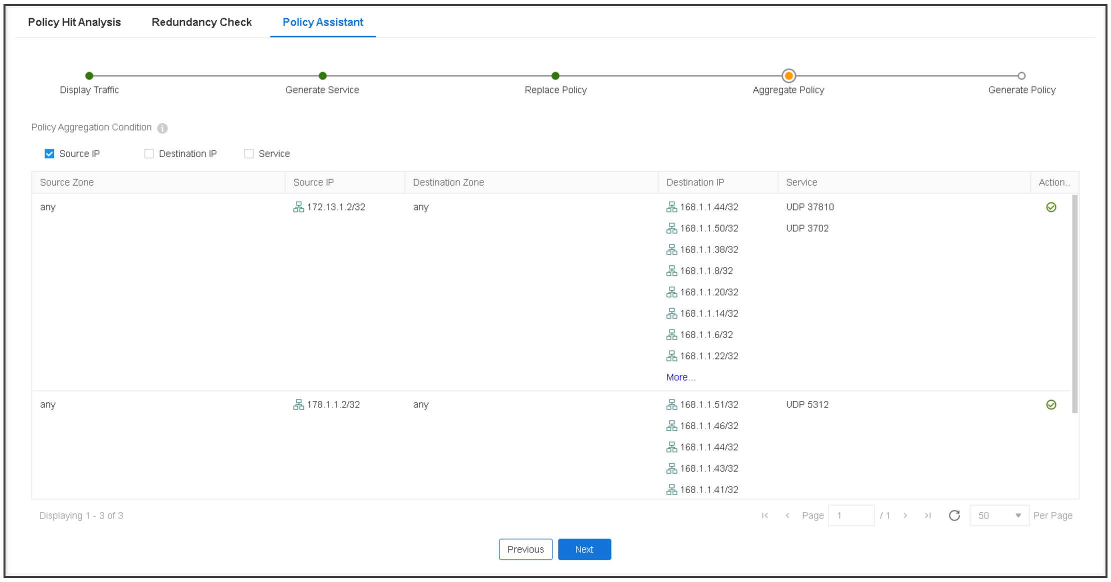
2. Click **Next** to enter into the next configurations.

Aggregating Policy

You can aggregate the policy items of the same source IP, destination IP and service, so as to reduce the redundant policies.

To aggregate policies, take the following steps:

1. Click **Aggregate Policy** on the configuration wizard.



Policy Aggregation Condition

☑ Source IP □ Destination IP □ Service

Source Zone	Source IP	Destination Zone	Destination IP	Service	Action..
any	172.13.1.2/32	any	168.1.1.44/32 168.1.1.50/32 168.1.1.38/32 168.1.1.8/32 168.1.1.20/32 168.1.1.14/32 168.1.1.6/32 168.1.1.22/32 More...	UDP 37810 UDP 3702	✓
any	178.1.1.2/32	any	168.1.1.51/32 168.1.1.46/32 168.1.1.44/32 168.1.1.43/32 168.1.1.41/32	UDP 5312	✓

Displaying 1 - 3 of 3

2. Select the aggregation conditions as Source IP, Destination IP or Service, and the policy items in the list will be aggregated as the selected condition.

3. Click **Next** to enter into the next configurations.

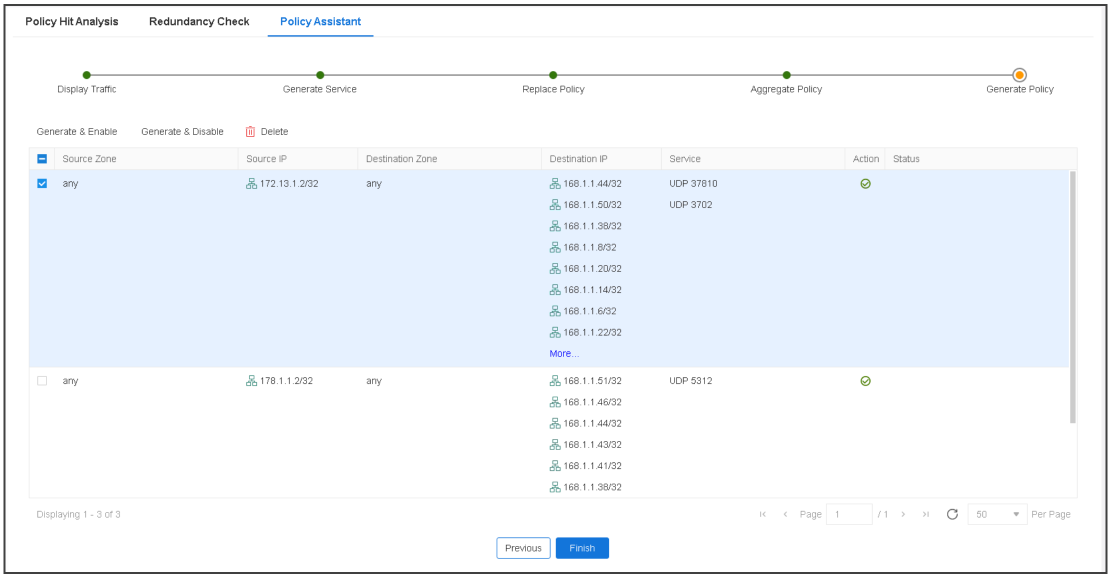
Generating Policy

The Generate Policy page displays all policy items after the configurations in Generate Service, Replace Policy and Aggregate Policy. You can select policy items as needed to generate policy and the selected policy will be display on the **Security Policy** > **Policy** page.

Note: For the generated security policies, the source IP, destination IP and service are determined by the selected aggregation conditions, while the source zone, destination zone and action keep the same with the original policy items.

To generate policies, take the following steps:

1. Click **Generate Policy** on the configuration wizard.



☐	Source Zone	Source IP	Destination Zone	Destination IP	Service	Action	Status
☑	any	172.13.1.2/32	any	168.1.1.44/32 168.1.1.50/32 168.1.1.38/32 168.1.1.8/32 168.1.1.20/32 168.1.1.14/32 168.1.1.6/32 168.1.1.22/32 More...	UDP 37810 UDP 3702	✓	
☐	any	178.1.1.2/32	any	168.1.1.51/32 168.1.1.46/32 168.1.1.44/32 168.1.1.43/32 168.1.1.41/32 168.1.1.38/32	UDP 5312	✓	

Displaying 1 - 3 of 3

Page 1 / 1 50 Per Page

Configure the options as follows:

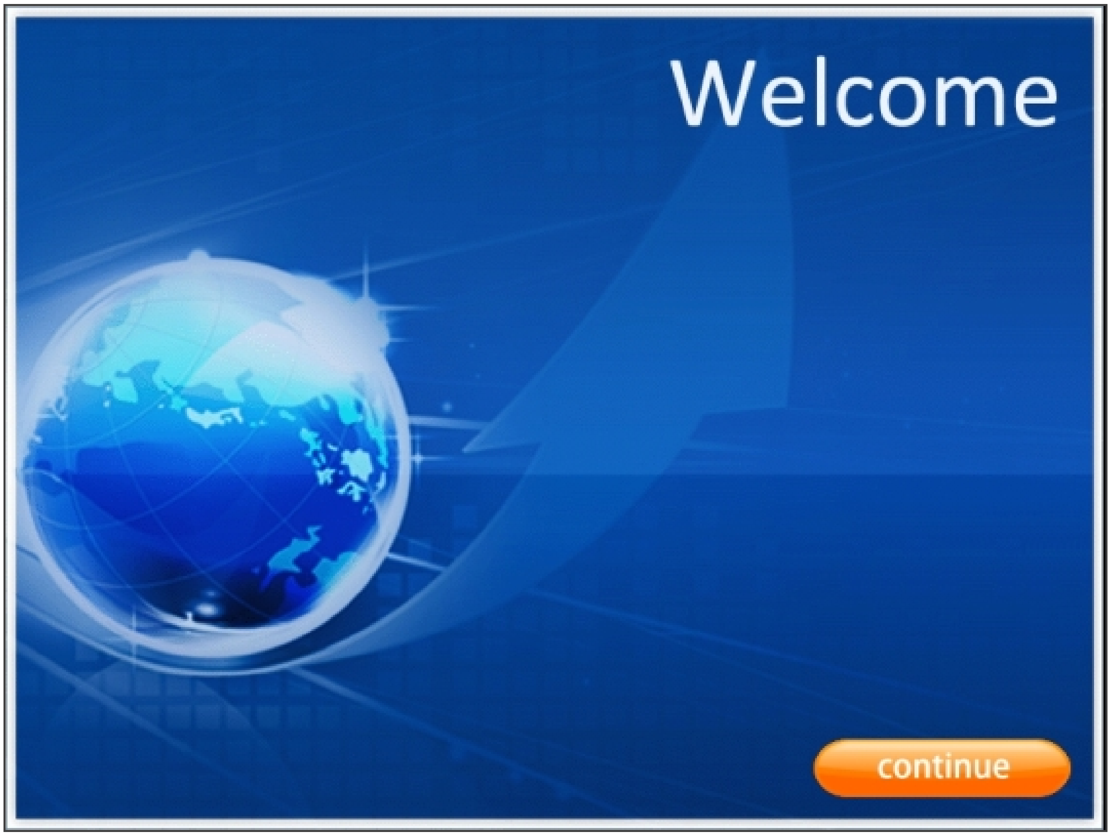
Option	Description
Generate & Enable	Select the check box before the policy items as needed, click **Generate & Enable**, and the policies will take effect after generation. The generated policies will be displayed on the Policy page and on the above of the original policies.
Generate & Disable	Select the check box before the policy items as needed, click **Generate & Disable**, and the policies will not take effect after generation. The generated policies will be displayed on the Policy page and on the above of the original policies.
Delete	Select the check box before the policy items as needed, click **Delete**, and the policies will be deleted.

2. Click **Finish** to finish the configurations of policy assistant.

User Online Notification

The system provides the policy-based user online notification function. The user online notification function integrates WebAuth function and Web redirect function.

After configuring the user online notification function, system redirects your HTTP request to a new notification page when you visit the Internet for the first time. In the process, a prompt page (see the picture below) will be shown first, and after you click **continue** on this page, system will redirect your request to the specified notification page. If you want to visit your original URL, you need to type the URL address into the Web browser.



Before you enable the user online notification function, you must configure the WebAuth function. For more information about configuring WebAuth function, view "Web Authentication" on Page 302.

Configuring User Online Notification

To configure the user online notification function, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with which you want to enable the user online notification function. Generally, it is recommended to select the security policy rule which is under the WebAuth policy rule and whose action is permit to transmit the HTTP traffic.
3. Click **Edit**.
4. In the Policy Configuration page, click the **Enable Web Redirect** button and type the notification URL into the **Notification page URL** box.
5. Click **OK** to save the settings.

Configuring the Parameters of User Online Notification

The parameters are:

- Idle time: The time that an online user stays online without traffic transmitting. If the idle time is exceeded, the HTTP request will be redirected to the user online notification page again.
- Background picture: You can change the background picture on the prompt page.

To configure the parameters, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with the user online notification function enabled.
3. Click ⋮ and select **Web Redirect Configuration**.
4. Type the idle time value into the **Idle time** box. The default value is 30 minutes. The range is 0 to 1440 minutes.

5. Change the background picture of the prompt page. Click **Browse** to choose the picture you want, and then click **Upload**. The uploaded picture must be zipped and named as logo.jpg, with the suggested size of 120px*40px.

Viewing Online Users

After configuring the user online notification function, you can get the information of online users from the Online Notification Users dialog box.

1. Select **Policy > Security Policy**.
2. Click ⋮ and select **Web Redirect IP List**.
3. In the Web Redirect IP List page, view the following information.

Option	Description
IP address	The IP address of the online user.
Sessions	Session number of the online user.
Interface	The source interface of the online user.
Lifetime (s)	The period of time during which the user is staying online.
Expiration (s)	The idle time of the user.

iQoS

System provides iQoS (intelligent quality of service) which guarantees the customer's network performance, manages and optimizes the key bandwidth for critical business traffic, and helps the customer greatly in fully utilizing their bandwidth resources.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested. iQoS is controlled by license. To use iQoS, apply and install the iQoS license.

Notes: If you have configured QoS in the previous QoS function before upgrading the system to verion 5.5, the previous QoS function will take effect. You still need to configure the previous QoS function in CLI. You cannot use the newest iQoS function in version 5.5 and the newest iQoS function will not display in the WebUI and will not take effect. If you have not configured the previous QoS function before upgrading the system to version 5.5, the system will enable the newest iQoS function in version 5.5. You can configure iQoS function in the WebUI and the previous QoS function will not take effect.

Implement Mechanism

The packets are classified and marked after entering system from the ingress interface. For the classified and marked traffic, system will smoothly forward the traffic through the shaping mechanism, or drop the traffic through the policing mechanism. If the shaping mechanism is selected to forward the traffic, the congestion management and congestion avoidance mechanisms will give different priorities to different types of packets so that the packets of higher priority can pass though the gateway earlier to avoid network congestion.

In general, implementing QoS includes:

- Classification and marking mechanism: Classification and marking is the process of identifying the priority of each packet. This is the first step of iQoS.

- Policing and shaping mechanisms: Policing and shaping mechanisms are used to identify traffic violation and make responses. The policing mechanism checks the traffic in real time and takes immediate actions according to the settings when it discovers a violation. The shaping mechanism works together with queuing mechanism. It makes sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly.

- Congestion management mechanism: Congestion management mechanism uses the queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work.

- Congestion avoidance mechanism: Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic.

Pipes and Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes.

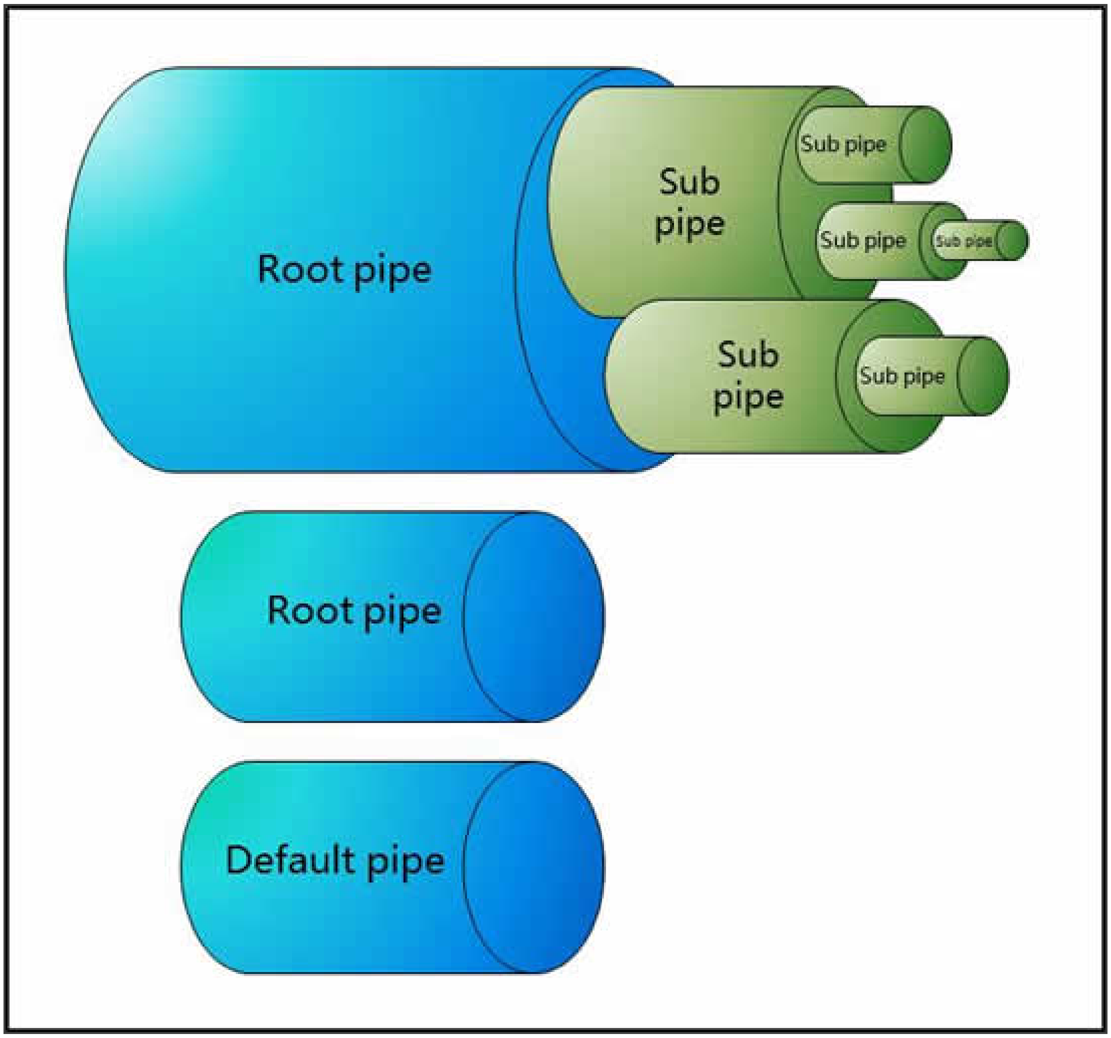
Pipes

By configuring pipes, the devices implement iQoS. Pipe, which is a virtual concept, represents the bandwidth of transmission path. System classifies the traffic by using the pipe as the unit, and controls the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe pre-defined by the system.

Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- Traffic matching conditions: Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. System will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the Policy > iQoS page.
- Traffic management actions: Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. Forward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

To provide flexible configurations, system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:



- You can create multiple root pipes that are independent. At most three levels of sub pipes can be nested to the root pipe.

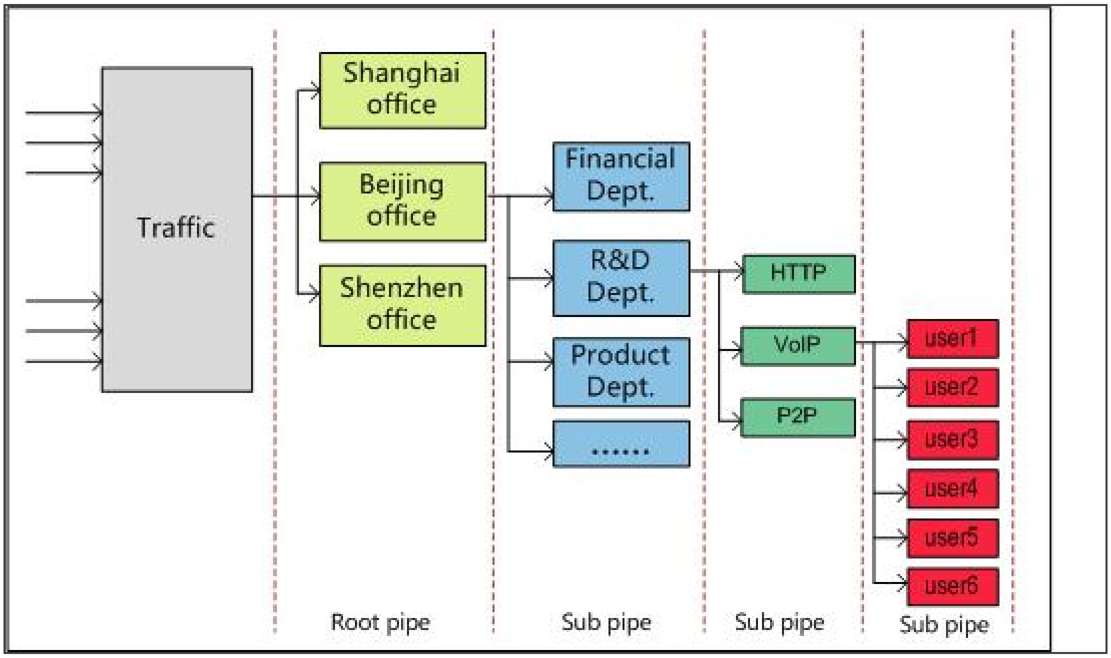
- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.

- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belong to this root pipe will inherit the configurations of the traffic direction set on the root pipe.

- The root pipe that is only configured the backward traffic management actions cannot work.

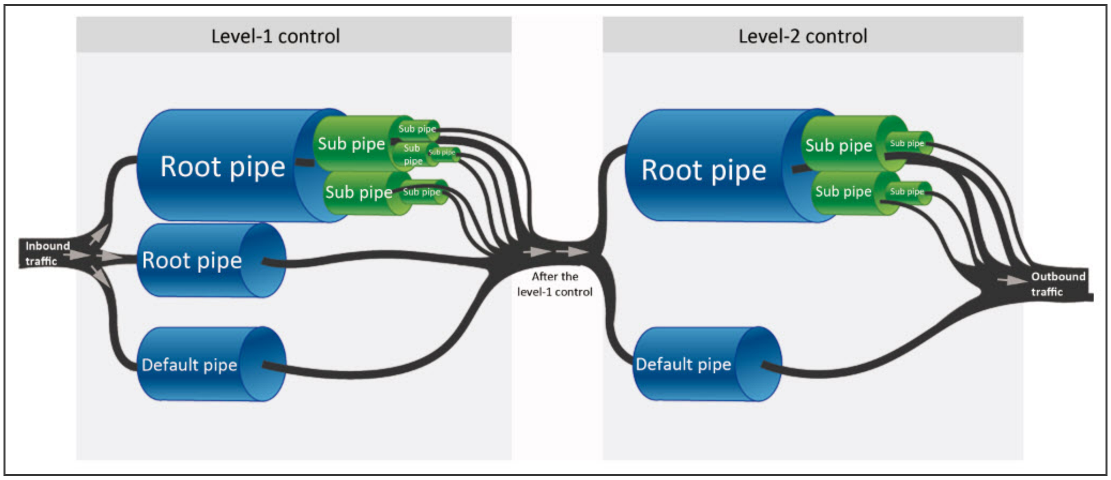
The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

1. Create a root pipe to limit the traffic of the office located in Beijing.
2. Create a sub pipe to limit the traffic of its R&D department.
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.
4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flowing into the device, the process of iQoS is shown as below:



According to the chart above, the process of traffic control is described below:

1. The traffic first flows into the level-1 control, and then system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the **Policy > iQoS** page. After the traffic flows into the root pipe, system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.

2. According to the traffic management actions configured for the pipes, system manages and controls the traffic that matches the traffic matching conditions.

3. The traffic dealt with by level-1 control flows into the level-2 control. System manages and controls the traffic in level-2 control. The principles of traffic matching, management and control are the same as the one of the level-1 control.

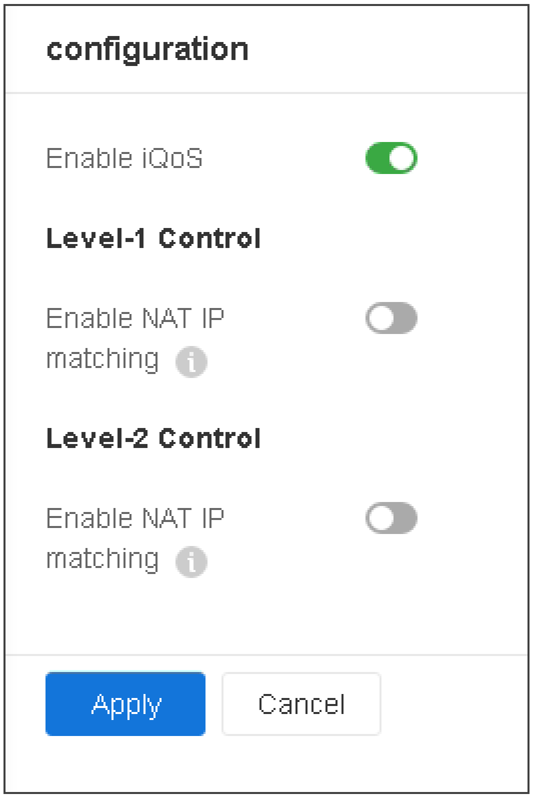
4. Complete the process of iQoS.

Enabling iQoS

To enable iQoS, take the following steps:

1. Select **Policy > iQoS > Configuration**.

2. Click the **Enable iQoS** button.



configuration

Enable iQoS ●

Level-1 Control

Enable NAT IP matching ○

Level-2 Control

Enable NAT IP matching ○

3. If you click the **Enable NAT IP matching** button in **Level-1 Control** or **Level-2 Control**, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is successful, system will limit the speed of these IP

addresses.

Notes: Before enabling NAT IP matching, you must config the NAT rules. Otherwise, the configuration will not take effect.

4. Click **Apply** to save the configurations.

Pipes

By using pipes, devices implement iQoS. Pipes in different traffic control levels will take effect in different stages.

Configuring pipes includes the following sections:

1. Create the traffic matching conditions, which are used to capture the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.

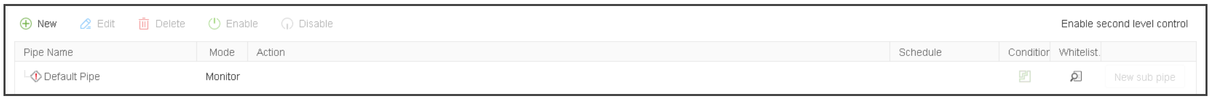
2. Create a white list according to your requirements. System will not control the traffic in the white list. Only root pipe and the default pipe support the white list.

3. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.

4. Specify the schedule. The pipe will take effect during the specified time period.

Basic Operations

Select **Policy > iQoS > Policy** to open the Policy page.



Pipe Name	Mode	Action	Schedule	Conditior	Whitelist.
Default Pipe	Monitor				

You can perform the following actions in this page:

- Disable the level-2 traffic control: Click **Disable second level control**. The pipes in the level-2 traffic control will not take effect. The Level-2 Control tab will not appears in this page.

- View pipe information: The pipe list displays the name, mode, action, schedule, and the description of the pipes.

- Click the ◢ icon to expand the root pipe and display its sub pipes.
- Click the ▣ icon of the root pipe or the sub pipe to view the condition settings.
- Click the ☰ icon of the root pipe to view the white list settings.
- ◇ represents the root pipe is usable, ⚠ represents the root pipe is unusable, ✎ represents the sub pipe is usable, ✎ represents the sub pipe is unusable,

  Default Pipe
  the gray text represents the pipe is disabled.

- Create a root pipe: Select the Level-1 Control or Level-2 Control tab, then click **New** in the menu bar to create a new root pipe.
- Create a sub pipe: Click the ⤵ icon of the root pipe or the sub pipe to create the corresponding sub pipe.
- Click **Enable** in the menu bar to enable the selected pipe. By default, the newly-created pipe will be enabled.
- Click **Disable** in the menu bar to disable the selected pipe. The disabled pipe will not take effect.
- Click **Delete** to delete the selected pipe. The default pipe cannot be deleted.

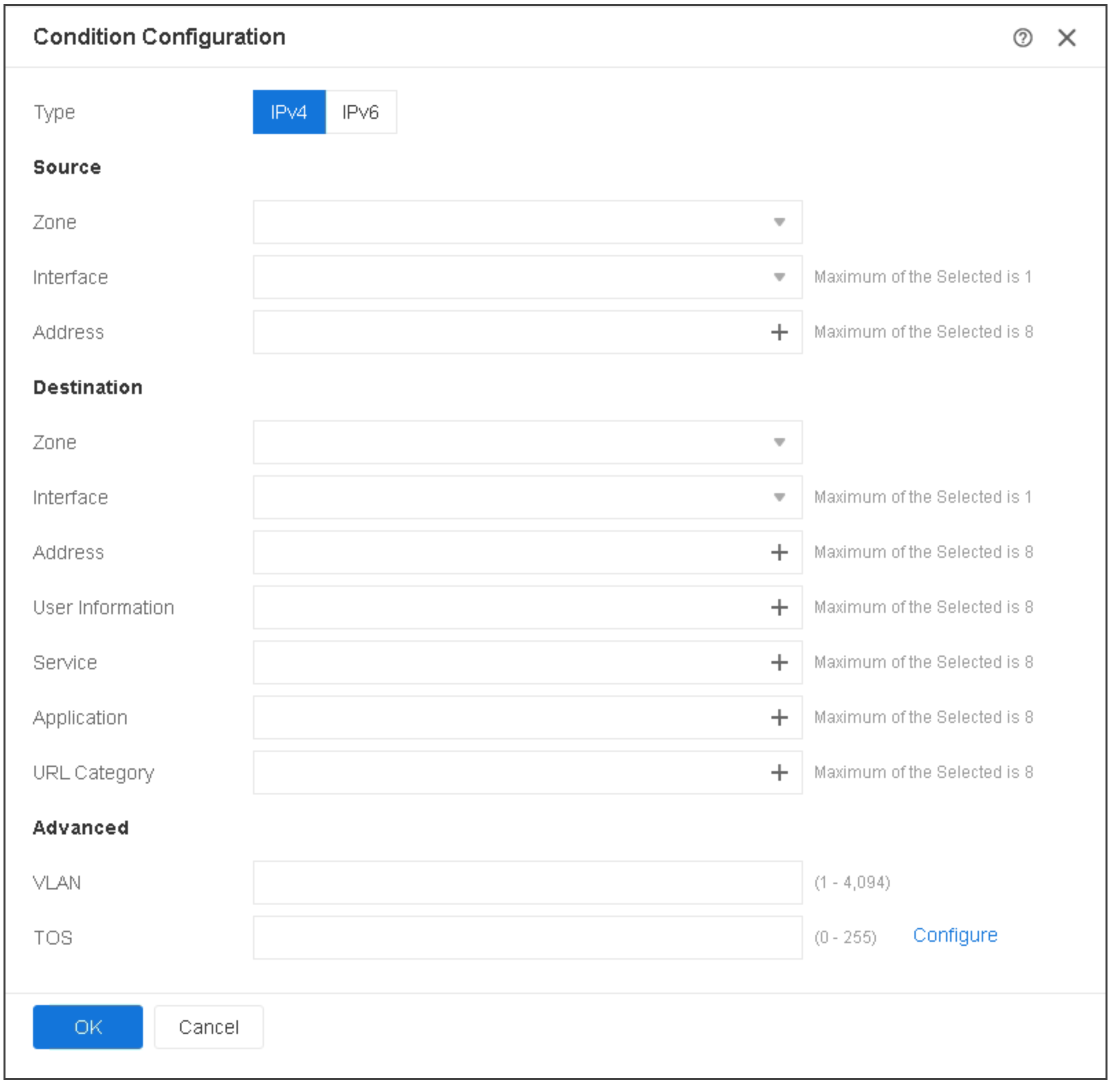
Configuring a Pipe

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.
Description	Specify the description of this pipe.
Mode	Shape, Policy, or Monitor. • 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. • The Monitor mode will monitor the matched traffic, generate the statistics, and will not control the traffic. • 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.

3. In Condition, click **New**.



Condition Configuration

Type: IPv4 | IPv6

Source

Zone

Interface — Maximum of the Selected is 1

Address — Maximum of the Selected is 8

Destination

Zone

Interface — Maximum of the Selected is 1

Address — Maximum of the Selected is 8

User Information — Maximum of the Selected is 8

Service — Maximum of the Selected is 8

Application — Maximum of the Selected is 8

URL Category — Maximum of the Selected is 8

Advanced

VLAN — (1 - 4,094)

TOS — (0 - 255) Configure

In the Condition Configuration page, configure the corresponding options.

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.

Option	Description
Source Information	
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.
Address	Specify the source address of the traffic. 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 address configuration. You can also perform other operations: - When selecting the **Address Book** type, you can click ⊕ to create a new address entry. - The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
Destination Information	
Zone	Specify the destination zone of the traffic. Select the zone

Option	Description
	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. 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 right 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. - The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
User Information	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

Option	Description
	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 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: - To add a new service or service group, select **User-defined** from the "Predefined" drop-down list, and click ⊕.

Option	Description
	- 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 **Clos**e complete the application configuration. You can also perform other operations: - To add a new application group, click ⊕. - To add a new application filter, click ⊕.
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. 1. In the "URL category" drop-down menu, the user can select one or more URL categories, up to 8

Option	Description
	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. **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. • Max Bandwidth: Specify the maximum 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.
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. • Max Bandwidth: Specify the maximum 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.

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

Viewing Statistics of Pipe Monitor

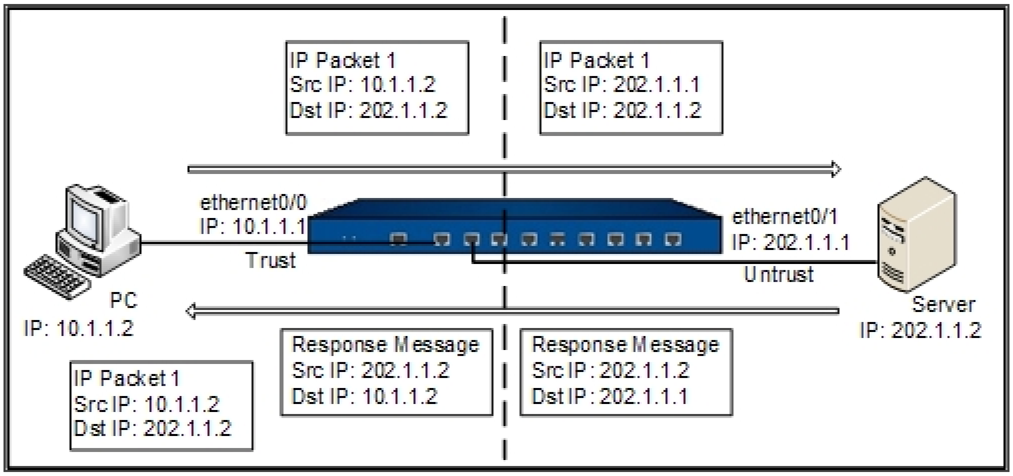
To view the statistics of pipe monitor, see "iQoS" on Page 827.

NAT

NAT, Network Address Translation, translates the IP address within an IP packet header to another IP address. When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, vice versa.

Basic Translation Process of NAT

When a device is implementing the NAT function, it lies between the public network and the private network. The following diagram illustrates the basic translation process of NAT.



As shown above, the device lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the device, the device checks the packet header. Finding that the IP packet is destined to the public network, the device translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the device also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the device, the device checks the packet header again and finds the mapping records in its NAT table, and replaces the destination address with the private address 10.1.1.2. In this process, the device is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is

202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

Implementing NAT

The devices translate the IP address and port number of the internal network host to the external network address and port number, and vice versa. This is the translation between the "private IP address + port number" and "public IP address + port number".

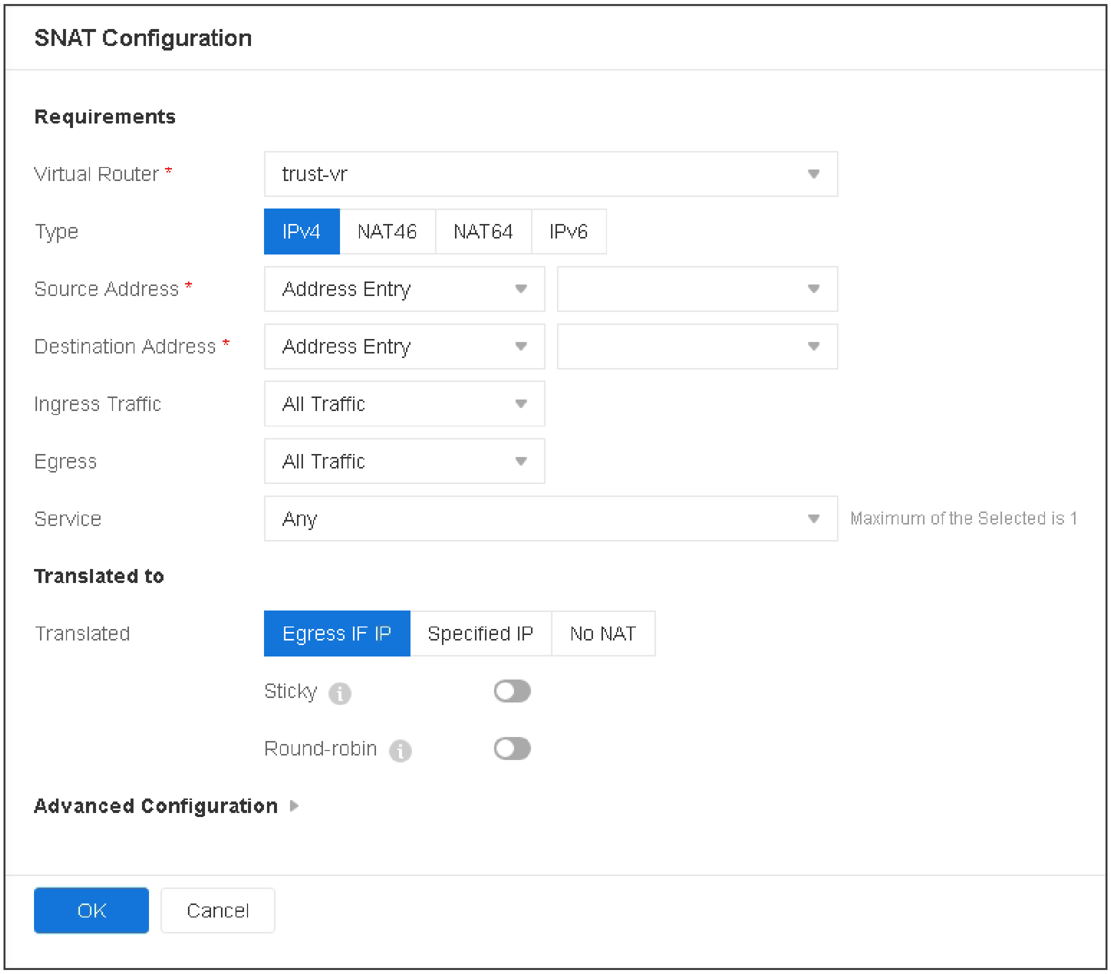
The devices achieve the NAT function through the creation and implementation of NAT rules. There are two types of NAT rules, which are source NAT rules (SNAT Rule) and destination NAT rules (DNAT Rule). SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses; DNAT translates destination IP addresses, and usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to public IP addresses.

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.



SNAT Configuration

Requirements

Virtual Router *: trust-vr

Type: IPv4

Source Address *: Address Entry

Destination Address *: Address Entry

Ingress Traffic: All Traffic

Egress: All Traffic

Service: Any

Maximum of the Selected is 1

Translated to

Translated: Egress IF IP

Sticky

Round-robin

Advanced Configuration

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

Requirements	
	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 Address	Specifies the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP 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 Address	Specifies the destination IP address of the traffic, including: • Address Entry - Select an address entry from the

Requirements	
	drop-down list. • IP Address - Type an IP 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.

Requirements	
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 - 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

Requirements	
	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.
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

Requirements	
	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. • 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" on Page 654. 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 suc-

Requirements	
	cessfully 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 **Note**： The Sticky function and the Round-robin function are mutually exclusive and cannot be configured at the same time.

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.
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.
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 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

Option	Description
	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.

Enabling/Disabling a SNAT Rule

By default the configured SNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule:

1. Select **Policy** > **NAT** > **SNAT**.
2. Select the SNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

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.

To adjust priority, take the following steps:

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.

Copying/Pasting a SNAT Rule

When there are a large number of NAT rules in system, to create a NAT rule which is similar to an configured NAT rule easily, you can copy the NAT rule and paste it to the specified location.

To copy/paste a SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Select the SNAT rule that you want to clone and click **Copy**.

3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.

    - Top: The rule is pasted to the top of all the rules in the SNAT rule list.

    - Bottom: The rule is pasted to the bottom of all the rules in the SNAT rule list.

- Before the Rule Selected: The rule will be pasted before the Rule being selected.

- After the Rule Selected: The rule will be pasted after the Rule being selected.

Exporting NAT444 Static Mapping Entries

You can export the NAT444 static mapping entries to a file . The exported file contains the ID, source IP address, translated IP address, start port, end port, and the protocol information.

To export the NAT444 static mapping entries, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Click **Export NAT444 Static Mapping Entries.**

3. Select a location to store the file and click **Save**.

The exported file is CSV format. It is recommended to export the file through the management interface.

Hit Count

The system supports statistics on SNAT rule hit counts, i.e., statistics on the matching between traffic and SNAT rules. Each time the inbound traffic is matched to a certain SNAT rule, the hit count will increment by 1 automatically.

To view a SNAT rule hit count, click **Policy > NAT > SNAT**. In the SNAT rule list, view the statistics on SNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a SNAT rule hit count, take the following steps:

1. Select **Policy > NAT > SNAT Hit Analysis**.

2. Click **Clear** to open the **Clearing NAT Hit Count** page.

   - All NAT: Clears the hit counts for all NAT rules.

- NAT ID: Clears the hit counts for a specified NAT rule ID.

3. Click **OK**.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

1. Select **Policy > NAT > SNAT Hit Analysis**.

2. Click **Analyze**.

Configuring DNAT

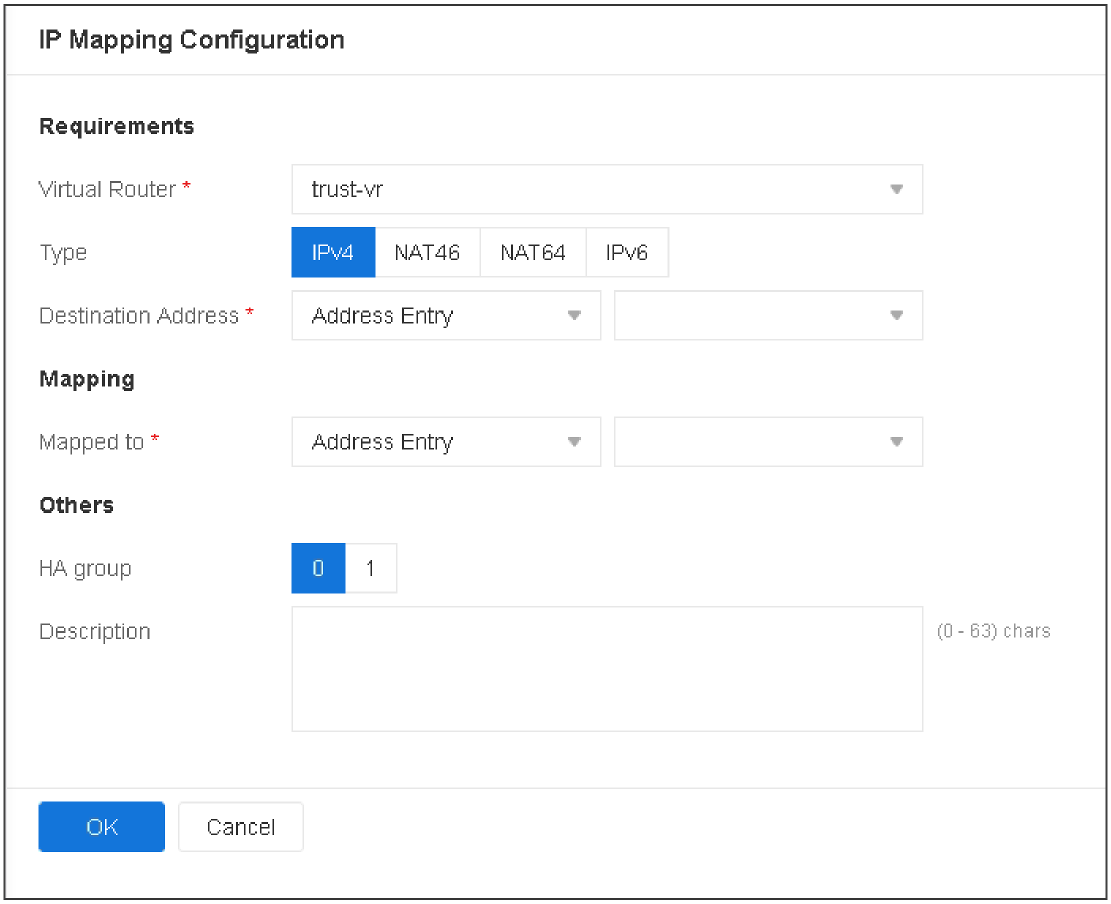
DNAT translates destination IP addresses, usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to the public IP addresses.

Configuring an IP Mapping Rule

To configure an IP mapping rule, take the following steps:

1. Select **Policy > NAT > DNAT**.

2. Click **New** and select **IP Mapping**.



IP Mapping Configuration

Requirements

Virtual Router *: trust-vr

Type: IPv4 | NAT46 | NAT64 | IPv6

Destination Address *: Address Entry

Mapping

Mapped to *: Address Entry

Others

HA group: 0 | 1

Description: (0 - 63) chars

In the IP Mapping Configuration page, configure the corresponding options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.
Destination Address	Specifies the destination IP address or interface of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT 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 DNAT 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 DNAT rule is NAT64 or IPv6.

Requirements	
	- Dynamic IP (Physical Interface) - Select an interface which obtains IP via the DHCP and PPPoE protocols. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Mapping	
Mapped to	Specifies the translated NAT IP address, including **Address Entry**, **IP Address**, and **IP/Netmask** (or **IPv6/Prefix**). The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

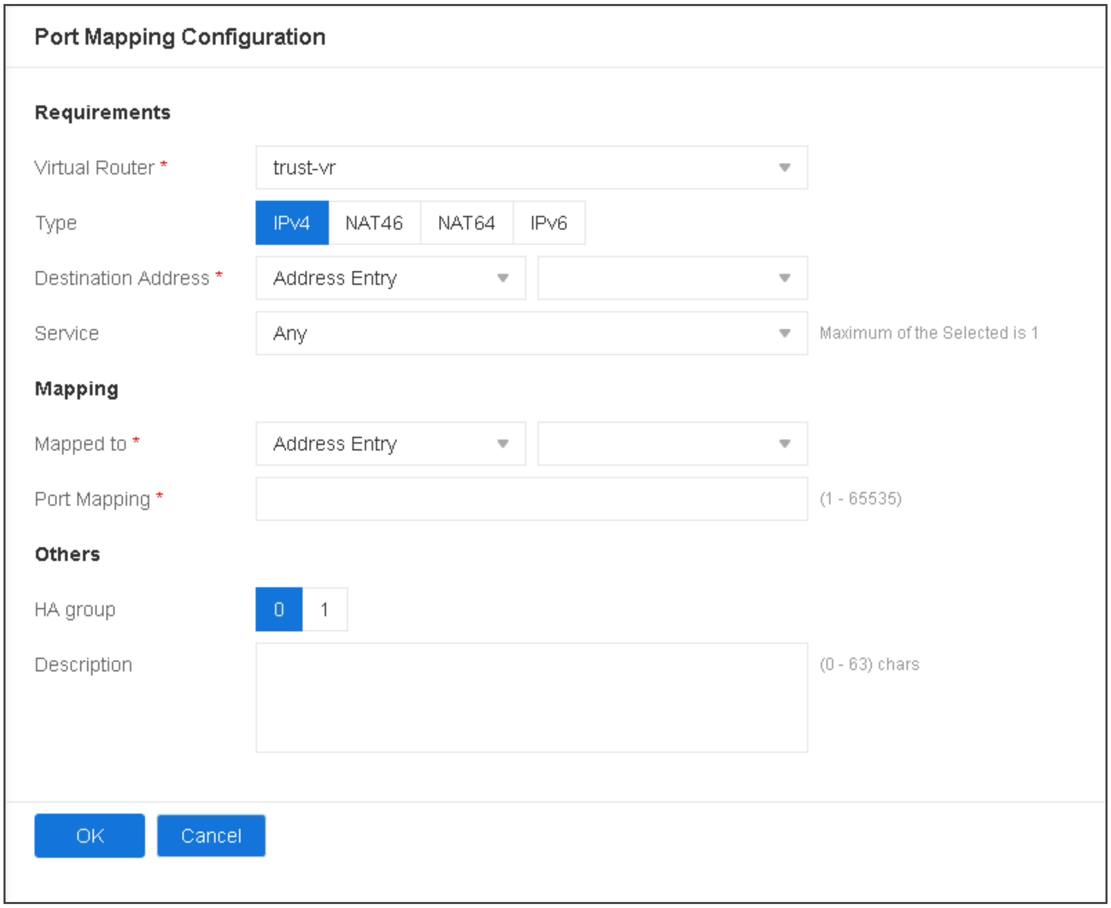
3. Click **OK** to save the settings.

Configuring a Port Mapping Rule

To configure a port mapping rule, take the following steps:

1. Select **Policy** > **NAT** > **DNAT**.

2. Click **New** and select **Port Mapping**.



Port Mapping Configuration

Requirements

Virtual Router * trust-vr

Type IPv4 NAT46 NAT64 IPv6

Destination Address * Address Entry

Service Any Maximum of the Selected is 1

Mapping

Mapped to * Address Entry

Port Mapping * (1 - 65535)

Others

HA group 0 1

Description (0 - 63) chars

In the Port Mapping Configuration page configure the corresponding options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.

Requirements	
Destination Address	Specifies the destination IP address or interface of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT 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 DNAT 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 DNAT rule is NAT64 or IPv6. • Dynamic IP(Physical Interface) - Select an interface which obtains IP via the DHCP and PPPoE protocols. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **New Ser-**

Requirements	
	vice or **New Group**.
Mapping	
Mapped to	Specifies the translated NAT IP address, including **Address Entry**, **IP Address**, and **IP/Netmask** (or **IPv6/Prefix**). The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Port Mapping	Types the translated port number of the Intranet server. The available range is 1 to 65535.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

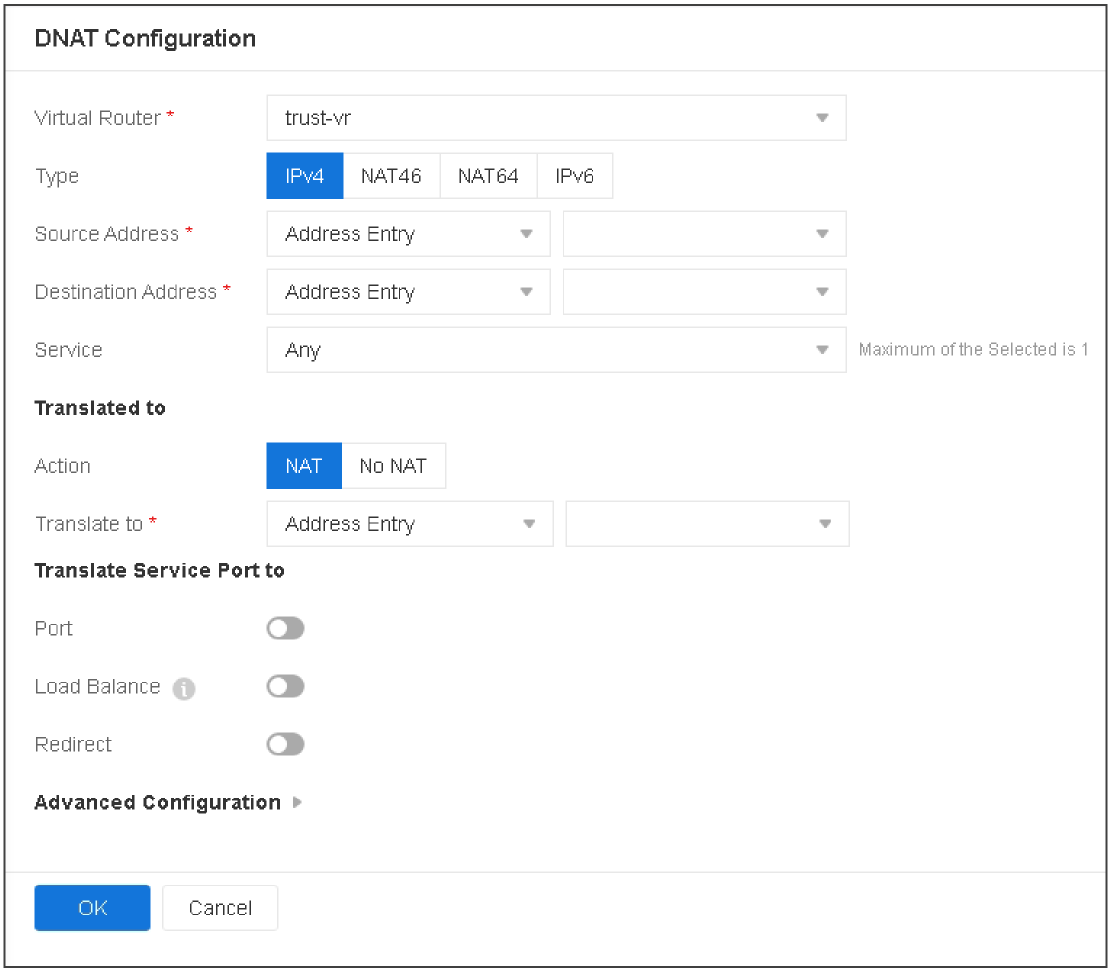
3. Click **OK** to save the settings.

Configuring an Advanced NAT Rule

You can create a DNAT rule and configure the advanced settings, or you can edit the advanced settings of an exiting DNAT rule.

To create a DNAT rule and configure the advanced settings, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Click **New** and select **Advanced Configuration**. To edit the advanced settings of an existing DNAT rule, select it and click **Edit**. The **DNAT configuration** page will appear.



DNAT Configuration

Virtual Router * trust-vr

Type [✓ IPv4] NAT46 NAT64 IPv6

Source Address * Address Entry

Destination Address * Address Entry

Service Any Maximum of the Selected is 1

Translated to

Action [✓ NAT] No NAT

Translate to * Address Entry

Translate Service Port to

Port ○

Load Balance ○

Redirect ○

In this page, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.

Requirements	
Source Address	Specifies the source IP address of the traffic, including: - Address Entry - Select an address entry from the drop-down list. - IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT 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 DNAT 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 DNAT rule is NAT64 or IPv6.
Destination Address	Specifies the destination IP address or interface of the traffic, including: - Address Entry - Select an address entry from the drop-down list. - IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT rule is NAT64 or IPv6.

Requirements	
	• IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the DNAT 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 DNAT rule is NAT64 or IPv6. • Dynamic IP(Physical Interface): Select an interface which obtains IP via the DHCP and PPPoE protocols. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **Add**.
Translated to	
Action	Specifies the action for the traffic you specified, including: • NAT - Implements NAT for the eligible traffic. • No NAT - Do not implement NAT for the eligible traffic. • V4-MAPPED - Implements NAT for the eligible traffic, and extracts the destination IPv4 address

Requirements	
	from the destination IPv6 address of the packet directly. This configuration option is available if the type of the DNAT rule is NAT64. The **Translated to** action for different types of DNAT rules may vary in this page, please refer to the actual page.
Translate to	When selecting the **NAT** option, you need to specify the translated IP address. The options include **Address Entry**, **IP Address**, **IP/Netmask** (or **IPv6/Prefix**), and **SLB Server Pool**. The **SLB Server Pool** configure option is available if the type of the DNAT rule is IPv4 or NAT64. For more information about the SLB Server Pool, view "SLB Server Pool " on Page 581.
Translate Service Port to	
Port	Click **Enable** to translate the port number of the service that matches the conditions above.
Load Balance	Click **Enable** to enable the function. Traffic will be balanced to different Intranet servers.
Redirect	Click **Enable** to enable the function. When the number of this **Translate to** is different from the **Destination Address** of the traffic or the **Destination Address** address is **any**, you must enable the redirect function for this DNAT rule.

Expand Advanced Configuration, configure the following options.

Track Server	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Track Ping Packets	After enabling this function, system will send Ping packets to check whether the Intranet servers are reachable.
Track TCP Packets	After enabling this function, System will send TCP packets to check whether the TCP ports of Intranet servers are reachable.
TCP Port	Specifies the TCP port number of the monitored Intranet server.
NAT Log	Enable the log function for this DNAT rule to generate the log information when traffic matches this NAT rule.
Position	Specifies the position of the rule. Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules by sequence, and then implement DNAT on 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. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all of the rules in the DNAT rule list. By default, the system will put the newly-created DNAT rule at the bottom of all of the SNAT rules. • Top - The rule is located at the top of all of the

Track Server	
	rules in the DNAT 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	The ID number is used to distinguish between NAT rules. Specifies the method you get the rule ID. It can be automatically assigned by system or manually assigned by yourself.
Description	Types the description.

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

Enabling/Disabling a DNAT Rule

By default the configured DNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule, take the following steps:

1. Select **Policy** > **NAT** > **DNAT**.
2. Select the DNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Copying/Pasting a DNAT Rule

When there are a large number of NAT rules in system, to create a NAT rule which is similar to an configured NAT rule easily, you can copy the NAT rule and paste it to the specified location.

To copy/paste a DNAT rule, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the DNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.
   - Top: The rule is pasted to the top of all of the rules in the DNAT rule list.
   - Bottom: The rule is pasted to the bottom of all of the rules in the DNAT rule list.
   - Before the Rule Selected: The rule will be pasted before the Rule selected.
   - After the Rule Selected: The rule will be pasted after the Rule selected.

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.

To adjust priority, take the following steps:

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.

Hit Count

The system supports statistics on DNAT rule hit counts, i.e., statistics on the matching between traffic and DNAT rules. Each time the inbound traffic is matched to a certain DNAT rule, the hit count will increment by 1 automatically.

To view a DNAT rule hit count, click **Policy > NAT > DNAT**. In the DNAT rule list, view the statistics on DNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a DNAT rule hit count, take the following steps:

1. Select **Policy > NAT > DNAT Hit Analysis**.
2. Click **Clear** to open the **Clearing NAT Hit Count** page.
   - All NAT: Clears the hit counts for all NAT rules.
   - NAT ID: Clears the hit counts for a specified NAT rule ID.
3. Click **OK**.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

1. Select **Policy > NAT > DNAT Hit Analysis**.

2. Click **Analyze**.

SLB Server

View SLB server status: After you enabling the track function (PING track, TCP track, or UDP track), system will list the status and information of the intranet servers that are tracked.

View SLB server pool status: After you enabling the server load balancing function, system will monitor the intranet servers and list the corresponding status and information.

Viewing SLB Server Status

To view the SLB server status, take the following steps:

1. Select **Policy** > **NAT** > **SLB Server Status**.
2. You can set the filtering conditions according to the virtual router, SLB server pool, and server address and then view the information.

Option	Description
Server	Shows the IP address of the server.
Port	Shows the port number of the server.
Status	Shows the status of the server.
Current Sessions	Shows the number of current sessions.
DNAT	Shows the DNAT rules that uses the server.
HA Group	Shows the HA group that the server belongs to.

Viewing SLB Server Pool Status

To view the SLB server pool status, take the following steps:

1. Select **Policy > NAT > SLB Server Pool Status**.

2. You can set the filtering conditions according to the virtual router, algorithm, and server pool name and then view the information.

Option	Description
Name	Shows the name of the server pool name.
Algorithm	Shows the algorithm used by the server pool.
DNAT	Shows the DNAT rules that use the server.
Abnormal Server/All Servers	Shows the number of abnormal servers and the total number of the servers.
Current Sessions	Shows the number of current sessions.

Session Limit

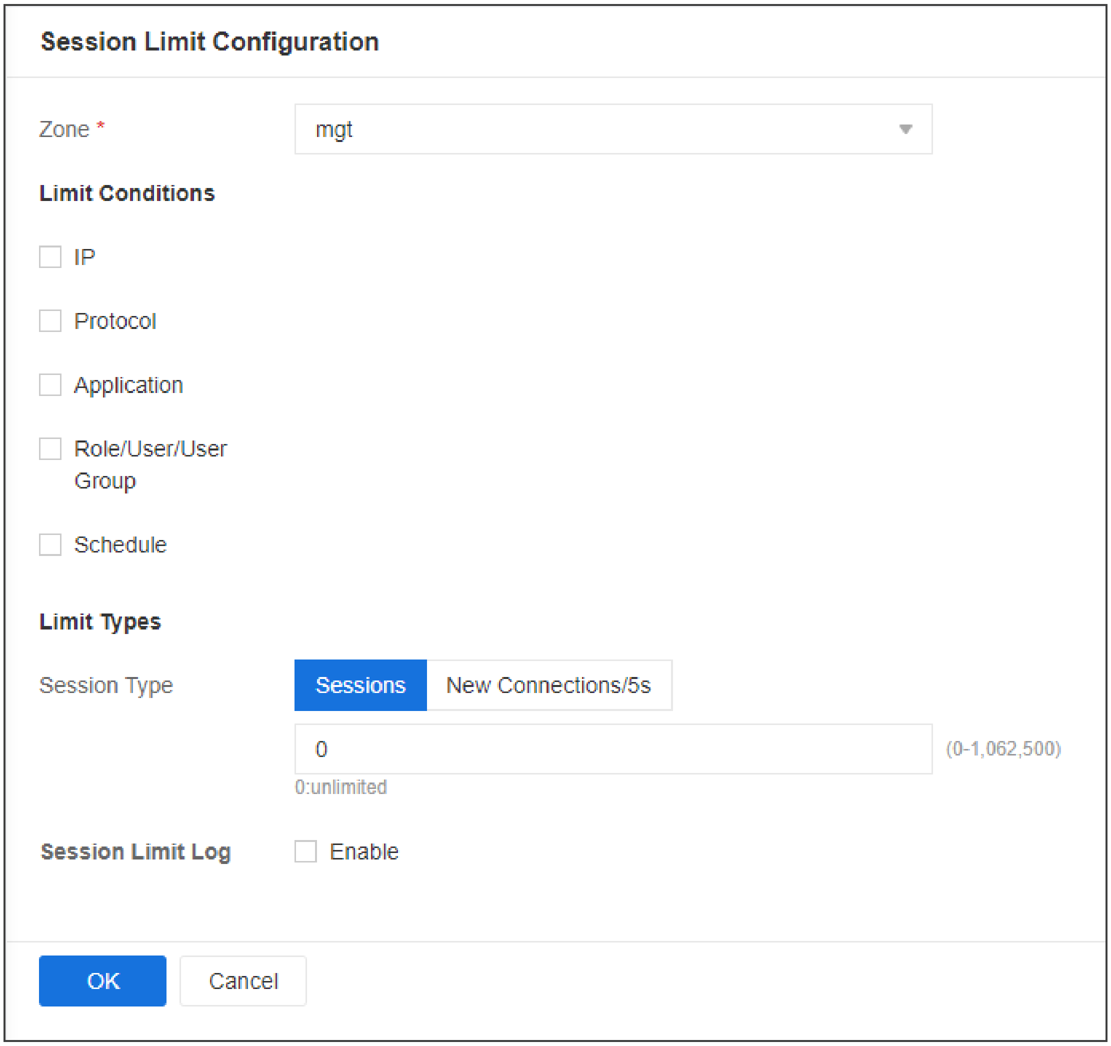
The devices support zone-based session limit function. You can limit the number of sessions and control the session rate to the source IP address, destination IP address, specified IP address, applications or role/user/user group, thereby protecting from DoS attacks and controlling the bandwidth of applications, such as IM or P2P.

Configuring a Session Limit Rule

To configure a session limit rule, take the following steps:

1. Select **Policy > Session Limit**.

2. Click **New**. The Session Limit Configuration page will appear.



Session Limit Configuration

Zone * mgt

Limit Conditions

□ IP

□ Protocol

□ Application

□ Role/User/User Group

□ Schedule

Limit Types

Session Type: [✓ Sessions] New Connections/5s

0 (0-1,062,500)

0:unlimited

Session Limit Log □ Enable

3. Select the zone where the session limit rule is located.

4. **Configure the limit conditions.**

IP	
Select the **IP** check box to configure the IP limit conditions.	
IP	Select the **IP** radio button and then select an IP address entry.

IP	
	• Select **All IPs** to limit the total number of sessions to all IP addresses. • Select **Per IP** to limit the number of sessions to each IP address.
Source IP	Select the **Source IP** radio button and specify the source IP address entry and destination IP address entry. When the session's source IP and destination IP are both within the specified range, system will limit the number of session as follows: • When you select **Per Source IP**, system will limit the number of sessions to each source IP address. • When you select **Per Destination IP**, system will limit the number of sessions to each destination IP address.
Protocol	
Protocol	Limits the number of sessions to the protocol which has been set in the text box.
Application	
Application	Limits the number of sessions to the selected application.
Role/User/User Group	
Select the **Role/User/User Group** check box to configure the corresponding limit conditions.	

IP	
Role	Select the **Role** radio button and a role from the **Role** drop-down list to limit the number of sessions of the selected role.
User	Select the **User** radio button and a user from the **User** drop-down list to limit the number of sessions of the selected user.
User Group	Select the **User Group** radio button and a user group from the **User Group** drop-down list to limit the number of sessions of the selected user group. • Next to the **User Group** radio button, select **All Users** to limit the total number of sessions to all of the users in the user group. • Next to the **User Group** radio button, select **Per User** to limit the number of sessions to each user.
Schedule	
Schedule	Select the **Schedule** check box and choose a schedule you need from the drop-down list to make the session limit rule take effect within the time period specified by the schedule.

5. **Configure the limit types.**

Session Type	
Session Number	Specify the maximum number of sessions. The value range is 0 to 1048576. The value of 0 indicates no lim-

Session Type	
	itation.
New Connections/5s	Specify the maximum number of sessions created per 5 seconds. The value range is 1 to 1048576.

6. Select the **Enable** after **Session Limit Log** to record the session limit log.

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

8. Click **Switch Mode** to select a matching mode. If you select **Use the Minimum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is limited to the minimum number of sessions of all matched session limit rules; if you select **Use the Maximum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is the maximum number of sessions of all matched session limit rlules.

Clearing Statistic Information

After configuring a session limit rule, the sessions which exceed the maximum number of sessions will be dropped. You can clear the statistical information of the dropped sessions of specified session limit rule according to your need.

To clear statistic information, take the following steps:

1. Select **Policy > Session Limit**.

2. Select the rule whose session's statistical information you want to clear.

3. Click **Clear**.

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.

Related Topics:

- "Configuring the Traffic Quota Rule" on Page 887
- "Configuring the Traffic Quota Profile" on Page 889
- "Configuring the Traffic Quota Zone" on Page 890
- "User Quota Monitor" on Page 1053

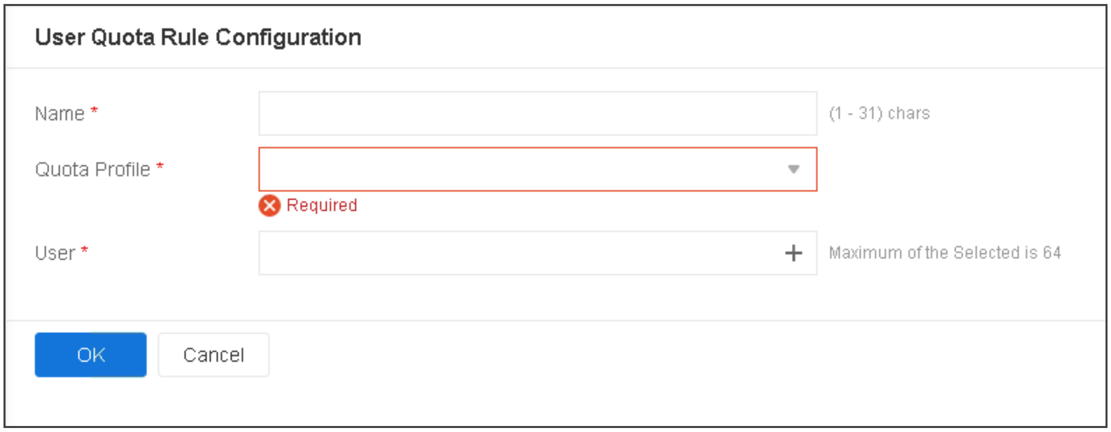
Configuring the Traffic Quota Rule

The traffic quota rule configuration including configuring user/ user group traffic quota rule and adjusting the traffic quota rule position.

Configuring the User/ User Group Traffic Quota Rule

To configure the user/ user group traffic quota rule, take the following steps:

1. Select **Policy** > **Traffic Quota** > **Rule**.
2. In the **User Quota Rule** or **User Group Quota Rule** tab, click **New**.



In the <User Traffic Quota Rule Configuration> or <User Group Traffic Quota Rule Configuration> page, configure the corresponding options.

Option	Description
Name	Specifies the name of user/ user group traffic quota rule.
Quota Profile	Select the created quota profile from the drop-down list, or click ⊕ to create a new traffic quota profile. For traffic quota profile configuration， see "Configuring the Traffic Quota Profile" on Page 889.

Option	Description
User/ User Group	Specifies the user/ user group of traffic quota rule. 1. From the **User** or **User Group** drop-down list, select the AAA server where the users and user groups reside. 2. Based on the type of AAA server, you can execute one or more actions: search a user/user group, expand the user/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add the them to the left pane. 4. After adding the desired objects, click **Close** to complete the user configuration.

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

Adjusting Traffic Quota Rule Priority

To adjust the rule priority, take the following steps:

1. Select **Policy** > **Traffic Quota** > **Rule**.

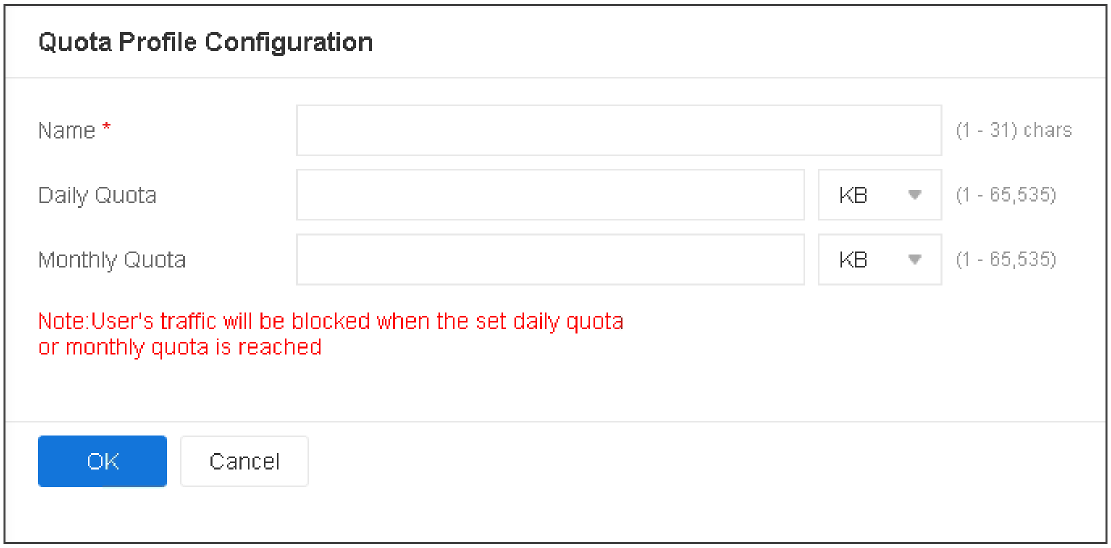
2. Select the check box of the traffic quota rule whose priority will be adjusted, and click **Priority** .

3. In the **Change User Quota Rule Priority**or **Change User Group Quota Rule Priority** page, click **First List** , **Last List** , **Before This Name** or **After This Name**. Then the rule will be moved before or after the specified name.

Configuring the Traffic Quota Profile

To configure the traffic quota profile, use the following steps:

1. Select **Policy** > **Traffic Quota** > **Profile**.
2. Click **New**to open the Quota Profile Configuration page.



Quota Profile Configuration

Name * (1 - 31) chars

Daily Quota KB (1 - 65,535)

Monthly Quota KB (1 - 65,535)

Note:User's traffic will be blocked when the set daily quota or monthly quota is reached

In the <Quota Profile Configuration> page, configure the corresponding options.

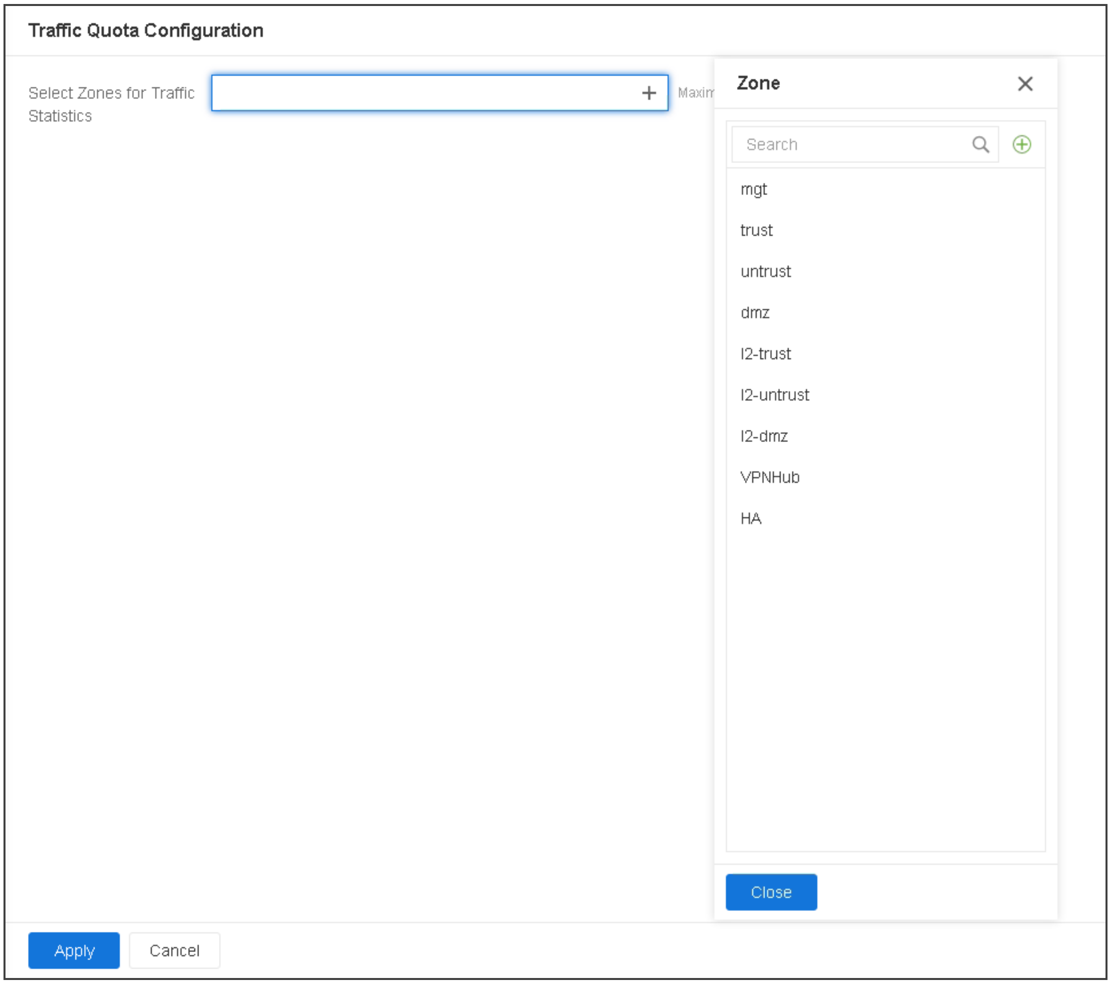
Option	Description
Name	Specifies the quota profile name.
Daily Quota	Type the daily quota in the text box and select the quota unit in the drop-down list, including KB, MB, GB, TB.
Monthly Quota	Type the monthly quota in the text box and select the quota unit in the drop-down list, including KB, MB, GB, TB.

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

Configuring the Traffic Quota Zone

To configure the zone that you want to enable the traffic quota function, take the following steps:

1. Select **Policy** > **Traffic Quota** > **Configuration**.
2. Click **Select Zones for Traffic Statistics**.



3. Click ⊕ to add a new zone entry to the **Selected** list.
4. In the **Selected** list, select the zone entry and click ✕ for the zone entry not be counted.
5. Click **Close** to save your settings.

Share Access

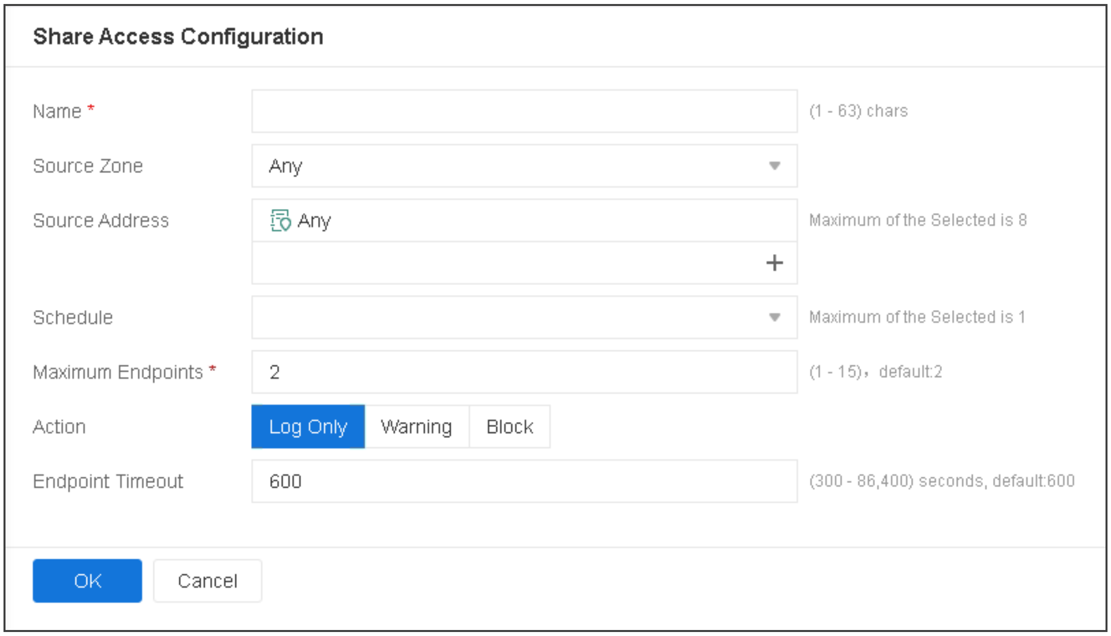
Share access means multiple endpoints access network with the same IP. The function of share access can block access from unknown device and allocate bandwidth for users, so as to prevent possible risks and ensure good online experience.

Configuring Share Access Rules

To configure a share access rule, take the following steps:

1. Select **Policy** > **Share Access**.

2. Click **New**. The Share Access Configuration page will appear.



Share Access Configuration

Name *		(1 - 63) chars
Source Zone	Any	
Source Address	Any	Maximum of the Selected is 8
Schedule		Maximum of the Selected is 1
Maximum Endpoints *	2	(1 - 15)，default:2
Action	Log Only	
Endpoint Timeout	600	(300 - 86,400) seconds, default:600

Option	Description
Name	Specifies the name of share access rule.
Source Zone	Specify the source zone of share access.
Source Address	Specify the source IP address segment of share access.

Option	Description
Schedule	Specify the schedule of share access. The share access rule takes effect in the period specified by the schedule. If the schedule is not configured, the share access rule will always be effective.
Maximum Endpoints	Specify the maximum number of share access endpoints. The range is 1-15. The default value is 2.
Action	When the number of endpoints with the same IP address exceeds the maximum allowed to be shared by system, the IP address of the endpoints will be processed according to the specified action. • Log Only: When the number of shared access endpoints exceeds the maximum, system will only record logs of the IP address out of limit, without affecting the normal connection of the access endpoints. • Warning: When the number of shared access endpoints exceeds the maximum, system will send warnings to endpoints out of limit and record logs during the specified control duration. • Control Duration: Specify the control duration of warning. The range is 30-3600s. The default value is 60s. After the duration is over, the system will re-detect whether the number of access endpoints exceeds the max-

Option	Description
	imum. • Warning Message: Specify the user-defined warning message, the range is 0-255 characters. • Block: When the number of shared access endpoints exceeds the maximum, system will block the IP address of the endpoints out of the limit and record logs during the specified control duration. • Control Duration: Specify the control duration of block. The range is 30-3600s. The default value is 60s. After the duration is over, the system will re-detect whether the number of access endpoints exceeds the maximum.
Endpoint Timeout	Specify the timeout time of endpoint. After the timeout time, when the endpoint no longer accesses network with the IP, system will clear the endpoint information. The range is 300-86400s. The default value is 600s.

ARP Defense

StoneOS provides a series of ARP defense functions to protect your network against various ARP attacks, including:

- ARP Learning: Devices can obtain IP-MAC bindings in an Intranet from ARP learning, and add them to the ARP list. By default this function is enabled. The devices will always keep ARP learning on, and add the learned IP-MAC bindings to the ARP list. If any IP or MAC address changes during the learning process, the devices will add the updated IP-MAC binding to the ARP list. If this function is disabled, only IP addresses in the ARP list can access the Internet.

- MAC Learning: Devices can obtain MAC-Port bindings in an Intranet from MAC learning, and add them to the MAC list. By default this function is enabled. The devices will always keep MAC learning on, and add the learned MAC-Port bindings to the MAC list. If any MAC address or port changes during the learning process, the devices will add the updated MAC-Port binding to the MAC list.

- IP-MAC-Port Binding: If IP-MAC, MAC-Port or IP-MAC-Port binding is enabled, packets that are not matched to the binding will be dropped to protect against ARP spoofing or MAC address list attacks. The combination of ARP and MAC learning can achieve the effect of "real-time scan + static binding", and make the defense configuration more simple and effective.

- Authenticated ARP: Authenticated ARP is implemented on the ARP client Hillstone Secure Defender. When a PC with Hillstone Secure Defender installed accesses the Internet via the interface that enables Authenticated ARP, it will perform an ARP authentication with the device, for the purpose that the MAC address of the device being connected to the PC is trusted.

- ARP Inspection: Devices support ARP Inspection for interfaces. With this function enabled, StoneOS will inspect all ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list.
- DHCP Snooping: With this function enabled, system can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and server.
- Host Defense: With this function enabled, the system can send gratuitous ARP packets for different hosts to protect them against ARP attacks.

Configuring ARP Defense

Configuring Binding Settings

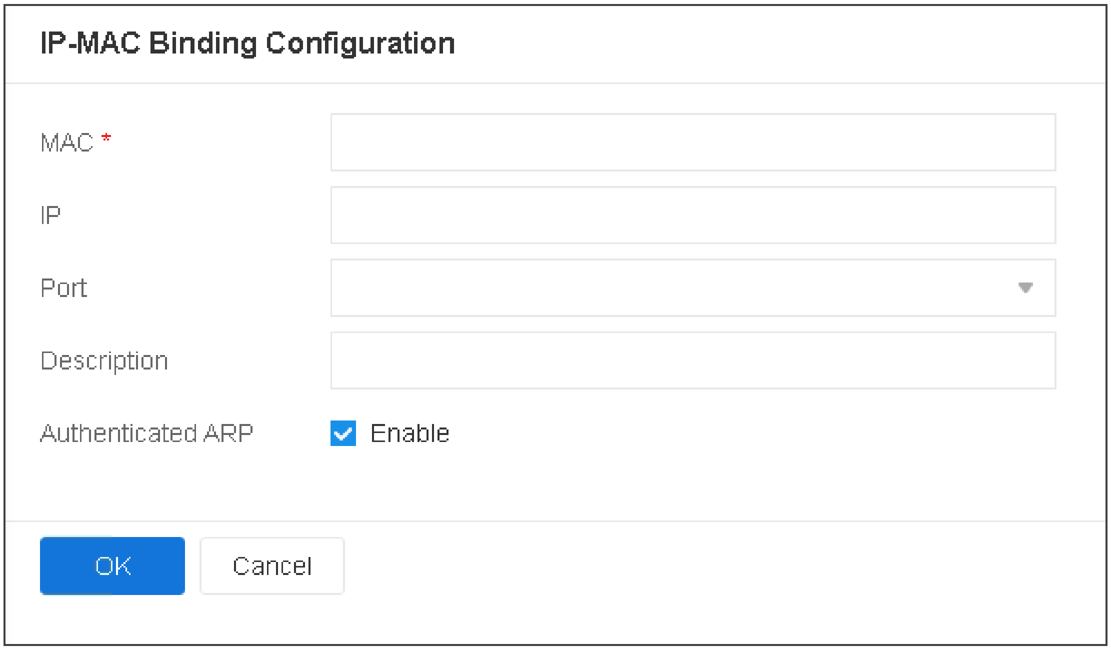
Devices support IP-MAC binding, MAC-Port binding and IP-MAC-Port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings.

Adding a Static IP-MAC-Port Binding

To add a static IP-MAC-Port binding, take the following steps:

1. Select **Policy** > **ARP Defense** > **IP-MAC Binding**.

2. Click **New**.



IP-MAC Binding Configuration

MAC *

IP

Port

Description

Authenticated ARP ☑ Enable

In the IP-MAC Binding Configuration page, configure the corresponding settings.

Option	Description
MAC	Specify a MAC address.
IP	Specify an IP address.
Port	Select a port from the drop-down list behind.
VLAN ID	If the port belongs to a VLAN, select the VLAN ID from the **VLAN ID** drop-down list.
Virtual Router	Select the virtual router that the binding item belongs to. By default, the binding item belongs to trust-vr.
Description	Specify the description for this item.
Authenticated ARP	Click the **Enable** button the authenticated ARP function.

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

Obtaining a Dynamic IP-MAC-Port Bindings

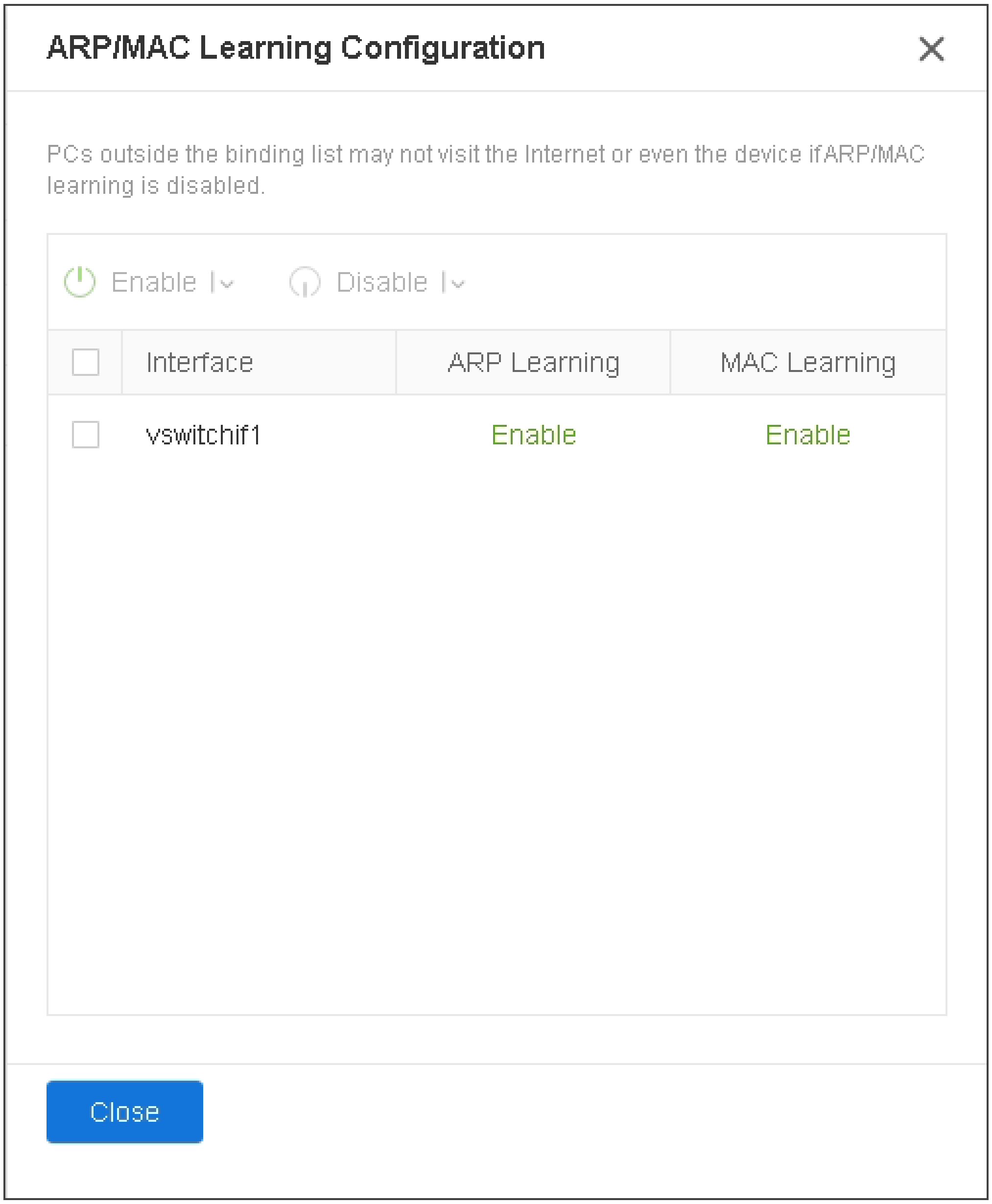
Devices can obtain dynamic IP-MAC-Port binding information from:

- ARP/MAC learning
- IP-MAC scan

To configure the ARP/MAC learning, take the following steps:

1. Select **Policy** > **ARP Defense** > **IP-MAC Binding**.

2. Click ⋮ and click **ARP/MAC Learning** from the pop-up menu.



PCs outside the binding list may not visit the Internet or even the device if ARP/MAC learning is disabled.

☐	Interface	ARP Learning	MAC Learning
☐	vswitchif1	Enable	Enable

3. In the ARP/MAC Learning Configuration page, select the interface that you want to enable the ARP/MAC learning function.

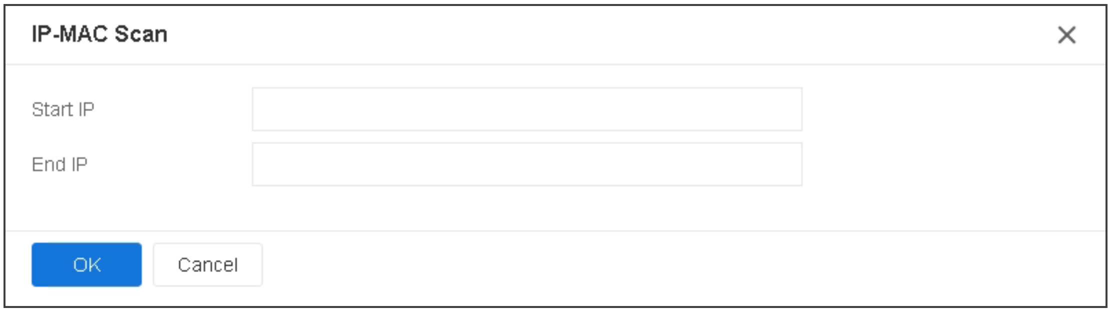
4. Click **Enable** and then select **ARP Learning** or **MAC Learning** in the pop-up menu. The system will enable the selected function on the interface you select.

5. Close the page and return to the IP-MAC Binding page.

To configure the ARP scan, take the following steps:

1. Select **Policy** > **ARP Defense** > **IP-MAC Binding**.

2. Select **Binding Configuration** and then click **IP-MAC Scan** from the pop-up menu.



3. In the IP-MAC Scan page, enter the start IP and the end IP.

4. Click **OK** to start scanning the specified IP addresses. The result will display in the table in the IP-MAC binding page.

Bind the IP-MAC-Port Binding Item

To bind the IP-MAC-Port binding item, take the following steps:

1. Select **Policy** > **ARP Defense** > **IP-MAC Binding**.

2. Select **Binding Configuration** and then click **Bind All** from the pop-up menu.

3. In the **Bind All** page, select the binding type.

4. Click **OK** to complete the configurations.

To unbind an IP-MAC-Port binding item:

1. Select **Policy** > **ARP Defense** > **IP-MAC Binding**.

2. Select **Binding Configuration** and then click **Unbind All** from the pop-up menu.

3. In the **Unbind All** page select the unbinding type.

4. Click **OK** to complete the configurations.

Importing/Exporting Binding Information

To import the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.

2. Select ⋮ and then click **Import** from the pop-up menu.

3. In the Import page, click **Browse** to select the file that contains the binding information. Only the UTF-8 encoding file is supported.

To export the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.

2. Select ⋮ and then click **Export** from the pop-up menu.

3. Choose the binding information type.

4. Click **OK** to export the binding information to a file.

Configuring Authenticated ARP

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The devices provide Authenticated ARP to protect the clients against ARP spoofing attacks. Authenticated ARP is implemented on the ARP client Hillstone Secure Defender. When a PC with Hillstone Secure Defender installed accesses the Internet via the interface that enables Authenticated ARP, it will perform an ARP authentication with the device to assure the MAC address of the device being connected to the PC is trusted. Besides. The ARP client is also designed with powerful anti-spoofing and anti-replay mechanisms to defend against various ARP attacks.

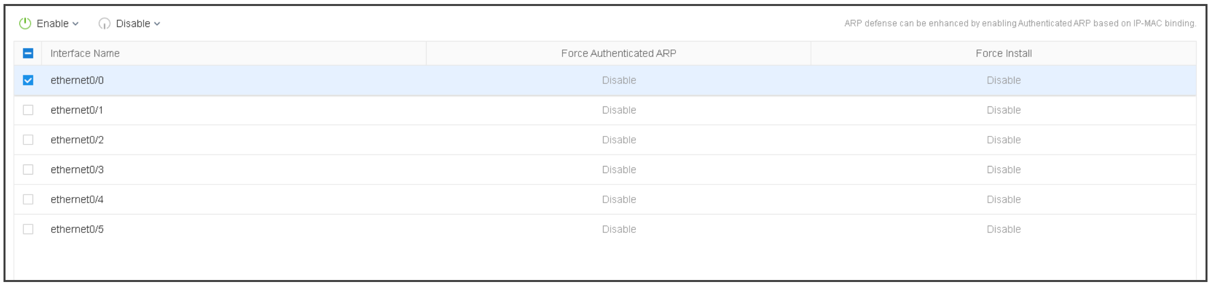
Notes: The Loopback interface and PPPoE sub-interface are not designed with ARP learning, so these two interfaces do not support Authenticated ARP.

To use the Authenticated ARP function, you need to enable the Authenticated ARP function in the device and install the Hillstone Secure Defender in the PCs.

To enable the Authenticated ARP in the device, take the following steps:

1. Select **Policy > ARP Defense > Authenticated ARP**.

2. Select the interfaces on which you want to enable the Authenticated ARP function.



ARP defense can be enhanced by enabling Authenticated ARP based on IP-MAC binding.

☐	Interface Name	Force Authenticated ARP	Force Install
☑	ethernet0/0	Disable	Disable
☐	ethernet0/1	Disable	Disable
☐	ethernet0/2	Disable	Disable
☐	ethernet0/3	Disable	Disable
☐	ethernet0/4	Disable	Disable
☐	ethernet0/5	Disable	Disable

3. Click **Enable** and select **Force Authenticated ARP** to enable the authenticated ARP function.

4. Enable or disable **Force Install** as needed. If the **Force Install** option is selected, PCs cannot access the Internet via the corresponding interface unless the ARP client has been installed; if the **Force Install** option is not selected, only PCs with the ARP client installed are controlled by Authenticated ARP.

To install Hillstone Secure Defender in the PCs, take the following steps:

1. Enable Authenticated ARP for an interface, and also select the **Force Install** option for the interface.

2. When a PC accesses the Internet via this interface, the Hillstone Secure Defneder's download page will pop up. Download HillstoneSecureDefender.exe as prompted.

3. After downloading, double-click **HillstoneSecureDefender.exe** and install the client as prompted by the installation wizard.

Configuring ARP Inspection

Devices support ARP Inspection for interfaces. With this function enabled, system will inspect all the ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list:

- If the IP address is in the ARP list and the MAC address matches, the ARP packet will be forwarded;
- If the IP address is in the ARP list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the ARP list, continue to check if the IP address is in the DHCP Snooping list;
- If the IP address is in the DHCP Snooping list and the MAC address also matches, the ARP packet will be forwarded;
- If the IP address is in the DHCP Snooping list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the DHCP Snooping, the ARP packet will be dropped or forwarded according to the specific configuration.

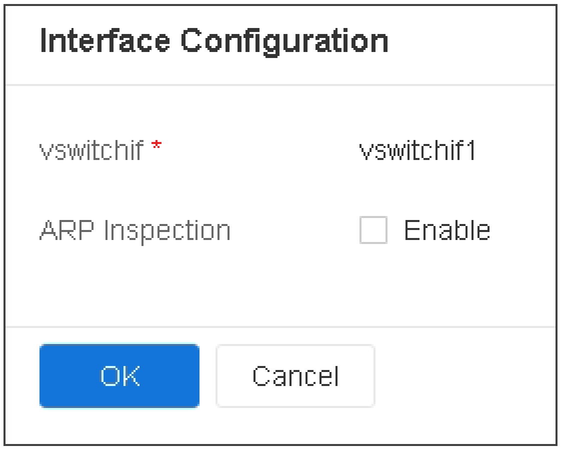
Both the VSwitch and VLAN interface of the system support ARP Inspection. This function is disabled by default.

To configure ARP Inspection of the VSwitch interface, take the following steps:

1. Select **Policy > ARP Defense > ARP Inspection**.

2. System already lists the existing VSwitch interfaces.

3. Double-click the item of a VSwitch interface.



Interface Configuration

vswitchif * vswitchif1

ARP Inspection □ Enable

4. In the Interface Configuration page, click the **Enable** button.

5. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.

6. Click **OK** to save the settings and close the page.

7. For the interfaces belonging to the VSwitch interface, you can set the following options:

   - If you do not need the ARP inspection in the interface, in the Advanced Options section, double-click the interface and select **Do Not Inspect** option in the pop-up page.

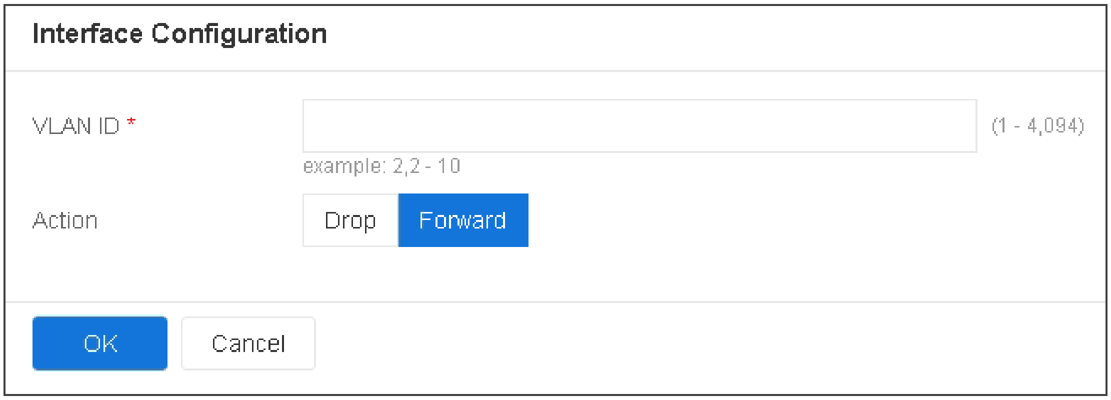
   - Configure the number of ARP packets received per second. When the ARP packet rate exceeds the specified value, the excessive ARP packets will be dropped. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

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

To configure the ARP inspection of the VLAN interface, take the following steps:

1. Select **Policy > ARP Defense > ARP Inspection**.

2. Click **New**.



3. In the Interface Configuration page, specify the VLAN ID.

4. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.

5. For the interfaces belongs to the VLAN, you can set the following options:

    - If you do not need the ARP inspection in the interface, in the Advanced Options section, double-click the interface and select **Do Not Inspect** option in the pop-up page.

    - Configure the number of ARP packets received per second. When the ARP packet rate exceeds the specified value, the excessive ARP packets will be dropped. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

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

Configuring DHCP Snooping

DHCP, Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for sub networks automatically. DHCP Snooping can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and the server. When ARP Inspection is also enabled, the system will check if an ARP packet passing through can be matched to any binding on the list. If not, the ARP packet will be dropped. In the network that allocates addresses via DHCP, you can prevent against ARP spoofing attacks by enabling ARP inspection and DHCP Snooping.

DHCP clients look for the server by broadcasting, and only accept the network configuration parameters provided by the first reachable server. Therefore, an unauthorized DHCP server in the network might lead to DHCP server spoofing attacks. The devices can prevent DHCP server spoofing attacks by dropping DHCP response packets on related ports.

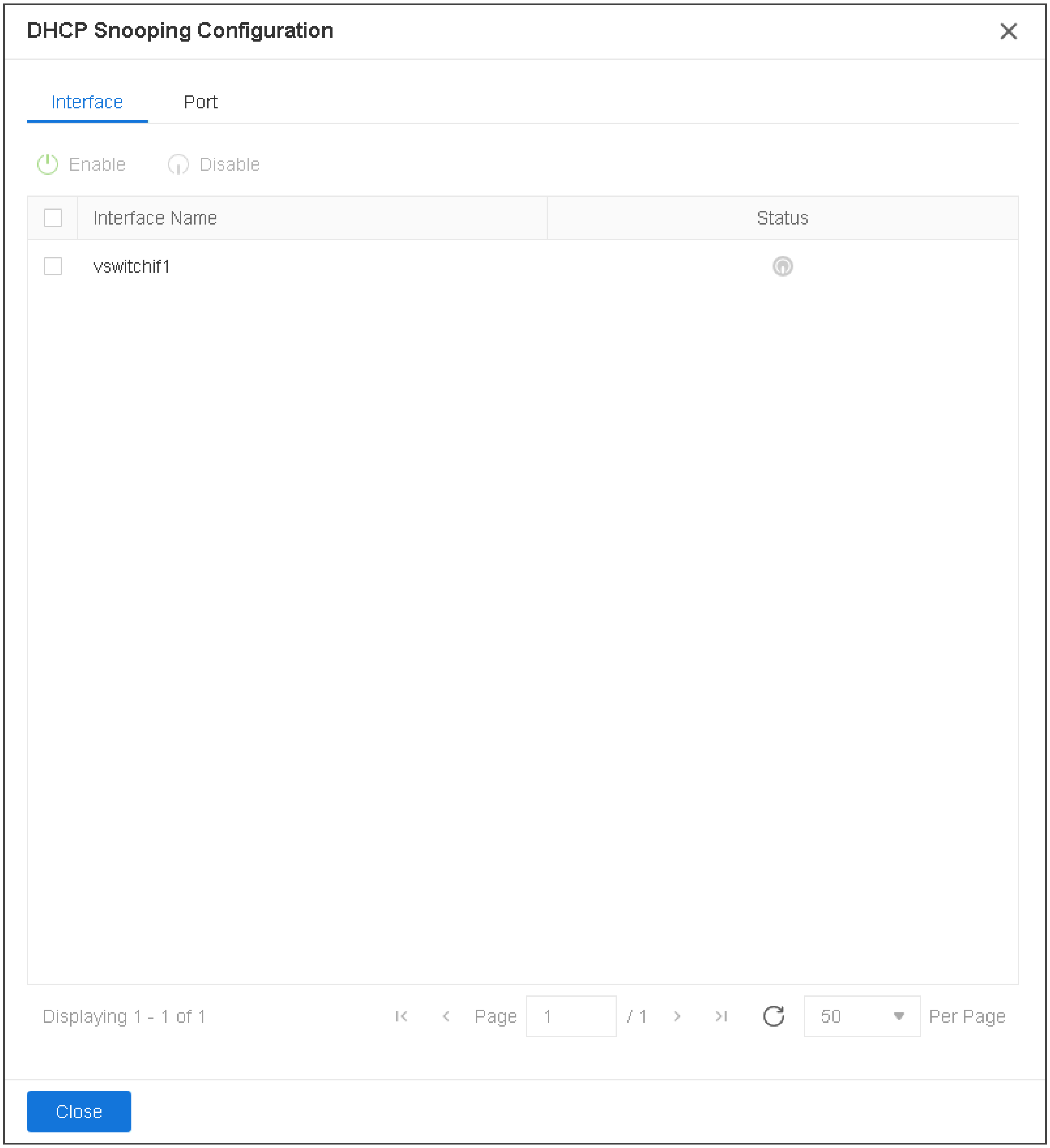
Besides, some malicious attackers send DHCP requests to a DHCP server in succession by forging different MAC addresses, and eventually lead to IP address unavailability to legal users by exhausting all the IP address resources. This kind of attacks is commonly known as DHCP Starvation. The devices can prevent against such attacks by dropping request packets on related ports, setting rate limit or enabling validity check.

The VSwitch interface of the system supports DHCP snooping. This function is disabled by default.

To configure DHCP snooping, take the following steps:

1. Select **Policy > ARP Defense > DHCP Snooping**.

2. Click **DHCP Snooping Configuration**.



DHCP Snooping Configuration

□	Interface Name	Status
□	vswitchif1	○

Displaying 1 - 1 of 1

3. In the Interface tab, select the interfaces that need the DHCP snooping function.

4. Click **Enable** to enable the DHCP snooping function.

5. In the Port tab, configure the DHCP snooping settings:

   - Validity check: Check if the client's MAC address of the DHCP packet is the same as the source MAC address of the Ethernet packet. If not, the packet will be dropped. Select the interfaces that need the validity check and then click **Enable** to enable this function.

   - Rate limit: Specify the number of DHCP packets received per second on the interface. If the number exceeds the specified value, system will drop the excessive DHCP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit. To configure the rate limit, double-click the interface and then specify the value in the **Rate** text box in the pop-up Port Configuration page.

   - Drop: In the Port Configuration page, if the **DHCP Request** check box is selected, the system will drop all of the request packets sent by the client to the server; if the **DHCP Response** check box is selected, system will drop all the response packets returned by the server to the client.

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

Viewing DHCP Snooping List

With DHCP Snooping enabled, system will inspect all of the DHCP packets passing through the interface, and create and maintain a DHCP Snooping list that contains IP-MAC binding information during the process of inspection. Besides, if the VSwitch, VLAN interface or any other Layer 3 physical interface is configured as a DHCP server, the system will create IP-MAC binding information automatically and add it to the DHCP Snooping list even if DHCP Snooping is not enabled. The bindings in the list contain information like legal users' MAC addresses, IPs, interfaces, ports, lease time, etc.

To view the DHCP snooping list, take the following steps:

1. Select **Policy** > **ARP Defense** > **DHCP Snooping**.

2. In the current page, you can view the DHCP snooping list.

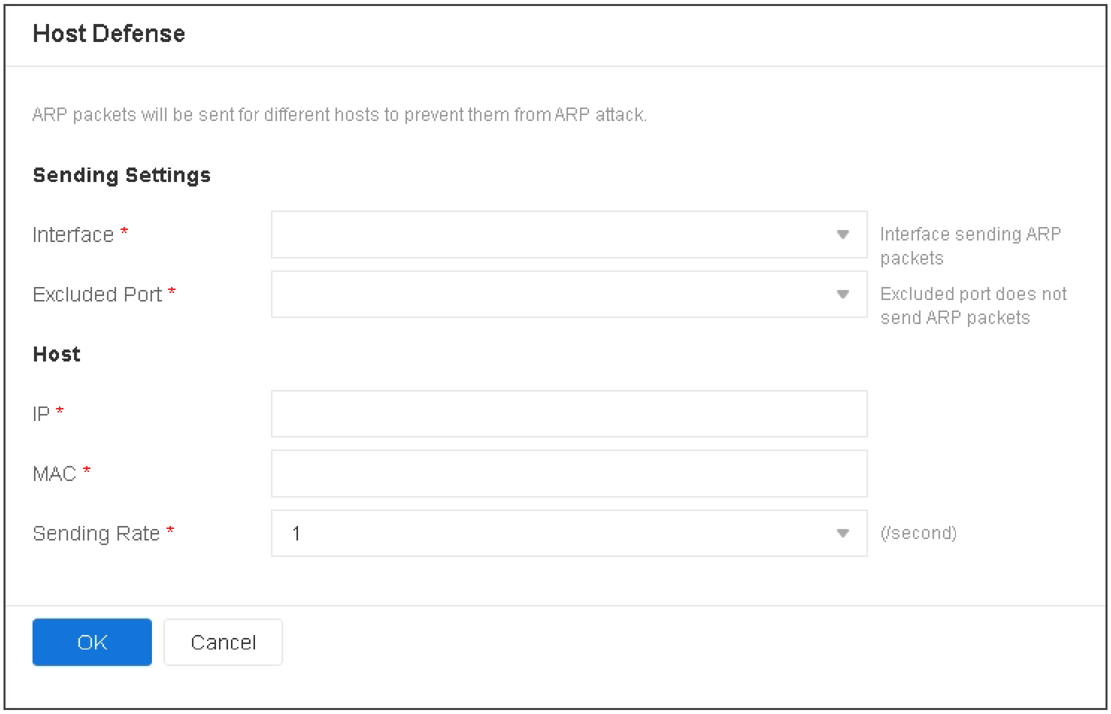
Configuring Host Defense

Host Defense is designed to send gratuitous ARP packets for different hosts to protect them against ARP attacks.

To configure host defense, take the following steps:

1. Select **Policy** > **ARP Defense** > **Host Defense**.

2. Click **New**.



Host Defense

ARP packets will be sent for different hosts to prevent them from ARP attack.

Sending Settings

Interface * — Interface sending ARP packets

Excluded Port * — Excluded port does not send ARP packets

Host

IP *

MAC *

Sending Rate * 1 (/second)

In the Host Defense page, configure the corresponding options.

Sending Settings	
Interface	Specify an interface that sends gratuitous ARP packets.

Sending Settings	
Excluded Port	Specify an excluded port, i.e., the port that does not send gratuitous ARP packets. Typically it is the port that is connected to the proxied host.
Host	
IP	Specify the IP address of the host that uses the device as a proxy.
MAC	Specify the MAC address of the host that uses the device as a proxy.
Sending Rate	Specify a gratuitous ARP packet that sends rate. The value range is 1 to 10/sec. The default value is 1.

3. Click **OK** to save your settings and return to the Host Defense page.

4. Repeat Step 2 and Step 3 to configure gratuitous ARP packets for more hosts. You can configure the device to send gratuitous ARP packets for up to 16 hosts.

Global Blacklist

After adding the IP addresses or services to the global blacklist, system will perform the block action to the IP address and service until the block duration ends. You can manually add IP addresses or services to the blacklist and system can also automatically add the IP addresses or services to the blacklist after you configure the IPS module.

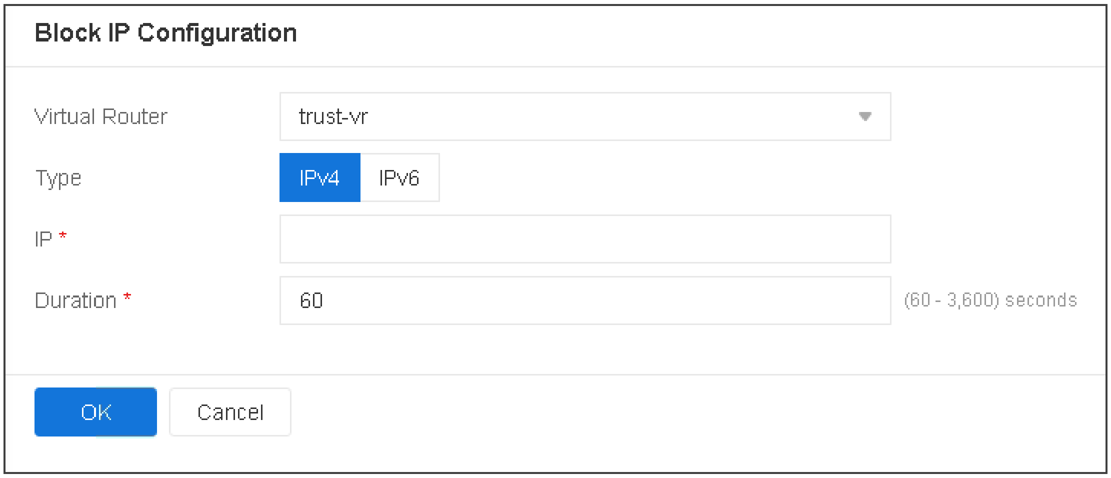
Configuring global blacklist includes IP block settings and service block settings, and both IPv4 and IPv6 address are supported.

Configuring IP Block Settings

To configure the IP block settings, take the following steps:

1. Select **Policy** > **Global Blacklist** > **IP Block**.

2. Click **New**. The Block IP Configuration page will appear.



Block IP Configuration

Virtual Router: trust-vr

Type: IPv4 | IPv6

IP *

Duration *: 60 (60 - 3,600) seconds

Configure the corresponding options.

Option	Description
Virtual Router	Select the virtual router that the IP address belongs to.

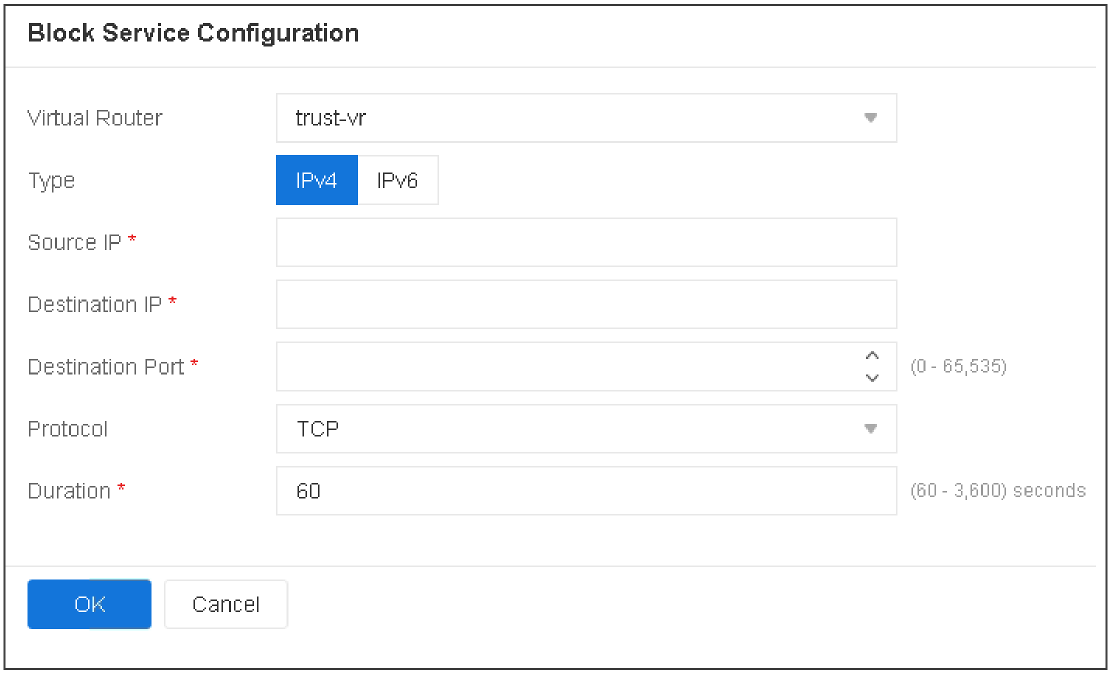
Option	Description
Type	Select the address type, including IPv4 and IPv6.
IP	Type the IP address that you want to block. This IP address can be not only the source IP address, but also the destination IP address.
Duration	Type the duration that the IP address will be blocked. The unit is second. The value ranges from 60 to 3600. The default value is 60.

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

Configuring Service Block Settings

To configure the service block settings, take the following steps:

1. Select **Policy** > **Global Blacklist** > **Service Block**.
2. Click **New**. The Block Service Configuration page will appear.



Block Service Configuration

Virtual Router	trust-vr
Type	IPv4 (selected) / IPv6
Source IP *	
Destination IP *	
Destination Port *	(0 - 65,535)
Protocol	TCP
Duration *	60 (60 - 3,600) seconds

Configure the corresponding options.

Option	Description
Virtual Router	Select the virtual router that the IP address belongs to.
Type	Select the address type, including IPv4 and IPv6.
Source IP	Type the source IP address of the blocked service. The service block function will block the service from the source IP address to the destination IP address.
Destination IP	Type the destination IP address of the blocked service.
Destination Port	Type the port number of the blocked service.
Protocol	Select the protocol of the blocked service.
Duration	Type the duration that the IP address will be blocked. The unit is second. The value ranges from 60 to 3600. The default value is 60.

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

Blacklist Global Configuration

To log the blacklist, take the following steps:

1. Select **Policy** > **Global Blacklist** > **Configuration**.
2. Click the **Enable** button, and system will log the hit blacklist traffic. If not, the log will not be logged.
3. Click **OK** to save the settings.

Chapter 11 Threat Prevention

Threat prevention is a device that can detect and block network threats. By configuring the threat prevention function, Hillstone devices can defend network attacks and reduce losses of the internal network.

Threat protections include:

- Anti Virus: It can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them.. Hillstone devices can detect protocol types of POP3, HTTP, SMTP, IMAP4 and FTP, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE , HTML, MAIL, RIFF and JPEG.
- Intrusion Prevention: It can detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
- Attack Defense: It can detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.
- Perimeter Traffic Filtering: It can filter the perimeter traffic based on known IP of black-/white list, and take block action on the malicious traffic that hits the blacklist.
- Botnet Prevention: It can detect botnet host in the internal network timely, as well as locate and take other actions according to the configuration, so as to avoid further threat attacks.

The threat protection configurations are based on security zones and policies.

- If a security zone is configured with the threat protection function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.

- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.

Notes:

- Threat protection is controlled by a license. To use Threat protection, apply and install the Threat Protection（TP） license, 、Anti Virus（AV）license orIntrusion Prevention System（IPS）license.

Threat Protection Signature Database

The threat protection signature database includes a variety of virus signatures, Intrusion prevention signatures, Perimeter traffic filtering signatures, . By default system updates the threat protection signature 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. Hillstone devices support auto updates and local updates. Non-root VSYS does not support updating signature database.

According to the severity, signatures can be divided into three security levels: critical, warning and informational. Each level is described as follows:

- Critical: Critical attacking events, such as buffer overflows.
- Warning: Aggressive events, such as over-long URLs.
- Informational: General events, such as login failures.

Anti-Virus

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The system is designed with an Anti-Virus that is controlled by licenses to provide an AV solution featuring high speed, high performance and low delay. With this function configured in StoneOS, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, etc., and proceed with the configured actions.

Anti-Virus function can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them. Hillstone devices can detect protocol types of POP3, HTTP, HTTPS, SMTP, IMAP4 and FTP, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE , HTML, MAIL, RIFF and JPEG.

If IPv6 is enabled, Anti-Virus function will detect files and protocols based on IPv6. How to enable IPv6, see StoneOS_CLI_User_Guide_IPv6.

The virus signature database includes over 10,000 signatures, and supports both daily auto update and real-time local update. See "Security Policy" on Page 768.

Notes: Anti-Virus is controlled by license. To use Anti-Virus , apply and install the Anti-Virus （AV） license.

Configuring Anti-Virus

This chapter includes the following sections:

- Preparation for configuring Anti-Virus function
- Configuring Anti-Virus function
- Configuring Anti-Virus global parameters

Preparing

Before enabling Anti-Virus, make the following preparations:

1. Make sure your system version supports Anti-Virus.
2. Import an Anti-Virus license and reboot. The Anti-Virus will be enabled after the rebooting.

Notes:

- You need to update the Anti-Virus signature database before enabling the function for the first time. To assure a proper connection to the default update server, you need to configure a DNS server for StoneOS before updating.
- Except M8860/M8260/M7860/M7360/M7260, if Anti-Virus is enabled, the max amount of concurrent sessions will decrease by half.

Configuring Anti-Virus Function

The Anti-Virus configurations are based on security zones or policies.

- If a security zone is configured with the Anti-Virus function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.

- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.

- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.

- To perform the Anti-Virus function on the HTTPS traffic, see the policy-based Anti-Virus.

To realize the zone-based Anti-Virus, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 74.

2. In the Zone Configuration page, expand Threat Protection.

3. Enable the threat protection you need and select an Anti-Virus rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list. To create an Anti-Virus rule, see Configuring_Anti-Virus_Rule.

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

To realize the zone-based Anti-Virus, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 768.

2. In the Policy Configuration page, expand the Protection tab.

3. Click the **Enable** button of **Anti-virus**. Then select an Anti-Virus rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create an Anti-Virus rule. For more information, see Configuring_Anti-Virus_Rule.

4. To perform the Anti-Virus function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the Anti-Virus function on the decrypted traffic.

   According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled Anti-Virus disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the Anti-Virus function on the decrypted traffic.
SSL proxy enabled Anti-Virus enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic.
SSL proxy disabled Anti-Virus enabled	System performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus profile. The HTTPS traffic will not be decrypted and the system will transfer it.

If the destination zone or the source zone specified in the security policy rule are configured with Anti-Virus as well, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy	Anti-Virus	System decrypts the HTTPS traffic

Policy Rule Configurations	Zone Configurations	Actions
enabled Anti-Virus disabled	enabled	according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the zone.
SSL proxy enabled Anti-Virus enabled	Anti-Virus enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the Anti-Virus function on the decrypted traffic according to the Anti-Virus rule of the policy rule.
SSL proxy disabled Anti-Virus enabled	Anti-Virus enabled	System performs the Anti-Virus function on the HTTP traffic according to the Anti-Virus rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

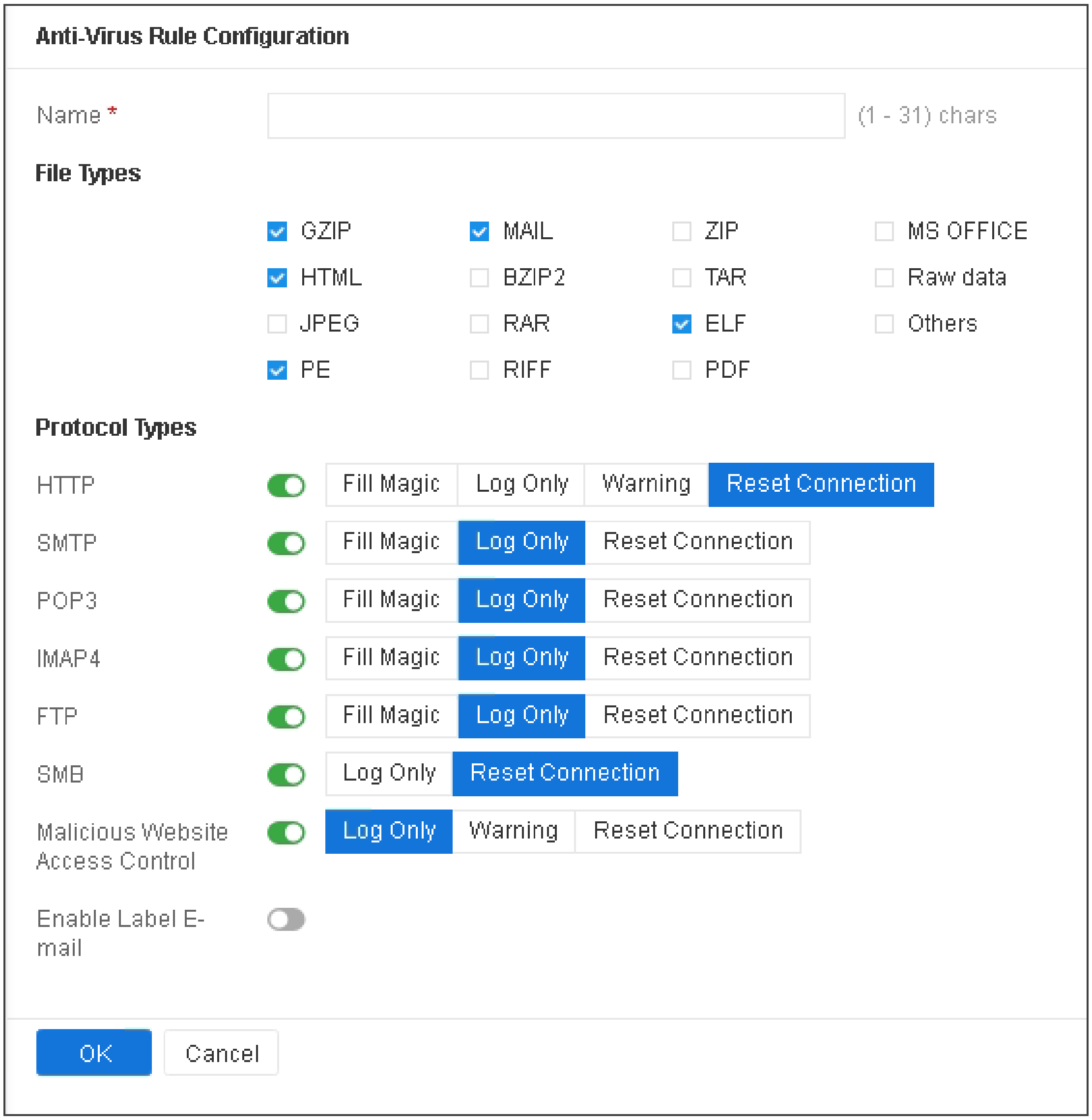
5. Click **OK** to save the settings.

Configuring an Anti-Virus Rule

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

1. Select **Object > Anti-Virus > Profile**.

2. Click **New**.



Anti-Virus Rule Configuration

Name * ____________________ (1 - 31) chars

File Types

☑ GZIP ☑ MAIL ☐ ZIP ☐ MS OFFICE
☑ HTML ☐ BZIP2 ☐ TAR ☐ Raw data
☐ JPEG ☐ RAR ☑ ELF ☐ Others
☑ PE ☐ RIFF ☐ PDF

Protocol Types

HTTP ☑ Fill Magic | Log Only | Warning | [✓ Reset Connection]
SMTP ☑ Fill Magic | [✓ Log Only] | Reset Connection
POP3 ☑ Fill Magic | [✓ Log Only] | Reset Connection
IMAP4 ☑ Fill Magic | [✓ Log Only] | Reset Connection
FTP ☑ Fill Magic | [✓ Log Only] | Reset Connection
SMB ☑ Log Only | [✓ Reset Connection]
Malicious Website Access Control ☑ [✓ Log Only] | Warning | Reset Connection
Enable Label E-mail ☐

In the Anti-Virus Rules Configuration page, enter the Anti-Virus rule configurations.

Option	Description
Name	Specifies the rule name.
File Types	Specifies the file types you want to scan. It can be GZIP,

Option	Description
	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.
Protocol Types	Specifies the protocol types (HTTP, SMTP, POP3, IMAP4, FTP) 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.
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.

Option	Description
	- 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.

Cloning an Anti-Virus Rule

System supports the rapid clone of an Anti-Virus rule. You can clone and generate a new Anti-Virus rule by modifying some parameters of the one current Anti-Virus rule.

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

1. Select **Object > Anti-Virus > Profile**.
2. Select an Anti-Virus rule in the list.
3. Click the **Clone** button above the list, and the **Name** configuration box will appear below the button. Then enter the name of the new Anti-Virus rule.
4. The cloned Anti-Virus rule will be generated in the list.

Configuring Anti-Virus Global Parameters

The Anti-Virus global parameters configuration includes:

- Enabling / Disabling the Anti-Virus function
- Configuring the decompression control function

Enabling / Disabling the Anti-Virus function

To enable / disable the Anti-Virus function, take the following steps:

1. Select **Object > Anti-Virus > Configuration**.
2. Click / clear the **Enable** button to enable / disable the Anti-Virus function.
3. Click **OK**.

Notes: After the configuration is completed, system must be rebooted to make it take effect。

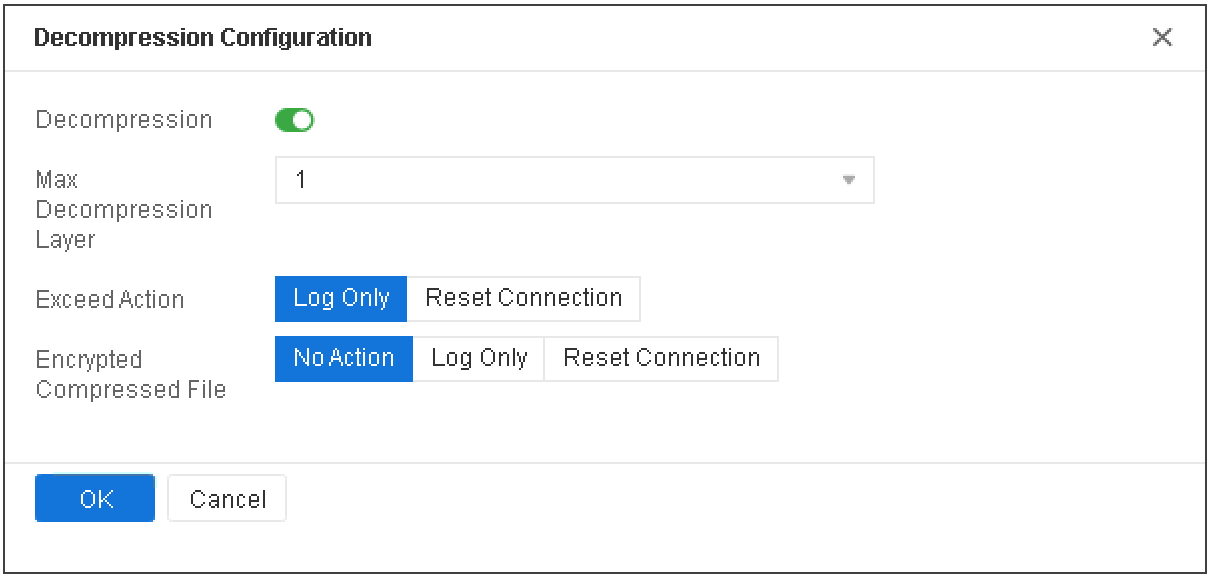
Configuring the Decompression Control Function

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. To configure the decompression control function, take the following steps:

1. Select **Object > Anti-Virus > Configuration**.

2. Click / clear the **Enable** button to enable / disable the Anti-Virus function.

3. Click **Configuration**.



Decompression Configuration

Decompression: ON

Max Decompression Layer: 1

Exceed Action: [✓ Log Only] Reset Connection

Encrypted Compressed File: [✓ No Action] Log Only Reset Connection

In the Decompression Configuration page, configure the following options.

Option	Description
Decompression	Click / clear the **Enable** button to enable / disable the decompression function.
Max Decompression Layer	By default, StoneOS can check the files of up to 5 decompression layers. To specify a decompression layer, select a value from the drop-down list. The value range is 1 to 5.
Exceed Action	Specifies an action for the compressed files that exceed the max decompression layer. Select an action from the drop-down list: • Log Only - Only generates logs but will not scan the files. This action is enabled by default. • Reset Connection - Resets connections for the files.
Encrypted Compressed File	Specifies an action for encrypted compressed files: • No Action - Will not take any actions against the files, but might further scan the files according to the Anti-Virus rule. • Log Only - Only generates logs but will not scan the files. • Reset Connection - Resets connections for the files.

4. Click **OK**.

Notes: For compressed files containing docx, pptx, xlsx, jar, and apk formats, when **Exceed Action** is specified as **Reset Connection**, the maximum compression layers should be added one more layer to prevent download failure.

Intrusion Prevention System

IPS, Intrusion Prevention System, is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration.

The IPS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, StoneOS will update the signature database automatically everyday to assure its integrity and accuracy.

- IPS will support IPv6 address if the IPv6 function is enabled.
- By integrating with the SSL proxy function, IPS can monitor the HTTPS traffic.

The protocol detection procedure of IPS consists of two stages: signature matching and protocol parse.

- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, system will process the traffic according to the action configuration. This part of detection is configured in the **Select Signature** section.
- Protocol parse: IPS analyzes the protocol part of the traffic. If the analysis results show the protocol part containing abnormal contents, system will process the traffic according to the action configuration. This part of detection is configured in the **Protocol Configuration** section.

Notes: Intrusion Prevention System is controlled by a license. To use Threat protection, apply and install the Intrusion Prevention System (IPS) license.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "00120" is the attacking signature ID. The 1st bit in the signature ID identifies protocol anomaly signatures, while the others identify attacking signatures. The mappings between IDs and protocols are shown in the table below:

ID	Protocol	ID	Protocol	ID	Protocol	ID	Protocol
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, Other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and Other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Configuring IPS

This chapter includes the following sections:

- Preparation for configuring IPS function
- Configuring IPS function

Preparation

Before enabling IPS, make the following preparations:

1. Make sure your system version supports IPS.
2. Import an Intrusion Prevention System (IPS) license and reboot. The IPS will be enabled after the rebooting.

> **Notes:** Except M8860/M8260/M7860/M7360/M7260, if IPS is enabled, the max amount of concurrent sessions will decrease by half.

Configuring IPS Function

The IPS configurations are based on security zones or policies.

- To perform the IPS function on the HTTPS traffic, see the policy-based IPS.

To realize the zone-based IPS, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 74.
2. In the Zone Configuration page, expand Threat Protection.

3. Enable the IPS you need and select an IPS rules from the profile drop-down list below, or you can click ⊕ from the profile drop-down list below. To create an IPS rule, see Configuring_an_IPS_Rule.

4. Click a direction (Inbound, Outbound, Bi-direction). The IPS rule will be applied to the traffic that is matched with the specified security zone and direction.

To realize the policy-based IPS, take the following steps:

1. Create a policy rule. For more inform action, refer to "Security Policy" on Page 768.

2. In the Policy Configuration page, expand Protection.

3. Click the **Enable** button of **IPS**. Then select an IPS rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create an IPS rule. For more information, see Configuring_an_IPS_Rule.

4. To perform the IPS function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the IPS function on the decrypted traffic.

   According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled IPS disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the IPS function on the decrypted traffic.
SSL proxy	System decrypts the HTTPS traffic according to the SSL

Policy Rule Configurations	Actions
enabledIPS enabled	proxy profile and performs the IPS function on the decrypted traffic.
SSL proxy disabled IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS profile. The HTTPS traffic will not be decrypted and system will transfer it.

If the destination zone or the source zone specified in the security policy rule is configured with IPS as well, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled IPS disabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the zone.
SSL proxy enabled IPS enabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the policy rule.
SSL proxy disabled IPS enabled	IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS rule of the policy rule. The HTTPS traffic

Policy Rule Configurations	Zone Configurations	Actions
		will not be decrypted and system will transfer it.

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

Configuring an IPS Rule

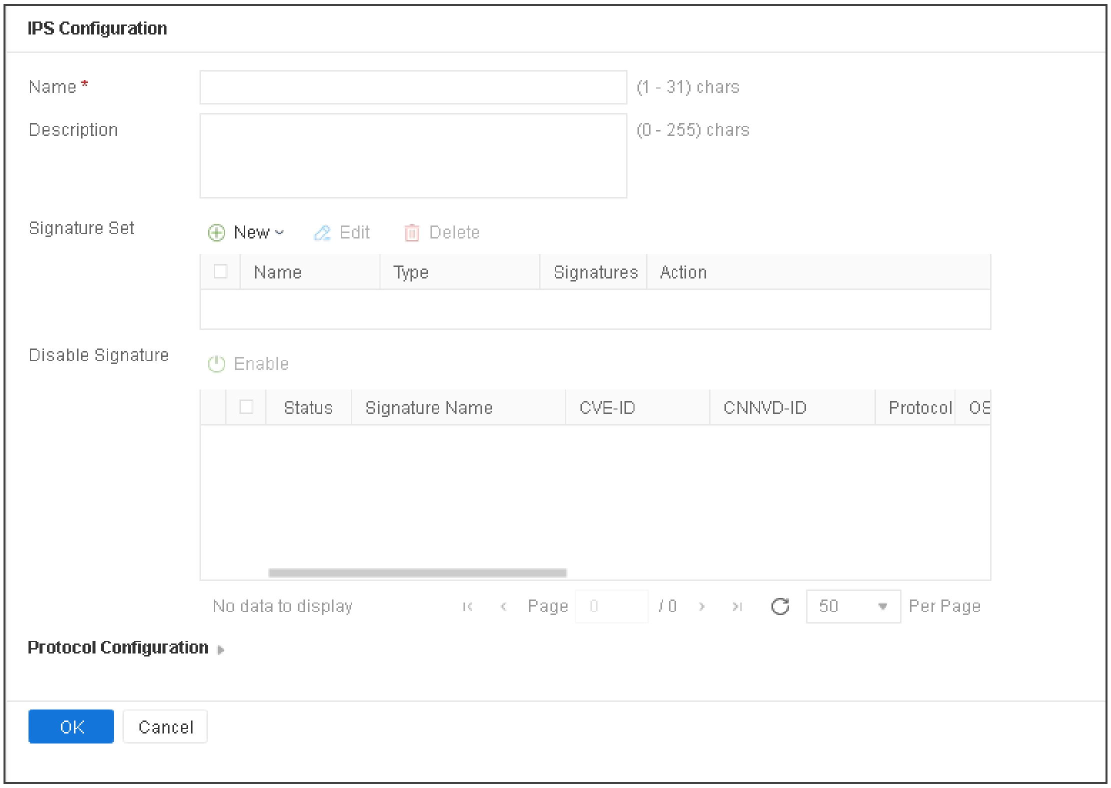
System has three default IPS rules: **predef_default** , **predef_loose** and **predef_critical**.

- The **predef_default** rule includes all the IPS signatures and its default action is reset.
- The **predef_loose** includes all the IPS signatures and its default action is log only.
- The **predef_critical** includes all the IPS signatures with high severity and its default action is log only.

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.



3. Type the name into the Rule name box.

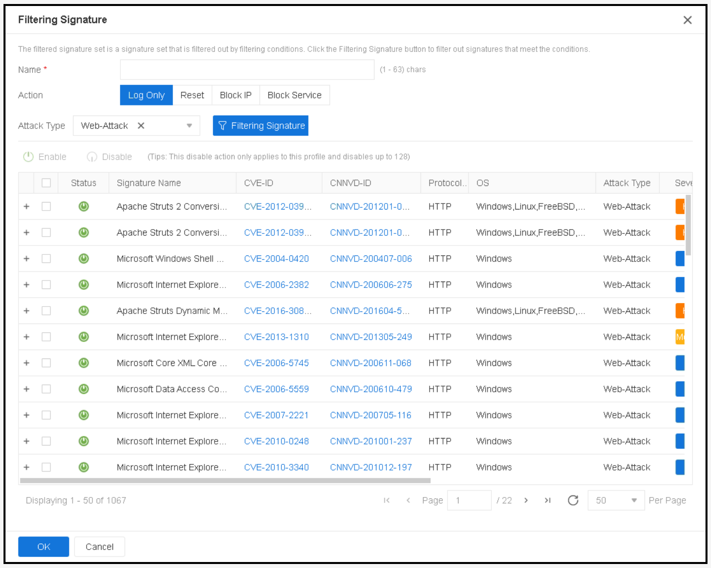
4. Type the description information into the **Description** text box.

5. 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**.

Click New to create a new signature set rule.

Option	Description
There are two methods: **Filtering Feature** and **Selection Feature**. Creating a new signature set contains:	

Option	Description
	- Name: Specify the name of signature. - Action: Specify the action performed on the abnormal traffic that match the signature set.
Methods	
Filter	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 105001 is in the Linux subcategory, the FreeBSD subcategory, and Other Linux subcategory at the same time. With Filter selected, system displays the main categories and subcategories above. You can select the subcategories to choose the signatures in this subcategory. As shown below, after selecting the Web Attack subcategory in the Attack Type main category, system will choose the signatures related to this subcategory. To view the detailed information of these chosen signatures, you can click the ID in the table. Click **Disable** or **Enable** 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.

Option	Description
	

Filtering Signature

The filtered signature set is a signature set that is filtered out by filtering conditions. Click the Filtering Signature button to filter out signatures that meet the conditions.

Name * (1 - 63) chars

Action: [✓ Log Only] Reset Block IP Block Service

Attack Type: Web-Attack ✕ | Filtering Signature

Enable Disable (Tips: This disable action only applies to this profile and disables up to 128)

	□	Status	Signature Name	CVE-ID	CNNVD-ID	Protocol..	OS	Attack Type	Seve
+	□	●	Apache Struts 2 Conversi...	CVE-2012-039...	CNNVD-201201-0...	HTTP	Windows,Linux,FreeBSD,...	Web-Attack	H
+	□	●	Apache Struts 2 Conversi...	CVE-2012-039...	CNNVD-201201-0...	HTTP	Windows,Linux,FreeBSD,...	Web-Attack	H
+	□	●	Microsoft Windows Shell ...	CVE-2004-0420	CNNVD-200407-006	HTTP	Windows	Web-Attack	
+	□	●	Microsoft Internet Explore...	CVE-2006-2382	CNNVD-200606-275	HTTP	Windows	Web-Attack	
+	□	●	Apache Struts Dynamic M...	CVE-2016-308...	CNNVD-201604-5...	HTTP	Windows,Linux,FreeBSD,...	Web-Attack	H
+	□	●	Microsoft Internet Explore...	CVE-2013-1310	CNNVD-201305-249	HTTP	Windows	Web-Attack	M
+	□	●	Microsoft Core XML Core ...	CVE-2006-5745	CNNVD-200611-068	HTTP	Windows	Web-Attack	
+	□	●	Microsoft Data Access Co...	CVE-2006-5559	CNNVD-200610-479	HTTP	Windows	Web-Attack	
+	□	●	Microsoft Internet Explore...	CVE-2007-2221	CNNVD-200705-116	HTTP	Windows	Web-Attack	
+	□	●	Microsoft Internet Explore...	CVE-2010-0248	CNNVD-201001-237	HTTP	Windows	Web-Attack	
+	□	●	Microsoft Internet Explore...	CVE-2010-3340	CNNVD-201012-197	HTTP	Windows	Web-Attack	

Displaying 1 - 50 of 1067 Page 1 / 22 50 Per Page

OK Cancel

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.
Action	
Log Only	Record a log.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Reset</td><td>Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.</td></tr>
<tr><td>Block IP</td><td>Block the IP address of the attacker. Specify a block duration. The value range is 60 to 3600 seconds, and the default value is 60.</td></tr>
<tr><td>Block Service</td><td>Block the service of the attacker. Specify a block duration. The value range is 60 to 3600 seconds, and the default value is 60.</td></tr>
<tr><td colspan="2"><b>Note</b>: 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. 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.
• The action of the signature set created by Search Condition has higher priority than the action of the signature set created by Filter.</td></tr>
</table>

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

7. In the Disabled Signature area, 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.

8. In the Protocol Configuration area, click ◀ . The protocol configurations specify the requirements that the protocol part of the traffic must meet. If the protocol part contains abnormal contents, system will process the traffic according to the action 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
HTTP	**Max Scan Length**: Specify the maximum length of scanning when scanning the HTTP packets. **Banner Detection**: Click the **Enable** button to enable protection against HTTP 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 HTTP packets. If abnormal contents exist, you can: • 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

Option	Description
	of the attacker and specify a block duration. **Max URI Length**: Specify a max URI length for the HTTP protocol. If the URI length exceeds the limitation, you can: • 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. **Allowed Methods**: Specify the allowed HTTP methods.

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

Protecting the Web server means system can detect the following attacks: SQL injection, XSS injection, external link check, ACL, and HTTP request flood and take actions when detecting them. A pre-defined Web server protection rule named **default** is built in. By default, this protection rule is enabled and cannot be disabled or deleted.

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

Option	Description
	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 Con-

Option	Description
	figuration 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.
SQL Injection Protection	Click the Enable button to enable SQL injection check. • Action: Log Only - Record a log. Rest - Reset

Option	Description
	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. • Sensitivity: Specifies the sensitivity for the SQL injection protection function. The higher the sensitivity is, the lower the false negative rate is. • 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. • 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. • Sensitivity: Specifies the sensitivity for the XSS injection protection function. The higher the

Option	Description
	sensitivity is, the lower the false negative rate is. • Check point: Specifies the check point for the XSS injection check. It can be Cookie, Cookie2, Post, Referer or URI.
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. • 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.

Option	Description
	- 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

Option	Description
	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 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.

Option	Description
	- 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. - For the protected full URL, when the number of HTTP connecting request per second towards this URL reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack towards this URL, and will enable the HTTP request flood protection. - Full URL: Enter the full URLs to protect particular URLs. Click this link to configure the URLs, for example, www.example.com/index.html. When protecting a particular URL, you can select a statistic object. 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

Option	Description
	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: • Auto (JS Cookie): The Web browser will

Option	Description
	finish the 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: 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,

Option	Description
	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 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. • White List: Specifies the white list for the HTTP request flood protection. The source IP added to the white list will not check the HTTP request flood protection.

In the DNS tab, configure the following settings:

Option	Description
DNS	**Max Scan Length**: Specify the maximum length of scanning when scanning the DNS packets.

Option	Description
	Protocol Anomaly Detection: Select **Enable** to analyze the DNS packets. If abnormal contents exist, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or send the 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.

In the FTP tab, configure the following settings:

Option	Description
FTP	**Max Scan Length**: Specify the maximum length of scanning when scanning the FTP packets. **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: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block

Option	Description
	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. **Max Command Line Length**: Specifies a max length (including carriage return) for the FTP command line. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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 **Max Response Line Length**: Specifies a max length for the FTP response line.If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block

Option	Description
	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. **Action for Brute-force**: If the login attempts per minute 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. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • 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. • Block Time - Specifies the block duration.

In the MSRPC tab, configure the following settings:

Option	Description
MSRPC	**Max Scan Length**: Specify the maximum length of scanning when scanning the MSRPC packets. **Protocol Anomaly Detection**: Select **Enable** to analyze

Option	Description
	the MSRPC packets. If abnormal contents exist, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max bind length**: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max request length**: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Action for Brute-force**: If the login attempts per minute

Option	Description
	fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the configuration. Select the Enable check box to enable brute-force. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • 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. • Block Time - Specifies the block duration.

In the POP3 tab, configure the following settings:

Option	Description
POP3	**Max Scan Length**: Specify the maximum length of scanning when scanning the POP3 packets. **Protocol Anomaly Detection**: Click the Enable button to analyze the POP3 packets. If abnormal contents exist, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreachable packets (UDP) and also generate logs. Block

Option	Description
	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. **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. **Max Command Line Length**: Specifies a max length (including carriage return) for the POP3 command line. If the length exceeds the limits, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max Parameter Length**: Specifies a max length for the POP3 client command parameter. If the length exceeds the limits, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates logs. Block IP - Block the IP address of the attacker and specify a

Option	Description
	block duration. Block Service - Block the service of the attacker and specify a block duration. **Max failure time**: Specifies a max failure time (within one single POP3 session) for the POP3 server. If the failure time exceeds the limits, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Action for Brute-force**: If the login attempts per minute 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. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • 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.

Option	Description
	- Block Time - Specifies the block duration.

In the SMTP tab, configure the following settings:

Option	Description
SMTP	**Max Scan Length**: Specify the maximum length of scanning when scanning the SMTP packets.**Protocol Anomaly Detection**: Click **Enable** to analyze the SMTP packets. If abnormal contents exist, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **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. **Max Command Line Length**: Specifies a max length (including carriage return) for the SMTP command line. If the length exceeds the limits, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the destination unreach-

Option	Description
	able 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. **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: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max Reply Line Length**: Specifies a max length reply length for the SMTP server. If the length exceeds the limits, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max Text Line Length**: Specifies a max length for the E-mail text of the SMTP client. If the length exceeds the

Option	Description
	limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max Content Type Length**: Specifies a max length for the content-type of the SMTP protocol. If the length exceeds the limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Max Content Filename Length**: Specifies a max length for the filename of E-mail attachment. If the length exceeds the limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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 ser-

Option	Description
	vice of the attacker and specify a block duration. **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: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Action for Brute-force**: If the login attempts per minute 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. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • 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. • Block Time - Specifies the block duration.

In the SUNRPC tab, configure the following settings:

Option	Description
SUNRPC	**Max Scan Length**: Specify the maximum length of scanning when scanning the SUNRPC packets. **Protocol Anomaly Detection**: Click **Enable** to analyze the SUNRPC packets. If abnormal contents exist, you can: • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Action for Brute-force**: If the login attempts per minute 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. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication / login failure count per minute. • 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.

Option	Description
	- Block Time - Specifies the block duration.

In the Telnet tab, configure the following settings:

Option	Description
Telnet	**Max Scan Length**: Specify the maximum length of scanning when scanning the Telnet packets.**Protocol Anomaly Detection**: Click **Enable** to analyze the Telnet packets. If abnormal contents exist, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends the 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. **Username/Password Max Length**: Specifies a max length for the username and password used in Telnet. If the length exceeds the limits, you can: - Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generates 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. **Action for Brute-force**: If the login attempts per minute

Option	Description
	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. Non-root VSYS does not support this option. • Login Threshold per Min - Specifies a permitted authentication/login failure count per minute. • 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. • Block Time - Specifies the block duration.

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

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

Cloning an IPS Rule

System supports the rapid cloning of an IPS rule. The user can generate a new IPS rule by modifying some parameters of the cloned IPS rule.

To clone an IPS rule, take the following steps:

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

2. Select an IPS rule in the list.

3. Click **Clone** above the list, the **Name** configuration box will appear below the button, enter

the name of the cloned IPS rule.

4. A cloned IPS rule will be generated in the list.

IPS Global Configuration

Configuring the IPS global settings includes:

- Enable the IPS function
- Specify how to merge logs
- Specify the work mode

Click **Object > Intrusion Prevention System > Configuration** to configure the IPS global settings.

Option	Description
IPS	Click/clear the **Enable** button to enable/disable the IPS function.
Log Aggregate Type	System can merge IPS logs which have the same protocol ID, the same VSYS ID, the same Signature ID, the same log ID, and the same merging type. Thus it can help reduce the number of logs and avoid receiving redundant logs. The function is disabled by default. Select the merging types in the drop-down list: • Do Not Merge - Do not merge any logs. • Source IP - Merge the logs with the same Source IP. • Destination IP - Merge the logs with the same Destination IP.

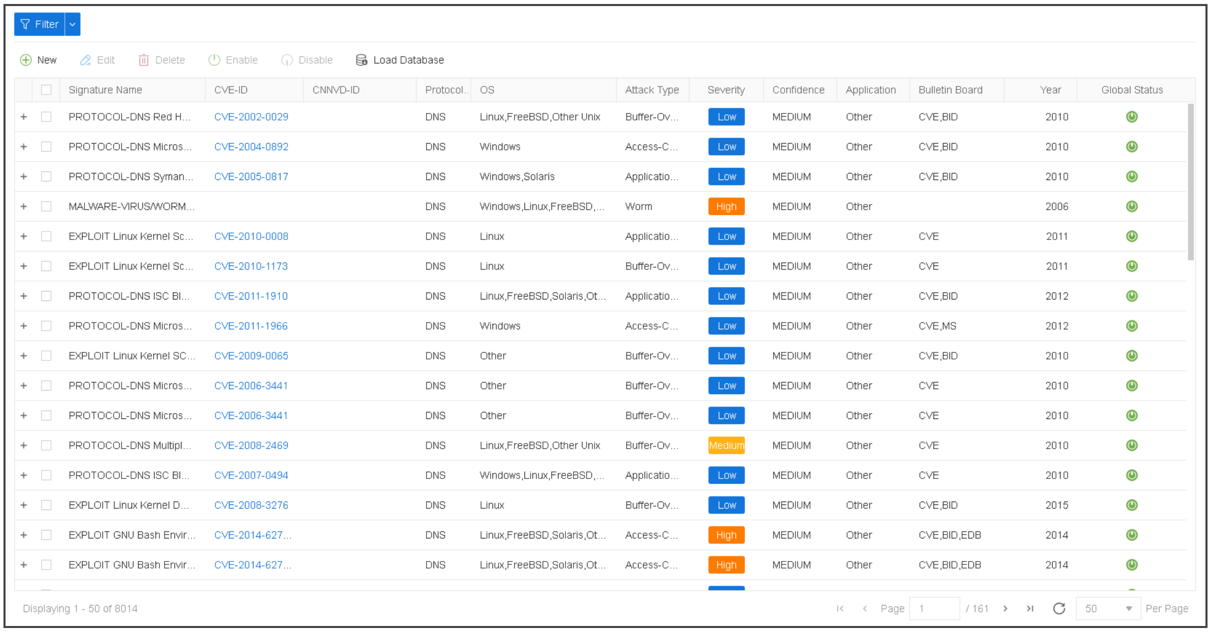
Option	Description
	• Source IP, Destination IP - Merge the logs with the same Source IP and the same Destination IP.
Aggregate Time	Specifies the time granularity for IPS threat log of the same merging type (specified above) to be stored in the database. At the same time granularity, the same type of log is only stored once. It ranges from 10 to 600 seconds.
Mode	Specifies a working mode for IPS: • IPS - If attacks have been detected, StoneOS will generate logs, and will also reset connections or block attackers. This is the default mode. • Log only - If attacks have been detected, StoneOS will only generate logs, but will not reset connections or block attackers.

After the configurations, click **OK** to save the settings.

Notes: Non-root VSYS does not support IPS global configuration.

Signature List

Select **Object** > **Intrusion Prevention System** > **Signature List**. You can see the signature list.



	□	Signature Name	CVE-ID	CNNVD-ID	Protocol..	OS	Attack Type	Severity	Confidence	Application	Bulletin Board	Year	Global Status
+	□	PROTOCOL-DNS Red H...	CVE-2002-0029		DNS	Linux,FreeBSD,Other Unix	Buffer-Ov...	Low	MEDIUM	Other	CVE,BID	2010	⏻
+	□	PROTOCOL-DNS Micros...	CVE-2004-0892		DNS	Windows	Access-C...	Low	MEDIUM	Other	CVE,BID	2010	⏻
+	□	PROTOCOL-DNS Syman...	CVE-2005-0817		DNS	Windows,Solaris	Applicatio...	Low	MEDIUM	Other	CVE,BID	2010	⏻
+	□	MALWARE-VIRUS/WORM...			DNS	Windows,Linux,FreeBSD,...	Worm	High	MEDIUM	Other		2006	⏻
+	□	EXPLOIT Linux Kernel Sc...	CVE-2010-0008		DNS	Linux	Applicatio...	Low	MEDIUM	Other	CVE	2011	⏻
+	□	EXPLOIT Linux Kernel Sc...	CVE-2010-1173		DNS	Linux	Buffer-Ov...	Low	MEDIUM	Other	CVE	2011	⏻
+	□	PROTOCOL-DNS ISC BI...	CVE-2011-1910		DNS	Linux,FreeBSD,Solaris,Ot...	Applicatio...	Low	MEDIUM	Other	CVE,BID	2012	⏻
+	□	PROTOCOL-DNS Micros...	CVE-2011-1966		DNS	Windows	Access-C...	Low	MEDIUM	Other	CVE,MS	2012	⏻
+	□	EXPLOIT Linux Kernel SC...	CVE-2009-0065		DNS	Other	Buffer-Ov...	Low	MEDIUM	Other	CVE,BID	2010	⏻
+	□	PROTOCOL-DNS Micros...	CVE-2006-3441		DNS	Other	Buffer-Ov...	Low	MEDIUM	Other	CVE	2010	⏻
+	□	PROTOCOL-DNS Micros...	CVE-2006-3441		DNS	Other	Buffer-Ov...	Low	MEDIUM	Other	CVE	2010	⏻
+	□	PROTOCOL-DNS Multipl...	CVE-2008-2469		DNS	Linux,FreeBSD,Other Unix	Buffer-Ov...	Medium	MEDIUM	Other	CVE	2010	⏻
+	□	PROTOCOL-DNS ISC BI...	CVE-2007-0494		DNS	Windows,Linux,FreeBSD,...	Applicatio...	Low	MEDIUM	Other	CVE	2010	⏻
+	□	EXPLOIT Linux Kernel D...	CVE-2008-3276		DNS	Linux	Buffer-Ov...	Low	MEDIUM	Other	CVE,BID	2015	⏻
+	□	EXPLOIT GNU Bash Envir...	CVE-2014-627...		DNS	Linux,FreeBSD,Solaris,Ot...	Access-C...	High	MEDIUM	Other	CVE,BID,EDB	2014	⏻
+	□	EXPLOIT GNU Bash Envir...	CVE-2014-627...		DNS	Linux,FreeBSD,Solaris,Ot...	Access-C...	High	MEDIUM	Other	CVE,BID,EDB	2014	⏻

Displaying 1 - 50 of 8014

The upper section is for searching signatures. The lower section is for managing signatures.

Searching Signatures

In the upper section, click **Filter** to set the search conditions to search the signatures that match the condition.

To clear all search conditions, click **Remove All**. To save the search conditions, click ⌄ and then click **Save Filters** to name this set of search conditions and save it.

Managing Signatures

You can view signatures, create a new signature, load the database, delete a signature, edit a signature, enable a signature, and disable a signature.

- View signatures: In the signature list, click the "+" button before the ID of a signature to view the details.
- Create a new signature: click **New**.

  In the User-defined Signature page, configure the following settings:

Option	Description
Name	Specifies the signature name.
Description	Specifies the signature descriptions.
Protocol	Specifies the affected protocol.
Flow	Specifies the direction. - To_Server means the package of attack is from the server to the client. - To_Client means the package of attack is from the client to the server. - Any includes To_Server and To_Client.
Source Port	Specifies the source port of the signature. - Any - Any source port. - Included - The source port you specified should be included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate. - Excluded - The source port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Destination Port	Specifies the destination port of the signature. - Any - Any destination port.

Option	Description
	- Included - The destination port you specified should be included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate. - Excluded - The destination port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Dsize	Specifies the payload message size. Select "----",">", "<" or "=" from the drop-down list and specifies the value in the text box. "----" means no setting of the parameters.
Severity	Specifies the severity of the attack.
Attack Type	Select the attack type from the drop-down list.
Application	Select the affected applications. "----" means all applications.
Operating System	Select the affected operating system from the drop-down list. "----" means all the operating systems.
Bulletin Board	Select a bulletin board of the attack.
Year	Specifies the released year of attack.
Detection Filter	Specifies the frequency of the signature rule. - Track - Select the track type from the drop-down

Option	Description
	list. It can be **by_source** or **by_destination**. System will use the statistic of the source IP or the destination IP to check whether the attack matches this rule. - Count - Specifies the maximum times the rule occurs in the specified time. If the attacks exceed the Count value, system will trigger rules and act as specified. - Seconds - Specifies the interval value of the rule occurs.

Configure Content, click New to specify the content of the signature:

Option	Description
Content	Specifies the signature content. Select the following check box if needed: - HEX - Means the content is hexadecimal. - Case Insensitive - Means the content is not case sensitive. - URI - Means the content needs to match URI field of HTTP request.
Relative	Specifies the signature content location. - If **Beginning** is selected, system will search from the header of the application layer packet.

Option	Description
	• Offset: System will start searching after the offset from the header of the application layer packet. The unit is byte. • Depth: Specifies the scanning length after the offset. The unit is byte. • If **Last Content** is selected, system will search from the content end position. • Distance: System will start searching after the distance from the former content end position. The unit is byte. • Within: Specifies the scanning length after the distance. The unit is byte.

- Load the database: After you create a new signature, click **Load Database** to make the newly created signature take effect.

- Edit a signature: Select a signature and then click **Edit**. You can only edit the user-defined signature. After editing the signature, click **Load Database** to make the modifications take effect.

- Delete a signature: Select a signature and then click **Delete**. You can only delete the user-defined signature. After deleting the signature, click **Load Database** to make the deletion take effect.

- Enable/Disable signatures: After selecting signatures, click **Enable** or **Disable**.

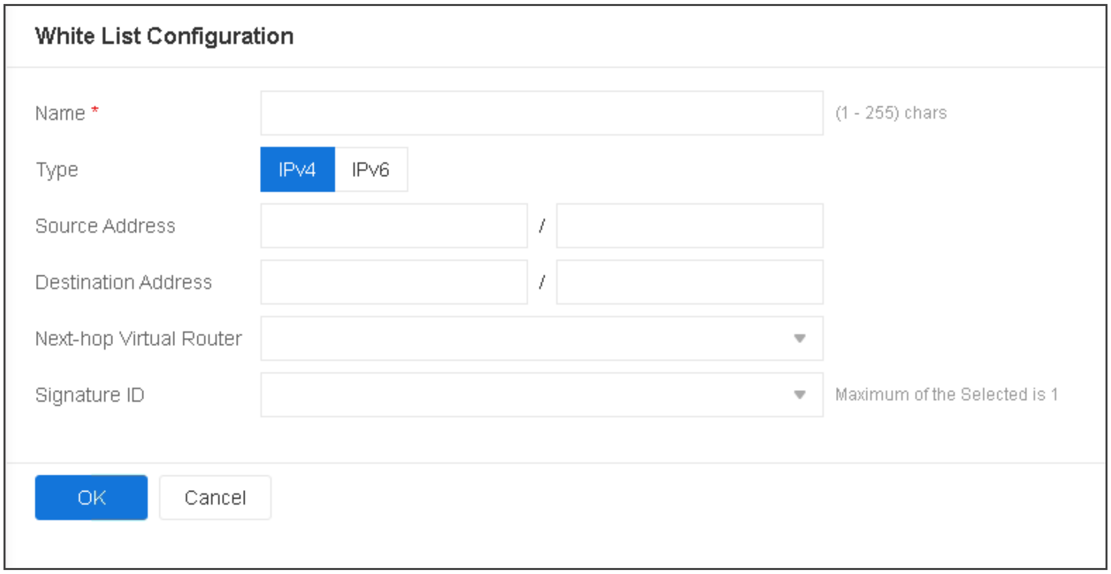
Notes: Non-root VSYS does not support signature list.

Configuring IPS White list

The device detects the traffic in the network in real time. When a threat is detected, the device generates alarms or blocks threats. With the complexity of the network environment, the threat of the device will generate more and more warning, too much threat to the user can not start making the alarm, and many of them are false positives. By providing IPS whitelist, the system no longer reports alarms or blocks to the whitelist, thus reducing the false alarm rate of threats. The IPS whitelist consists of source address, destination address, and threat ID, and the user selects at least one item for configuration.

To configure an IPS white list :

1. Select **Object> Intrusion Prevention System >Whitelist**
2. Click **New**.



White List Configuration

Name *		(1 - 255) chars
Type	IPv4 IPv6	
Source Address	/	
Destination Address	/	
Next-hop Virtual Router	▾	
Signature ID	▾	Maximum of the Selected is 1

In the WhiteList Configuration page, enter the White List configurations.

Option	Description
Name	Specifies the white-list name.
Type	Select the address type, including IPv4 or IPv6.
Source Address	Specifies the source address of the traffic to be matched by IPS.
Destination Address	Specifies the destination address of the traffic to be matched by IPS.
Next-hop Virtual Router	Select the Next-hop VRouter from the drop-down list.
Signature ID	Select the signature ID from the drop-down list. A whitelist can be configured with a maximum of one threat ID. When the threat ID is not set, the traffic can be filtered based on the source and destination IP address. When user have configured threat ID, the source address, destination address and threat ID must be all matched successfully before the packets can be released.

3. Click **OK**.

Sandbox

A sandbox executes a suspicious file in a virtual environment, collects the actions of this file, analyzes the collected data, and verifies the legality of the file.

The Sandbox function of the system uses the cloud sandbox technology. The suspicious file will be uploaded to the cloud side. The cloud sandbox will collect the actions of this file, analyze the collected data, verify the legality of the file, give the analysis result to the system and deal with the malicious file with the actions set by system.

The Sandbox function contains the following parts:

- Collect and upload the suspicious file: The Sandbox function parses the traffic, and extracts the suspicious file from the traffic.
    - If there are no analyze result about this file in the local database, system will upload this file to the cloud intelligence server, and the cloud server intelligence will upload the suspicious file to the cloud sandbox for analysis.
    - If this file has been identified as an illegal file in the local database of the Sandbox function, system will generate corresponding threat logs and cloudsandbox logs.

  Additionally, you can specify the criteria of the suspicious files by configuring a sandbox profile.

- Check the analysis result returned from the cloud sandbox and take actions: The Sandbox function checks the analysis results of the suspicious file returned from the cloud sandbox, verifies the legality of the file, saves the result to the local database. If this suspicious file is identified as an illegal file, you need to deal with the file according to the actions (reset the connection or report logs) set by system. If it's the first time to find malicious file in local sandbox, system will record threat logs and cloud sandbox logs and cannot stop the malicious link. When malicious file accesses the cached threat information in the local machine, the threat will be effective only by resetting connection.
- Maintain the local database of the Sandbox function: Record the information of the uploaded files, including uploaded time and analysis result. This part is completed by the Sandbox function automatically.

Notes: The Sandbox function is controlled by license. To use the Sandbox function, install the Cloud sandbox license.

Related Topics: Configuring Sandbox

Configuring Sandbox

This chapter includes the following sections:

- Preparation for configuring the Sandbox function
- Configuring the Sandbox rules
- Sandbox global configurations

Preparation

Before enabling the Sandbox function, make the following preparations:

1. Make sure your system version supports the Sandbox function.
2. The current device is registered to the Cloud platform.
3. Import the Cloud sandbox license and reboot. The Sandbox function will be enabled after rebooting.

> **Notes:** Except M8860/M8260/M7860/M7360/M7260, if the Sandbox function is enabled, the max amount of concurrent sessions will decrease by half.

Configuring Sandbox

System supports the policy-based Sandbox. To create the policy-based Sandbox, take the following steps:

1. Click **Object** > **Sandbox** > **Configuration**. Click the **Enable** button to enable the Sandbox function.
2. Click **Object** > **Sandbox** > **Profile** to create a sandbox rule you need.

3. Bind the sandbox rule to a policy. Click **Policy > Security Policy**.Select the policy rule you want to bind or click **New** to create a new policy. In the Policy Configuration page, expand **Protection** and then click the **Enable** button of Sandbox.

Configuring a Sandbox Rule

A sandbox rule contains the files types that device has detected, the protocols types that the device has detected, the white list settings, and the file filter settings.

- File Type: Support to detect PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP and Script file.
- Protocol Type: Support to detect HTTP, FTP, POP3, SMTP, IMAP4 and SMB protocol.
- White list: A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox.
- File filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox determines whether this suspicious file is legal or not.
- Actions: When the suspicious file accesses the threat items in the local sandbox, system will deal with the malicious file with the set actions.

There are three built-in sandbox rules with the files and protocols type configured, white list enabled and file filter configured. The three default sandbox rules includes predef_low, predef_middle and predef_high.

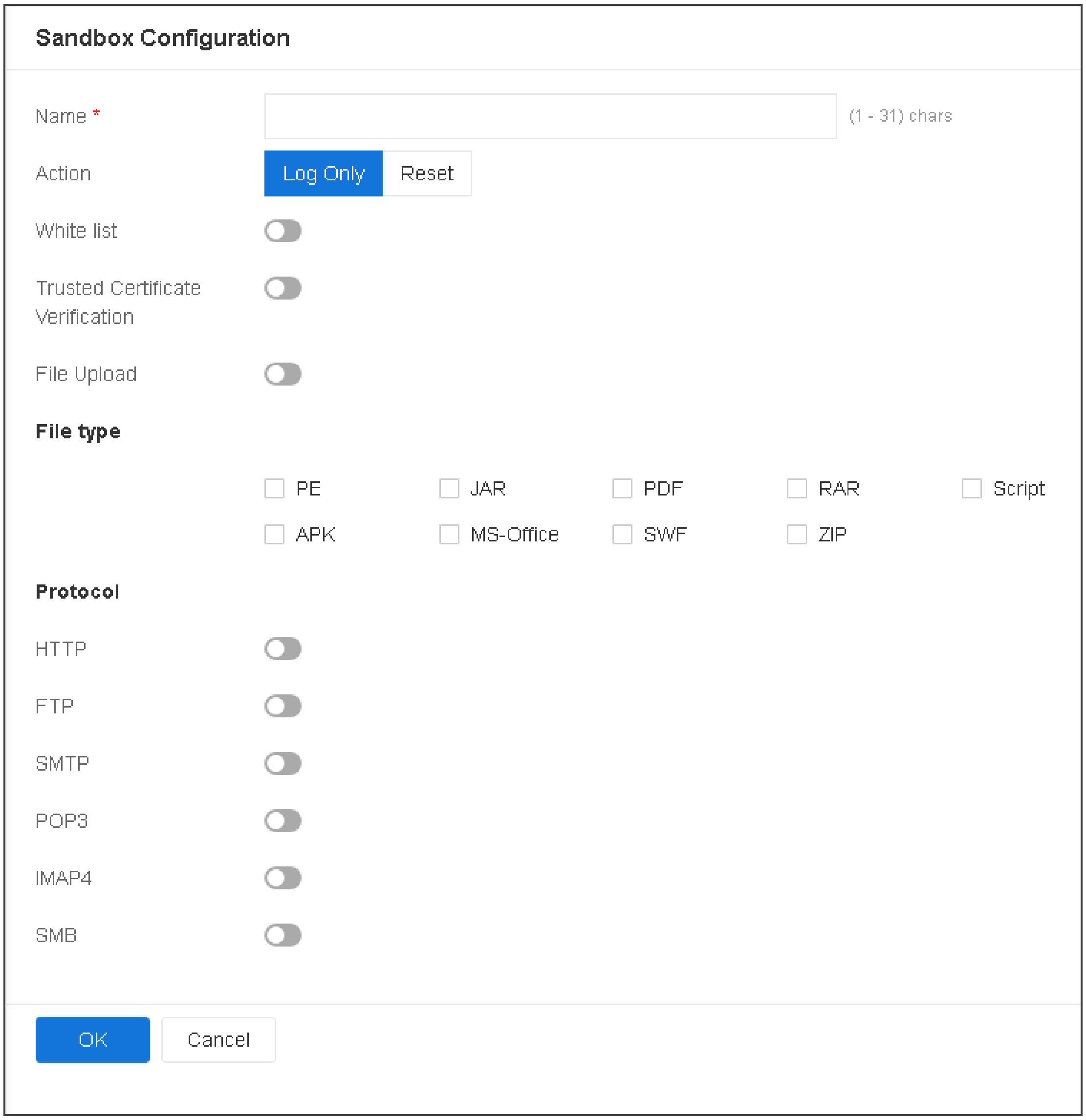
- **predef_low**: A loose sandbox detection rule, whose file type is PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.

- **predef_middle**: A middle-level sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.
- **predef_high**: A strict sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF/SWF/RAR/ZIP/Script and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.

To create a new sandbox rule, take the following steps:

1. Select **Object > Sandbox > Profile**.

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



Sandbox Configuration

Name * (1 - 31) chars

Action: Log Only | Reset

White list

Trusted Certificate Verification

File Upload

File type

□ PE □ JAR □ PDF □ RAR □ Script

□ APK □ MS-Office □ SWF □ ZIP

Protocol

HTTP

FTP

SMTP

POP3

IMAP4

SMB

OK | Cancel

In the Sandbox Configuration page, configure the following settings.

Option	Description
Name	Enter the name of the sandbox rule.
Action	When the suspicious file accesses the threat items in the

Option	Description
	local sandbox, system will deal with the malicious file with the set actions. Actions: • Log Only - When detecting malicious files, system will pass traffic and record logs only (threat log and cloud sandbox log). • Reset - When detecting malicious files, system will reset connection of malicious link and record threat logs and cloud sandbox logs only.
White List	Click **Enable** to enable the white list function. A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox. You can update the white list in **System > Upgrade Management > Signature Database Update > Sandbox Whitelist Database Update**.
Trusted Certificate Verification	Click **Enable** to enable the verification for the trusted certification. After enabling, system will not detect the PE file whose certification is trusted.
File Upload	By default, the file will be uploaded to the cloud sandbox when it marks it is classified as suspicious. You can disable the function of suspicious file uploading, which will prevent the suspicious file from being uploaded to the cloud sandbox. Click the **Disable** to disable the function

Option	Description
	of suspicious file uploading.
File Filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox determines whether this suspicious file is legal or not. The logical relation is AND.	
File Type	Mark the file of the specified file type as a suspicious file. The system can mark the PE(.exe), APK, JAR, MS-Office, PDF, SWF, RAR, ZIP and Script file as a suspicious file now. If no file type is specified, the Sandbox function will mark no file as a suspicious one.
Protocol	Specifies the protocol to scan. System can scan the HTTP, FTP, POP3, SMTP, IMAP4 and SMB traffic now. If no protocol is specified, the Sandbox function will not scan the network traffic.After specifying the protocol type, you have to specify the direction of the detection: • **Upload** - The direction is from client to server. • **Download** - The direction is from server to client. • **Bi-directional** - The direction includes uploading and downloading directions.

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

Threat List

The threat list means the list of threat items in the local sandbox. There are two sources of the threat items:

- The local sandbox finds suspicious files and reports to cloud. After verifying the file is malicious, the cloud will send the synchronous threat information to other devices, which has connected to the cloud and enabled Sandbox function. After the device receiving the synchronous threat information and matching the threat, the threat item will be listed in the threat list and system will block it with the set actions.
- The local sandbox finds suspicious file and reports to cloud. The cloud then analyzes and returns the result to the device. If the result is malicious, the threat item will be listed in the threat list.

You can filter and check threat items through specifying MD5 or the name of virus on the threat list page, as well as add the selected threat item to trust list. Take the following steps:

1. Click **Object > Sandbox > Threat List**.
2. Select the threat item that needs to be added to the trust list and click **Add to Trust** button. When threat item is added, once it's matched, the corresponding traffic will be released.

Trust List

You can view all the sandbox threat information which can be detected on the device and add them to the trust list. Once the item in trust list is matched, the corresponding traffic will be released and not controlled by the actions of sandbox rule.

To remove threat items in the trust list, take the following steps:

1. Click **Object > Sandbox > Trust List**.
2. Select the threat item that needs to be removed in the trust list and click **Remove from Trust** button. The threat item will be removed from the trust list.

Sandbox Global Configurations

To configure the sandbox global configurations, take the following steps:

1. Select **Object > Sandbox > Configuration**.
2. Click the **Enable** button of Sandbox to enable the Sandbox function. Clear the Enable check box to disable the Sandbox function.
3. Specify the file size for the files you need. The file that is smaller than the specified file size will be marked as a suspicious file.
4. If you click the **Report benign file log** button, system will record cloudsandbox logs of the file when it marks it as a benign file. By default, system will not record logs for the benign files.
5. If you click the **Report greyware file log** button, system will record cloudsandbox logs of the file when it marks it as a greyware file. A greyware file is the one system cannot judge it is a benign file or a malicious file. By default, system will not record logs for the greyware files.
6. Click **OK** to save the settings.

Attack-Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, belonging to a category of network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.

Devices provide attack defense functions based on security zones, and can take appropriate actions against network attacks to assure the security of your network systems.

ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amounts of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for a response. Due to the heavy load, the attacked target cannot complete its normal transmission task.

ARP Spoofing

LAN transmits network traffic based on MAC addresses. ARP spoofing attacks occur by filling in the wrong MAC address and IP address to make a wrong corresponding relationship of the target host's ARP cache table. This will lead to the wrong destination host IP packets, and the packet network's target resources will be stolen.

SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish are equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is ICMP fragment. Generally an ICMP packet will not be fragmented; so many systems cannot properly process ICMP fragments. If your system receives any ICMP fragment, it's almost certain that the system is under attack.

IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized access to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweeping or port scanning, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

Teardrop Attack

Teardrop attack is a denial of service attack. It is a attack method based on morbid fragmented UDP packets, which works by sending multiple fragmented IP packets to the attacker (IP fragmented packets include the fragmented packets of which packet, the packet location, and other information). Some operating systems contain overlapping offset that will crash, reboot, and so on when receiving fragmented packets.

Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

Fraggle Attack

A fraggle attack is basically the same with a smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

Land Attack

During a Land attack, an attacker will carefully craft a packet and set its source and destination address to the address of the server that will be attacked. In such a condition the attacked server will send a message to its own address, and this address will also return a response and establish a Null connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

IP Fragment Attack

An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.

IP Option Attack

An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.

Huge ICMP Packet Attack

An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.

TCP Flag Attack

An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.

DNS Query Flood Attack

The DNS server processes and replies to all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

TCP Split Handshake Attack

When a client establishes TCP connection with a malicious TCP server, the TCP server will respond to a fake SYN packet and use this fake one to initialize the TCP connection with the client. After establishing the TCP connection, the malicious TCP server switches its role and becomes the client side of the TCP connection. Thus, the malicious traffic might enter into the intranet.

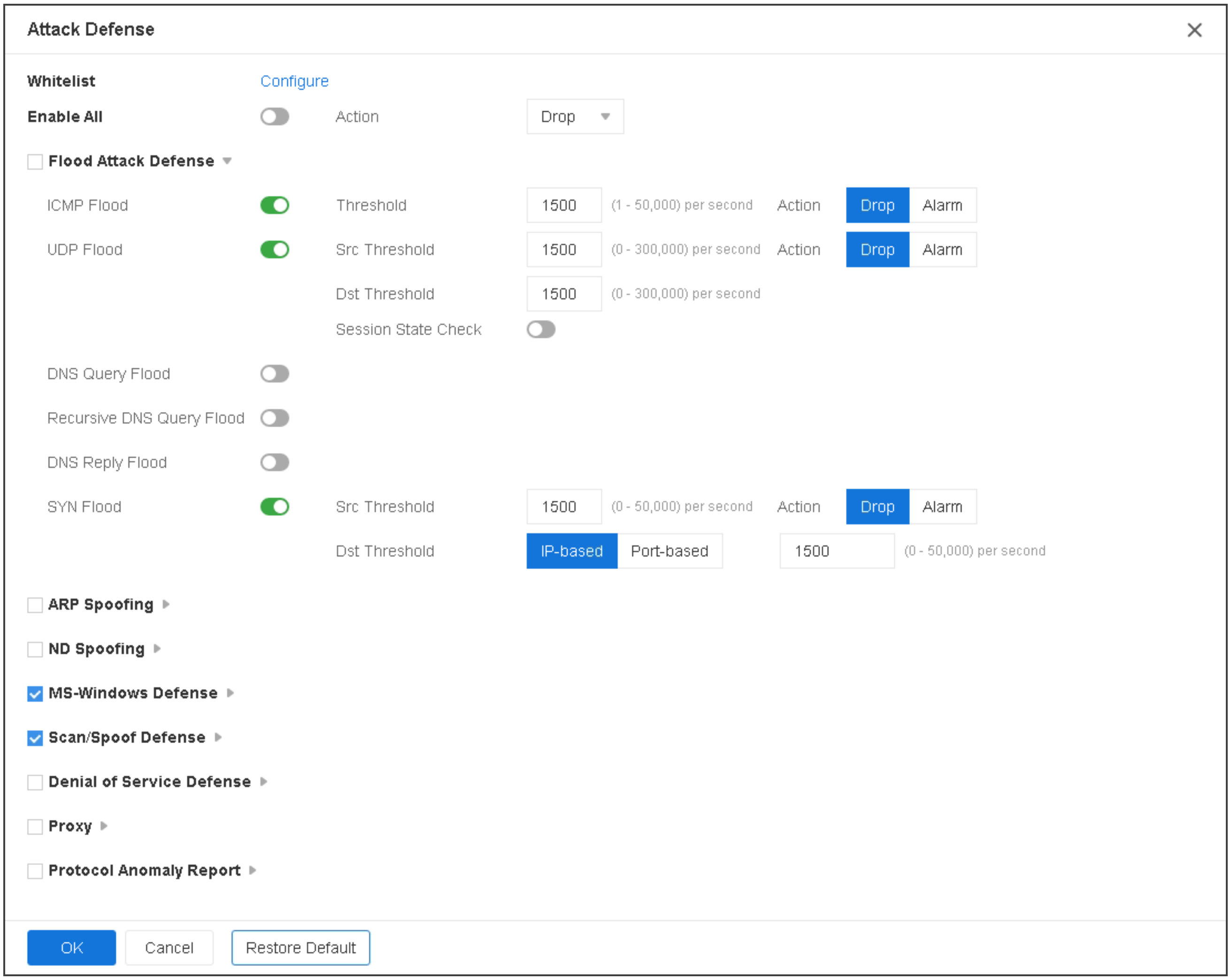
Configuring Attack Defense

To configure the Attack Defense based on security zones, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 74.

2. In the Zone Configuration page, expand Threat Protection.

3. To enable the Attack Defense functions, click the **Enable** button, and click **Configure**.



Attack Defense

Whitelist: Configure

Enable All: ○ Action: Drop

□ Flood Attack Defense

ICMP Flood: ● Threshold: 1500 (1 - 50,000) per second Action: Drop / Alarm

UDP Flood: ● Src Threshold: 1500 (0 - 300,000) per second Action: Drop / Alarm

Dst Threshold: 1500 (0 - 300,000) per second

Session State Check: ○

DNS Query Flood: ○

Recursive DNS Query Flood: ○

DNS Reply Flood: ○

SYN Flood: ● Src Threshold: 1500 (0 - 50,000) per second Action: Drop / Alarm

Dst Threshold: IP-based / Port-based 1500 (0 - 50,000) per second

□ ARP Spoofing

□ ND Spoofing

☑ MS-Windows Defense

☑ Scan/Spoof Defense

□ Denial of Service Defense

□ Proxy

□ Protocol Anomaly Report

In the Attack Defense page, enter the Attack Defense configurations.

Option	Description
Whitelist	IP address or IP range in the whitelist is exempt from attack defense check. Click **Configure**. • IP/Netmask - Click New to add to the whitelist and specifies the IP address and netmask. • Address entry - Click New to add to the whitelist and specifies the address entry.
Select All	**Enable all**: Click this button to enable all the Attack Defense functions for the security zone. **Action**: Specifies an action for all the Attack Defense functions, i.e., the defense measure system will be taken if any attack has been detected. • Drop - Drops packets. This is the default action. • Alarm - Gives an alarm but still permits packets to pass through. • Do not specify global actions.
Flood Attack Defense	Click the ▶ button to expand the information of all flood attack defenses. Select the **Flood Attack Defense** check box to enable all flood attack defenses.
	ICMP Flood: Click this button to enable ICMP flood defense for the security zone. • Threshold - Specifies a threshold for inbound ICMP pack-

Option	Description
	ets. If the number of inbound ICMP packets matched to one single IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. • Action - Specifies an action for ICMP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of IMCP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period.
	UDP Flood: Click this button to enable UDP flood defense for the security zone. • Src threshold - Specifies a threshold for outbound UDP packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. • Dst threshold - Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The

Option	Description
	value range is 1 to 50000. The default value is 1500. • Action - Specifies an action for UDP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of UDP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. • Session State Check - Select this check box to enable the function of session state check. After the function is enabled, system will not check whether there is UDP Flood attack in the backward traffic of UDP packet of the identified sessions.
	DNS Query Flood: Click this button to enable DNS query flood defense for the security zone. • Src threshold - Specifies a threshold for outbound DNS query packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Dst threshold - Specifies a threshold for inbound DNS query packets. If the number of inbound DNS query packets matched to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action.

Option	Description
	- Action - Specifies an action for DNS query flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the DNS query packets to pass through.
	Recursive DNS Query Flood: Click this button to enable recursive DNS query flood defense for the security zone. - Src threshold - Specifies a threshold for outbound recursive DNS query packets packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. - Dst threshold - Specifies a threshold for inbound recursive DNS query packets packets. If the number of inbound DNS query packets destined to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. - Action - Specifies an action for recursive DNS query flood attacks. If the default action Drop is selected, StoneOS

Option	Description
	will only permit the specified number (threshold) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the recursive DNS query packets to pass through.
	SYN Flood: Select this check box to enable SYN flood defense for the security zone. • Src threshold - Specifies a threshold for outbound SYN packets (ignoring the destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Src threshold is void. • Dst threshold - Specifies a threshold for inbound SYN packets destined to one single destination IP address per second. • IP-based - Click IP-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value

Option	Description
	range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void. - Port-based - Click Port-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination port of the destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void. After clicking Port-based, you also need to type an address into or select an IP Address or Address entry from the Dst address combo box to enable port-based SYN flood defense for the specified segment. The SYN flood attack defense for other segments will be IP based. The value range for the mask of the Dst address is 24 to 32. - Action - Specifies an action for SYN flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of SYN packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. Besides if Src threshold and Dst threshold are also configured, StoneOS will first

Option	Description
	detect if the traffic is a destination SYN flood attack: if so, StoneOS will drop the packets and give an alarm, if not, StoneOS will continue to detect if the traffic is a source SYN attack.
	DNS Reply Flood: Click this button to enable DNS reply flood defense for the security zone. • Src threshold - Specifies a threshold for outbound DNS reply packets. If the number of outbound DNS reply packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Dst threshold - Specifies a threshold for inbound DNS reply packets. If the number of inbound DNS reply packets matched to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS reply flood and take the specified action. • Action - Specifies an action for DNS reply flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of DNS reply packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the DNS reply packets to pass through.

Option	Description
ARP Spoofing	Click the ▶ button to expand the information of the ARP spoofing. Select the **ARP Spoofing** check box to enable all ARP spoofing defenses.
	Max IP number per MAC: Click this button to check the max IP number per MAC. Specifies whether system will check the IP number per MAC in the ARP table. If the parameter is set to 0, system will not check the IP number; if it is set to a value other than 0, system will check the IP number, and if the IP number per MAC is larger than the parameter value, system will take the specified action. The value range is 0 to 1024.
	ARP Send Rate: Click this button to check the ARP send rate. Specifies if StoneOS will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), StoneOS will not send any gratuitous ARP packet; if it is set to a value other than 0, StoneOS will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10.
	Reverse Query: Click this button to enable Reverse query. Select this check box to enable Reverse query. When StoneOS receives an ARP request, it will log the IP address and reply with another ARP request; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP

Option	Description
	request packet.
ND Spoofing	**Max IP number per MAC**: Click this button to check the max IP number per MAC. Specifies whether system will check the IP number per MAC in the ND table. System will check the IP number, and if the IP number per MAC is larger than the parameter value, system will take the specified action. The value range is 1 to 1024. **ND Send Rate**: Click this button to check the ND send rate. Specifies if StoneOS will send gratuitous ND packet(s). StoneOS will send gratuitous ND packet(s), and the number sent per second is the specified parameter value. The value range is 1 to 10. **Reverse Query**: Click this button to enable Reverse query. Select this check box to enable Reverse query. When StoneOS receives a NS/NA packet, it will log the IP address and reply with another NS/NA packet; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ND packet.
MS-Windows Defense	Click the ▶ button to expand the information of MS-Windows defense. Select the **MS-Windows Defense** check box to enable MS-Windows defense.
	Win Nuke Attack: Click this button to enable WinNuke attack defense for the security zone. If any WinNuke attack has been

Option	Description
	detected, system will drop the packets and give an alarm.
Scan/Spoof Defense	Click the ▶ button to expand the information of Scan/Spoof Defense. Select the **Scan/Spoof Defense** check box to enable all scan/spoof defenses.
	IP Address Spoof: Click this button to enable IP address spoof defense for the security zone. If any IP address spoof attack has been detected, StoneOS will drop the packets and give an alarm.
	IP Address Sweep: Click this button to enable IP address sweep defense for the security zone. • Threshold - Specifies a time threshold for IP address sweep. If over 10 ICMP packets from one single source IP address are sent to different hosts within the period specified by the threshold, StoneOS will identify them as an IP address sweep attack. The value range is 1 to 5000 milliseconds. The default value is 1. • Action - Specifies an action for IP address sweep attacks. If the default action Drop is selected, StoneOS will only permit 10 IMCP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (threshold), and also give an alarm. All the excessive packets of the same type will be dropped during this period.
	Port Scan: Click this button to enable port scan defense for the

Option	Description
	security zone. - Threshold - Specifies a time threshold for port scan. If over 10 TCP SYN packets are sent to different ports within the period specified by the threshold, StoneOS will identify them as a port scan attack. The value range is 1 to 5000 milliseconds. The default value is 1. - Action - Specifies an action for port scan attacks. If the default action Drop is selected, StoneOS will only permit 10 TCP SYN packets destined to different ports to pass through and drops the other packets of the same type during the specified period, and also gives an alarm.
Denial of Service Defense	Click the ▶ button to expand the information of denial of service defense. Select the **Denial of Service Defense** check box to enable all denial of service defenses.
	Ping of Death Attack:Click this button to enable Ping of Death attack defense for the security zone. If any Ping of Death attack has been attacked, StoneOS will drop the attacking packets, and also give an alarm.
	Teardrop Attack: Click this button to enable Teardrop attack defense for the security zone. If any Teardrop attack has been attacked, StoneOS will drop the attacking packets, and also give an alarm.
	IP Fragment: Click this button to enable IP fragment defense for

Option	Description
	the security zone. • Action - Specifies an action for IP fragment attacks. The default action is Drop.
	IP Option: Click this button to enable IP option attack defense for the security zone. StoneOS will defend against the following types of IP options: Security, Loose Source Route, Record Route, Stream ID, Strict Source Route and Timestamp. • Action - Specifies an action for IP option attacks. The default action is Drop.
	Smurf or Fragile Attack: Click this button to enable Smurf or fragile attack defense for the security zone. • Action - Specifies an action for Smurf or fragile attacks. The default action is Drop.
	Land Attack: Click this button to enable Land attack defense for the security zone. • Action - Specifies an action for Land attacks. The default action is Drop.
	Large ICMP Packet: Click this button to enable large ICMP packet defense for the security zone. • Threshold - Specifies a size threshold for ICMP packets. If the size of any inbound ICMP packet is larger than the threshold, StoneOS will identify it as a large ICMP packet

Option	Description
	and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024. • Action - Specifies an action for large ICMP packet attacks. The default action is Drop.
Proxy	Click the ▶ button to expand the information of proxy defense. Select the **Proxy** check box to enable all proxy defenses.
	SYN Proxy: Click this button to enable SYN proxy for the security zone. SYN proxy is designed to defend against SYN flood attacks in combination with SYN flood defense. When both SYN flood defense and SYN proxy are enabled, SYN proxy will act on the packets that have already passed detections for SYN flood attacks. • Proxy trigger rate - Specifies a min number for SYN packets that will trigger SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets matched to one single port of one single destination IP address per second exceeds the specified value, StoneOS will trigger SYN proxy or SYN-Cookie. The value range is 1 to 50000. The default value is 1000. • Cookie - Select this check box to enable SYN-Cookie. SYN-Cookie is a stateless SYN proxy mechanism that enables StoneOS to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand

Option	Description
	the range between "Proxy trigger rate" and "Max SYN packet rate" appropriately. • Max SYN packet rate - Specifies a max number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, StoneOS will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. • Timeout - Specifies a timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30.
Protocol Anomaly Report	Click the ▶ button to expand the information of protocol anomaly report. Select the **Protocol Anomaly Report** check box to enable the function of all protocol anomaly reports.
	TCP Anomalies: Click this button to enable TCP option anomaly defense for the security zone. • Action - Specifies an action for TCP option anomaly

Option	Description
	attacks. The default action is Drop. **TCP Split Handshake**: Click this button to enable TCP split handshake defense for the security zone. - Action - Specifies an action for TCP split handshake attacks. The default action is Drop.

4. To restore the system default settings, click **Restore Default**.

5. Click **OK**.

Perimeter Traffic Filtering

Perimeter Traffic Filtering can filter the perimeter traffic based on known risk IP list, and take logging/block action on the malicious traffic that hits the risk IP list.

The risk IP list includes the following three types:

- IP Reputation list: Retrieve the risk IP (such as Botnet, Spam, Tor nodes, Compromised, Brute-forcer, and so on.) list from the Perimeter Traffic Filtering signature database.
- User-defined black/white list : According to the actual needs of users, the specified IP address is added to a user-definedblack/white list.

Notes:

- You need to update the IP reputation database before enabling the IP Reputation function for the first time. By default, system will update the database at the certain time everyday, and you can modify the updating settings according to your own requirements, see "Upgrading System" on Page 1223.
- Perimeter Traffic Filtering is controlled by license. To use Threat protection, apply and install the PTF license.

Enabling Perimeter Traffic Filtering

To realize the zone-based Perimeter Traffic Filtering, take the following steps:

1. Create a zone. For more information , refer to "Security Zone" on Page 74;
2. In the Zone Configuration page, expand Threat Protection.
3. Click the **Enable** button after the **Perimeter Traffic Filtering**.

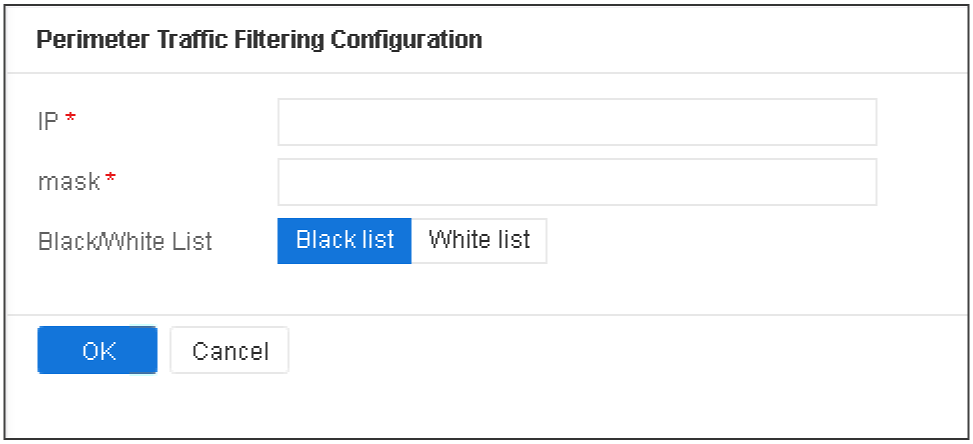
4. Specifies an action for the malicious traffic that hits the blacklist. Click the **User-defined** or **IP Reputation** button , and select the action from drop-down list:

   - Log Only: Only generates logs if the malicious traffic hits the blacklist. This is the default option.
   - Drop: Drop packets if the malicious traffic hits the blacklist.
   - Block IP: Block the IP address and specify a block duration if the malicious traffic hits the IP Reputation list.

Configuring User-defined Black/White List

To configure the user-defined black/white list , take the following steps:

1. Select **Object > Perimeter Traffic Filtering**.
2. Click **New**.



Perimeter Traffic Filtering Configuration

IP *	
mask *	
Black/White List	Black list | White list

In Perimeter Traffic Filtering Configuration page, enter the user-defined black/white list configuration.

Option	Description
IP	Specify the IP address for the user-defined black/white list.
mask	Specify the netmask of the IP address.
Black/White List	Select the radio button to add the IP address to the black-list or whitelist .

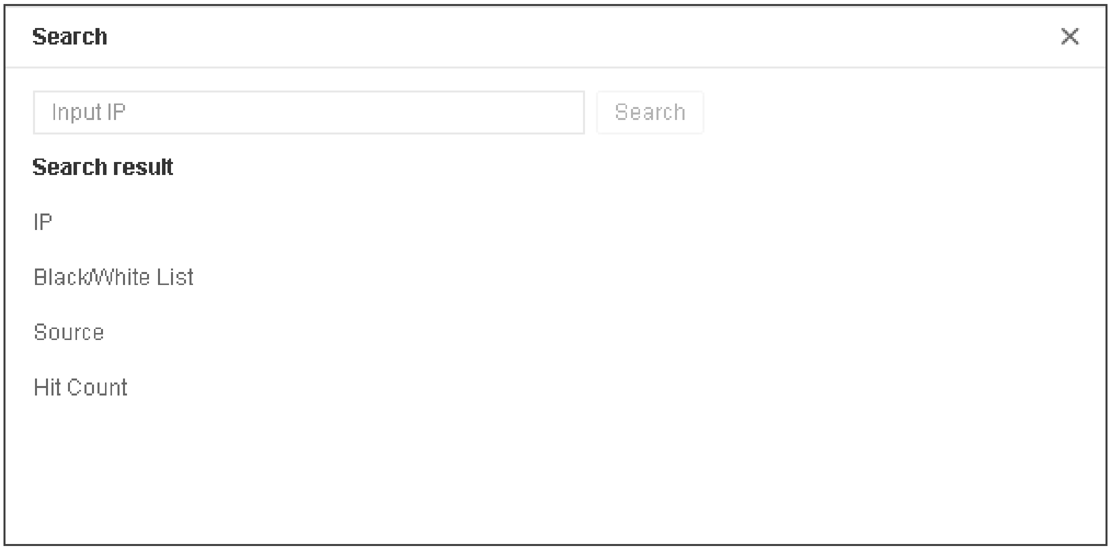
3. Click **OK**.

Searching Black/White List

To search the black/white list, take the following steps:

1. Select **Object > Perimeter Traffic Filtering**.

2. Click **Search**.



Search

Input IP

Search result

IP

Black/White List

Source

Hit Count

3. Enter the IP address and click **Search**. The results will be displayed in this page.

Botnet Prevention

Botnet refers to a kind of network that uses one or more means of communication to infect a large number of hosts with bots, forming a one-to-many controlled network between the controller and the infected host, which will cause a great threat to network and data security.

The botnet prevention function can detect botnet host in the internal network timely, as well as locate and take other actions according to the configuration, so as to avoid further threat attacks.

The botnet prevention configurations are based on security zones or policies. If the botnet prevention profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the botnet prevention profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration.

Notes: The botnet prevention function is controlled by license. To use the botnet prevention function, install the Botnet Prevention license.

Related Topics:

- "Configuring Botnet Prevention" on Page 1005
- "Address Liberary" on Page 1008
- "Botnet Prevention Global Configuration" on Page 1010

Configuring Botnet Prevention

This chapter includes the following sections:

- Preparation for configuring Botnet Prevention function
- Configuring Botnet Prevention function

Preparing

Before enabling botnet prevention, make the following preparations:

1. Make sure your system version supports botnet prevention.
2. Import a botnet prevention license and reboot. The botnet prevention will be enabled after the rebooting.

> **Notes:**
>
> - You need to update the botnet prevention signature database before enabling the function for the first time. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating.

Configuring Botnet Prevention Function

The Botnet Prevention configurations are based on security zones or policies.

To realize the zone-based Botnet Prevention, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 74.
2. In the Zone Configuration page, expand Threat Protection.

3. Enable the threat protection you need and select a Botnet Prevention rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list. To create a Botnet Prevention rule, see Configuring a Botnet Prevention Rule.

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

To realize the zone-based Botnet Prevention, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 768.

2. In the Policy Configuration page, expand the Protection.

3. Click the **Enable** button of **Botnet Prevention**. Then select an Anti-Spam rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create a Botnet Prevention rule. For more information, see Configuring a Botnet Prevention Rule.

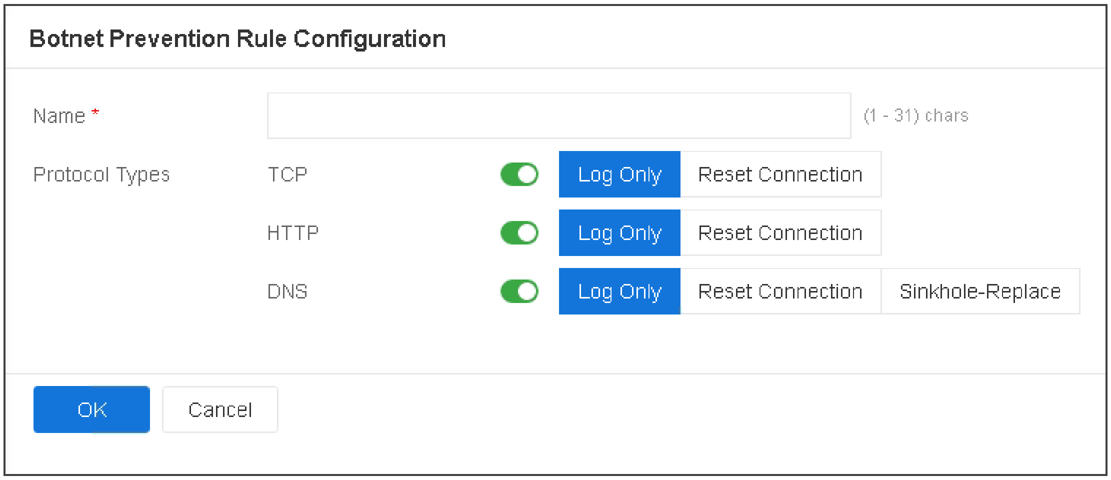
4. Click **OK** to save the settings.

Configuring a Botnet Prevention Rule

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

1. Click **Object** > **Botnet Prevention**> **Profile**.

2. Click **New**.



Botnet Prevention Rule Configuration

Name *					(1 - 31) chars
Protocol Types	TCP	●	Log Only	Reset Connection	
	HTTP	●	Log Only	Reset Connection	
	DNS	●	Log Only	Reset Connection	Sinkhole-Replace

OK Cancel

In the Botnet Prevention Rule Configuration page, enter the Botnet Prevention rule configurations.

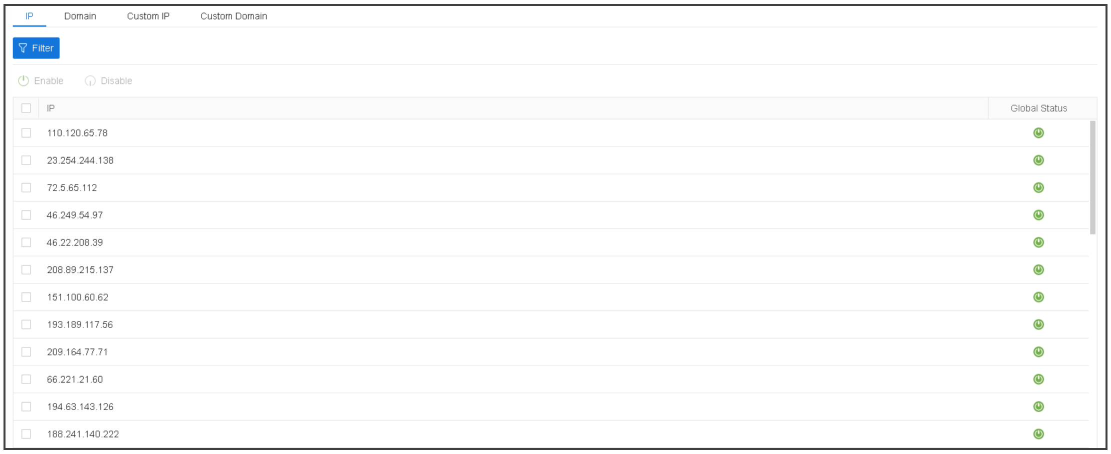
Option	Description
Name	Specifies the rule name.
Protocol Types	Specifies the protocol types (TCP, HTTP, DNS) you want to scan and specifies the action the system will take after the botnet is found. • Log Only - Only generates log. • Reset Connection - If botnets has been detected, system will reset 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.

3. Click **OK**.

Address Liberary

The address library includes a predefined address library and a custom address library. The predefined address database is automatically obtained through the botnet prevention signature database, and the custom address database is an IP address or domain name manually added by the user.

Select **Object > Botnet Prevention > Address Liberary**. You can see the IP address and domain name list page of the predefined address library and custom address library.



□	IP	Global Status
□	110.120.65.78	●
□	23.254.244.138	●
□	72.5.65.112	●
□	46.249.54.97	●
□	46.22.208.39	●
□	208.89.215.137	●
□	151.100.60.62	●
□	193.189.117.56	●
□	209.164.77.71	●
□	66.221.21.60	●
□	194.63.143.126	●
□	188.241.140.222	●

Enabling/Disabling the Address Entry

To disable the signature of the specified IP/domain, take the following steps:

1. Click **IP** , **Domain**, **Custom IP** or **Custom Domain**tab.

2. Select the IP or domain entry that you want to enable/disable, and then click **Enable** or **Disable**.

Creating a Custom Address Entry

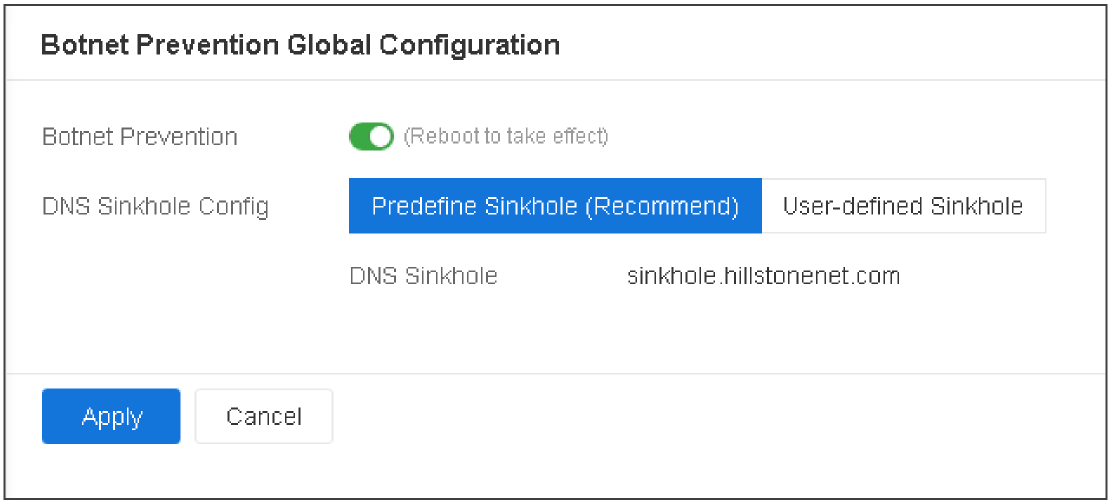
To create a signature of the specified IP/domain name, take the following steps:

1. Click **Custom IP** or **Custom Domain** tab.
2. Click **New** to open the **Botnet Custom IP Configuration** or **Botnet Custom Domain Configuration** page.
3. Enter the IP or domain name entry in the text box.
4. Click **OK**.
5. Select the IP or domain name entry that you want to delete/enable/disable, and then click **Delete**, **Enable** or **Disable**.

Botnet Prevention Global Configuration

To configure the Botnet Prevention global settings, take the following steps:

1. Click **Object** > **Botnet Prevention** > **Configuration**.



Botnet Prevention Global Configuration

Botnet Prevention ● (Reboot to take effect)

DNS Sinkhole Config: Predefine Sinkhole (Recommend) | User-defined Sinkhole

DNS Sinkhole: sinkhole.hillstonenet.com

2. Click/clear the **Enable** button to enable/disable the Botnet Prevention function.

3. Specify the Sinkhole IP address that replaces the IP address in the DNS response message. You can select the system's predefined Sinkhole IP address or specify a user-defined Sinkhole IP address. After selecting **User-defined Sinkhole**, specify a custom IPv4 address and an IPv6 address. If only the IPv4 address is configured, the system will automatically map the configured IPv4 address to the corresponding IPv6 address when the DNS server communicates by using the IPv6 protocol.

4. Click **Apply** to apply the settings.

Chapter 12 Monitor

The monitor section includes the following functions:

- **Monitor**: The Monitor function statistically analyzes the devices and displays the statistics in a bar chart, line chart, tables, and so on, which helps the users have information about the devices.
- **Report**: Through gathering and analyzing the device traffic data, traffic management data, threat data, monitor data and device resource utilization data, the function provides the all-around and multi-demensional staticstcs.
- **Log**: Records various system logs, including system logs, threat logs, session logs, NAT logs, NBC logs and configuration logs.

Monitor

System can monitor the following objects.

- **User Monitor**: Displays the application statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month) The statistics include the application traffic and applications' concurrent sessions.
- **Application Monitor**: Displays the statistics of applications, application categories, application subcategories, application risk levels, application technologies, application characteristics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month). The statistics include the application traffic and applications' concurrent sessions.
- **Cloud Application Monitor**: Displays statistics of cloud based applications, including their traffic, new sessions and concurrent sessions.
- **Share Access Monitor**: Displays the access terminal statistics of specified filter condition(Virtual router, IP, host number), including operation system , online time, login time and last online time of users.
- **End Point Detect**:Displays the endpoint data information list synchronized with the endpoint security control center.
- **User Quota Detect**:Displays the user traffic quota statistics list.
- **Device Monitor**: Displays the device statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month), including the total traffic, interface traffic, zone traffic, CPU/memory status, sessions, Online IP and hardware status.
- **URL Hit**: If system is configured with " URL Filtering" on Page 659, the predefined stat-set of URL Hit can gather statistics on user/IPs, URLs and URL categories.

- **Link Status Monitor:**Displays the traffic statistics of the interfaces that have been bound within the specified period .
- **Application Block**: If system is configured with "Security Policy" on Page 768 the application block can gather statistics on the applications and user/IPs.
- **Keyword Block**: If system is configured with"Web Content" on Page 712, "Email Filter" on Page 724, "Web Posting" on Page 718, the predefined stat-set of Keyword Block can gather statistics on the Web keyword, Web keywords, email keywords, posting keywords and users/IPs.
- **Authenticated User**: If system is configured with"Web Authentication" on Page 302, "1Single Sign-On" on Page 314, "SSL VPN" on Page 410 , "L2TP VPN" on Page 523 the auth user can gather statistics on the authenticated users.
- **Monitor Configuration**: Enable or disable some monitor items as needed.
- **User Defined Monitor**: Provides a more flexible approach to view the statistics.

Notes: If IPv6 is enabled, system will count the total traffic/sessions/AD/URLs/applications of IPv4 and IPv6 address. Only User Monitor/Application Monitor/Cloud Application Monitor/Device Monitor/URL Hit/Application Block/User-defined Monitor support IPv6 address.

User Monitor

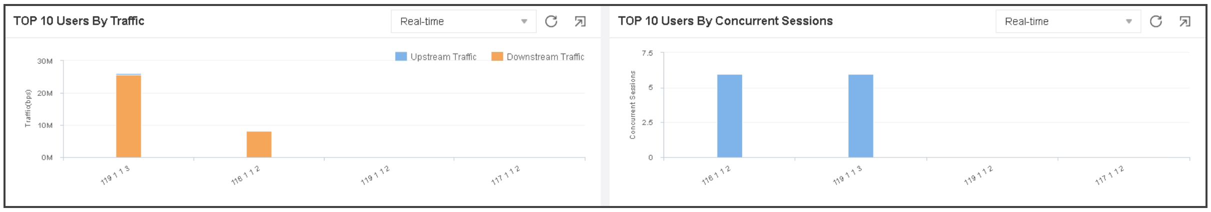
User monitor displays the application statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month ） . The statistics include the application traffic and applications' concurrent sessions.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

> **Notes:** Non-root VSYS also supports user monitor, but does not support address book statistics.

Summary

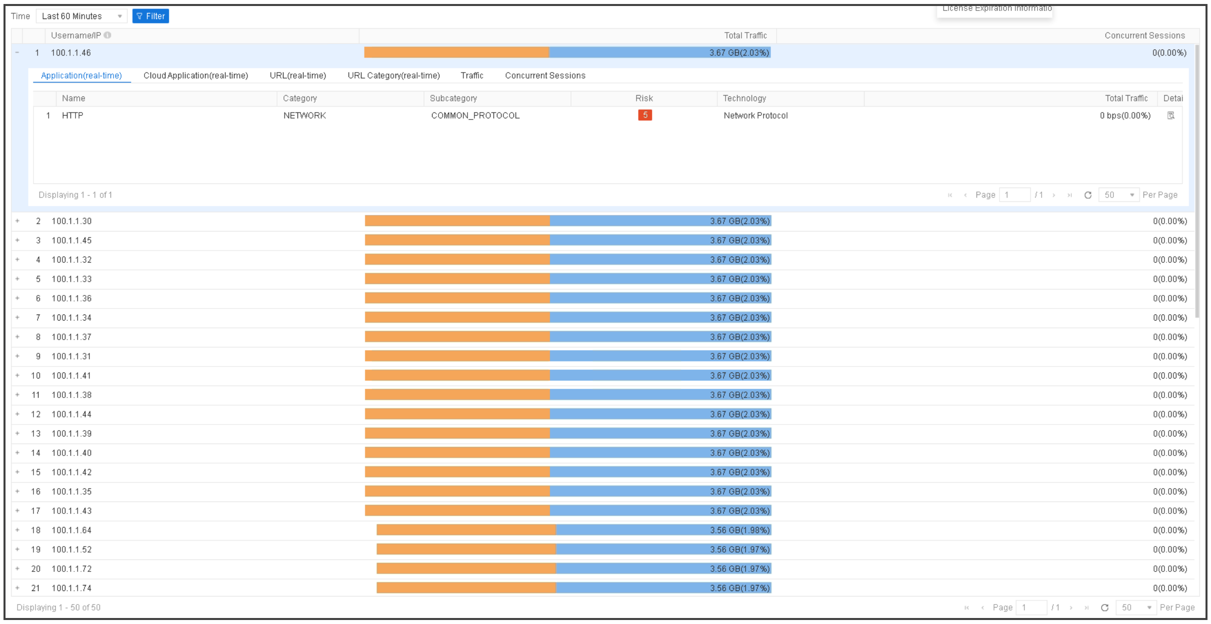
Summary displays the user traffic/concurrent sessions ranking during a specified period or of specified interfaces/zones. Click **Monitor > User Monitor > Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Click "↻" to refresh the monitoring data in this page.
- Click "↗" to close the current frame.
- Hover your mouse over a bar to view the user's average upstream traffic, downstream traffic, total trafficor concurrent sessions .
- When displaying the user traffic statistics, the Upstream and Downstream legends are used to select the statistical objects in the bar chart.

User Details

Click **Monitor > User Monitor> User Details**.



Time Last 60 Minutes ▾ Filter

		Username/IP	Total Traffic	Concurrent Sessions
-	1	100.1.1.46	3.67 GB(2.03%)	0(0.00%)

Application(real-time) | Cloud Application(real-time) | URL(real-time) | URL Category(real-time) | Traffic | Concurrent Sessions

	Name	Category	Subcategory	Risk	Technology	Total Traffic	Detai
1	HTTP	NETWORK	COMMON_PROTOCOL	5	Network Protocol	0 bps(0.00%)	

Displaying 1 - 1 of 1 Page 1 / 1 50 Per Page

		Username/IP	Total Traffic	Concurrent Sessions
+	2	100.1.1.30	3.67 GB(2.03%)	0(0.00%)
+	3	100.1.1.45	3.67 GB(2.03%)	0(0.00%)
+	4	100.1.1.32	3.67 GB(2.03%)	0(0.00%)
+	5	100.1.1.33	3.67 GB(2.03%)	0(0.00%)
+	6	100.1.1.36	3.67 GB(2.03%)	0(0.00%)
+	7	100.1.1.34	3.67 GB(2.03%)	0(0.00%)
+	8	100.1.1.37	3.67 GB(2.03%)	0(0.00%)
+	9	100.1.1.31	3.67 GB(2.03%)	0(0.00%)
+	10	100.1.1.41	3.67 GB(2.03%)	0(0.00%)
+	11	100.1.1.38	3.67 GB(2.03%)	0(0.00%)
+	12	100.1.1.44	3.67 GB(2.03%)	0(0.00%)
+	13	100.1.1.39	3.67 GB(2.03%)	0(0.00%)
+	14	100.1.1.40	3.67 GB(2.03%)	0(0.00%)
+	15	100.1.1.42	3.67 GB(2.03%)	0(0.00%)
+	16	100.1.1.35	3.67 GB(2.03%)	0(0.00%)
+	17	100.1.1.43	3.67 GB(2.03%)	0(0.00%)
+	18	100.1.1.64	3.56 GB(1.98%)	0(0.00%)
+	19	100.1.1.52	3.56 GB(1.97%)	0(0.00%)
+	20	100.1.1.72	3.56 GB(1.97%)	0(0.00%)
+	21	100.1.1.74	3.56 GB(1.97%)	0(0.00%)

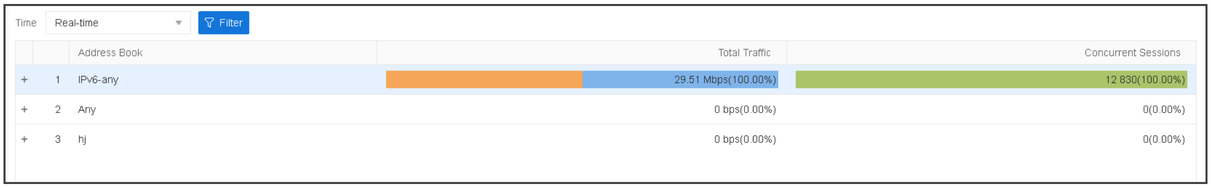
Displaying 1 - 50 of 50 Page 1 / 1 50 Per Page

- 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**.

Address Book Details

Click **Monitor>User Monitor>Address Book Details**.



Time Real-time ▾ Filter

		Address Book	Total Traffic	Concurrent Sessions
+	1	IPv6-any	29.51 Mbps(100.00%)	12 830(100.00%)
+	2	Any	0 bps(0.00%)	0(0.00%)
+	3	hj	0 bps(0.00%)	0(0.00%)

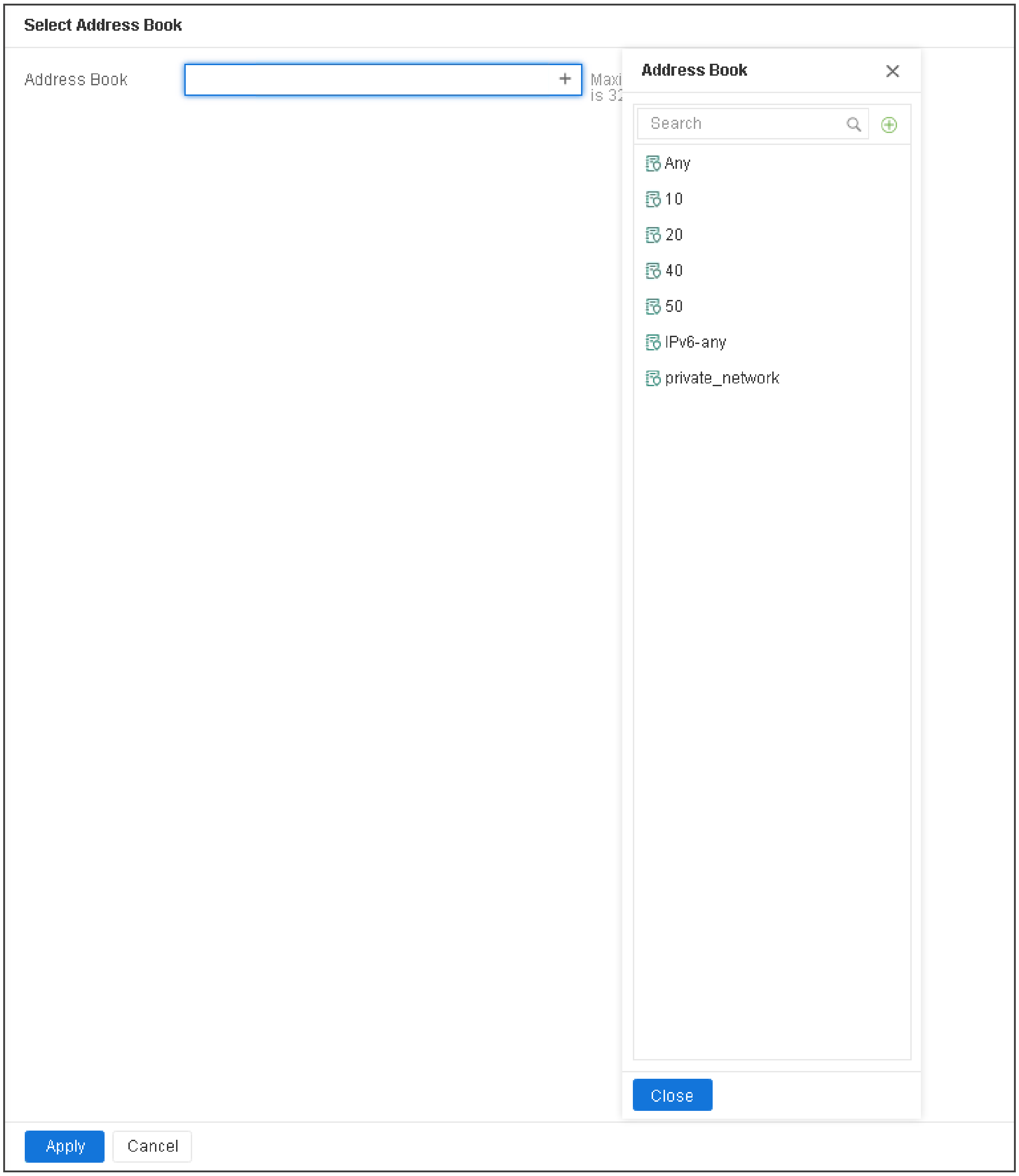
- Click Filter to select the condition in the drop-down list to search the desired address entry.
- To view the detailed information of a address entry, select the address entry in the list, and click "+".
    - Application (real-time): Select the Application (real-time) tab to displays the detailed information of the upstream traffic, downstream traffic, and 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 address book.
    - User (real-time) : Select the User tab to display the total traffic of selected address book.

- Traffic: Select the Traffic tab to display the traffic trends of selected address entry.
- Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of selected address entry.

Monitor Address Book

The monitor address is a database that stores the user 's address which is used for statistics.

Click **Monitor > User Monitor> Select Address Book**.



In this page, you can perform the following actions:

- Click the desired address entry check box to add a new address entry to the left list.
- In the left list, click an address entry to remove it from the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click the time button on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last Hour: Displays the statistical information within the latest 1 hour.
- Last Day: Displays the statistical information within the latest 1 day.
- Last Month: Displays the statistical information within the latest 1 month.

Application Monitor

Application monitor displays the statistics of applications, application categories, application sub-categories, application risk levels, application technologies, and application characteristics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month) .The statistics include the application traffic and applications' concurrent sessions.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

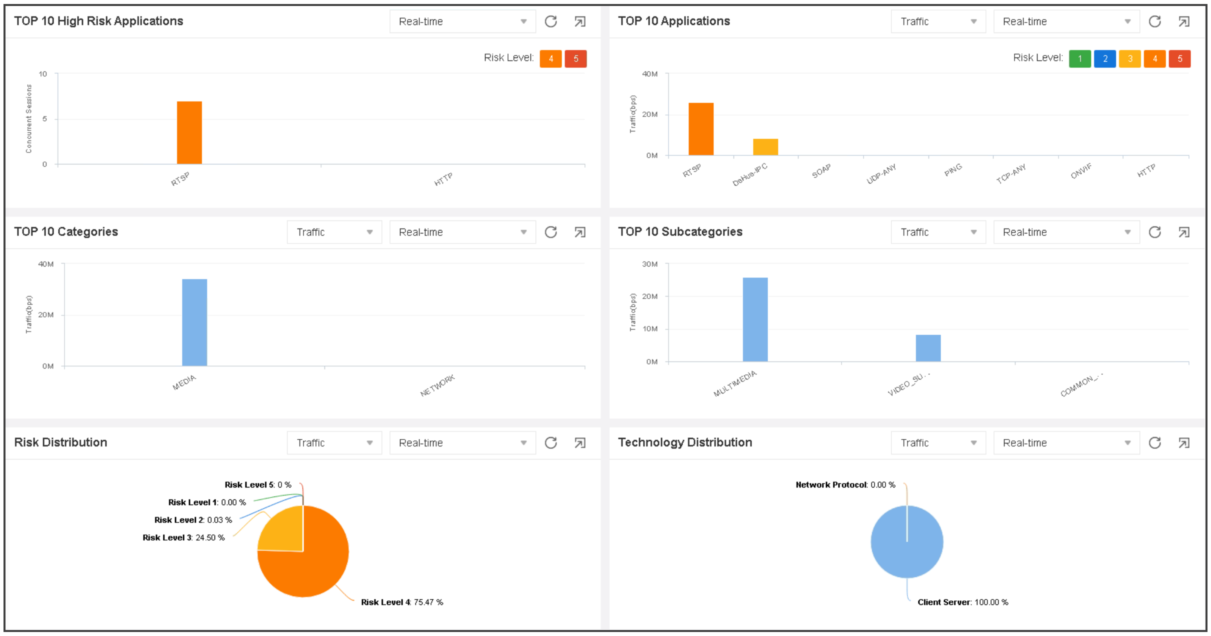
Notes: Non-root VSYS also supports application monitor, but does not support to monitor application group.

Summary

The summary displays the following contents during a specified period:

- The concurrent sessions of top 10 hot and high-risk applications.
- The traffic/concurrent sessions of top 10 applications.
- The traffic/concurrent sessions of top 10 application categories.
- The traffic/concurrent sessions of top 10 application subcategories.
- The traffic/concurrent sessions organized by application risk levels.
- The traffic/concurrent sessions organized by application technologies.
- The traffic/concurrent sessions organized by application characteristics.

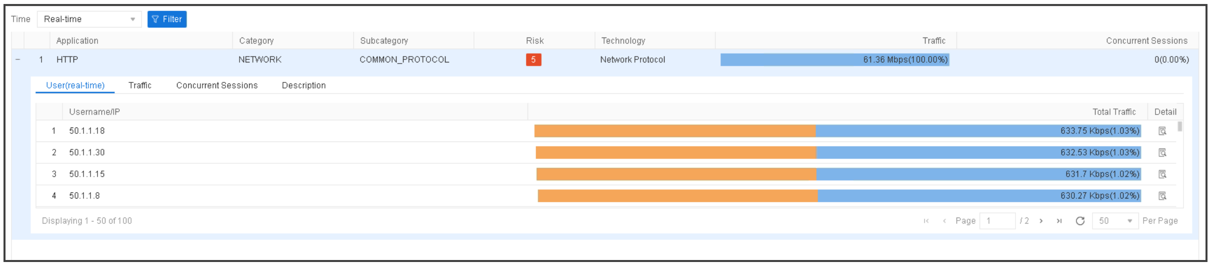
Click **Monitor>Application Monitor>Summary**.



- Select different Statistical_Period to view the statistical information in different periods of time.
- From the drop-down menu, specify the type of statistics: Traffic or Concurrent Sessions.
- Click "↻" to refresh the monitoring data in this page.
- Click "↗" to close the current frame.
- Hover your mouse over a bar or a pie graph to view the concrete statistical values of total traffic or concurrent sessions.

Application Details

Click **Monitor** > **Application Monitor** > **Application Details**.



Time Real-time

		Application	Category	Subcategory	Risk	Technology	Traffic	Concurrent Sessions
−	1	HTTP	NETWORK	COMMON_PROTOCOL	5	Network Protocol	61.36 Mbps(100.00%)	0(0.00%)

	Username/IP	Total Traffic	Detail
1	50.1.1.18	633.75 Kbps(1.03%)	
2	50.1.1.30	632.53 Kbps(1.03%)	
3	50.1.1.15	631.7 Kbps(1.02%)	
4	50.1.1.8	630.27 Kbps(1.02%)	

Displaying 1 - 50 of 100 Page 1 / 2 50 Per Page

- Click the **Time** drop-down menu to select different Statistical_Period to view the statistical information in that periods of time.

- Click Filter button and select **Application** in the drop-down menu. You can search the desired application by entering the keyword of the application's name in the text field.

- To view the detailed information of a certain application, select the application entry in the list, and click "+".

  - Users(real-time): Select the Users (real-time) tab to displays the detailed information of users who are using the selected application. Click in details column to see the trends of upstream traffic, downstream traffic, total traffic.

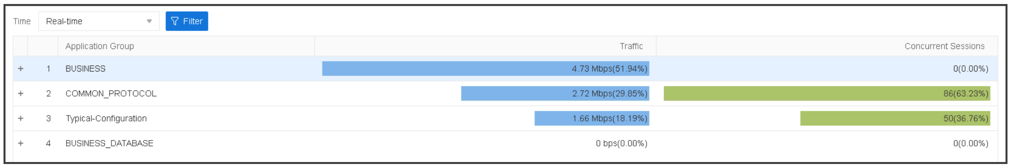
  - Traffic: Select the Traffic tab to display the traffic trends of selected application.

  - Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application.

  - Description: Select the Description tab to displays the detailed information of the selected application.

Group Details

Click **Monitor>Application Monitor>Group Details**.



		Application Group	Traffic	Concurrent Sessions
+	1	BUSINESS	4.73 Mbps(51.94%)	0(0.00%)
+	2	COMMON_PROTOCOL	2.72 Mbps(29.85%)	86(63.23%)
+	3	Typical-Configuration	1.66 Mbps(18.19%)	50(36.76%)
+	4	BUSINESS_DATABASE	0 bps(0.00%)	0(0.00%)

- Click **Time** drop-down menu to select a different Statistical_Period to view the statistical information in that periods of time.

- Click Filter button and select **Application Group** in the drop-down menu. You can search the desired application group by entering the keyword of the application group name in the text field.

- To view the detailed information of a certain application group, select the application group entry in the list, and click "+".

  - User (real-time): Select the Users (real-time)tab to display the detailed information of users who are using the selected application group. Click in details column, you can see the trends of the upstream traffic, downstream traffic, total traffic .

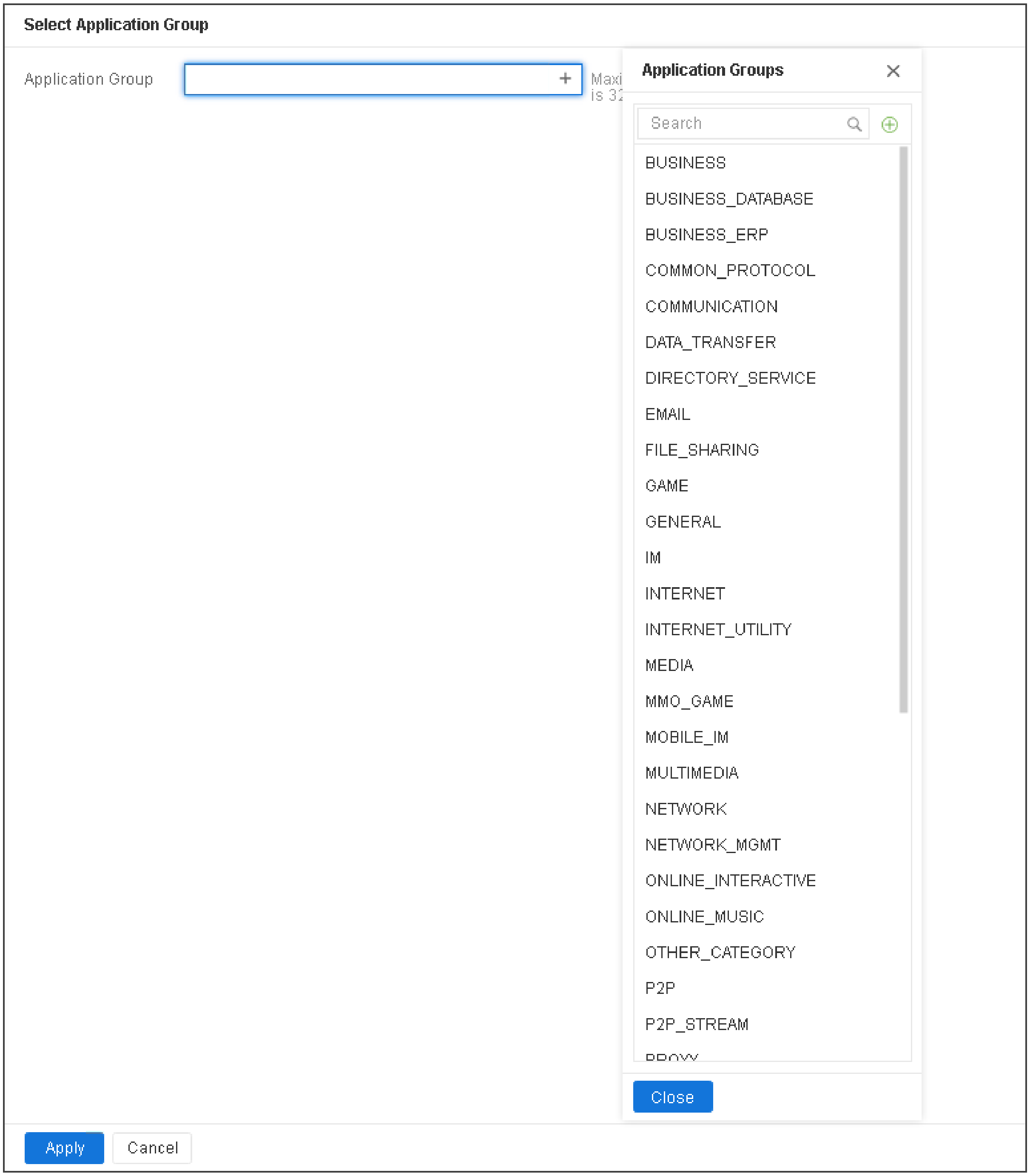
  - Application(real-time): Select the Application(real-time) tab to display the detailed information of applications in use which belongs to the selected application group. Click in details column to see the trends of the upstream traffic, downstream traffic, total traffic of the selected application.

  - Traffic: Select the Traffic tab to display the traffic trends of selected application group.

  - Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application group.

Select Application Group

Click **Monitor>Application Monitor>Select Application Group**. There are global application groups in the right column.



BUSINESS

BUSINESS_DATABASE

BUSINESS_ERP

COMMON_PROTOCOL

COMMUNICATION

DATA_TRANSFER

DIRECTORY_SERVICE

EMAIL

FILE_SHARING

GAME

GENERAL

IM

INTERNET

INTERNET_UTILITY

MEDIA

MMO_GAME

MOBILE_IM

MULTIMEDIA

NETWORK

NETWORK_MGMT

ONLINE_INTERACTIVE

ONLINE_MUSIC

OTHER_CATEGORY

P2P

P2P_STREAM

PROXY

In this page, you can perform the following actions:

- Click the desired address entry check box to add a new address entry to the left list.
- In the left list, click an address entry to remove it from the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click **Real-time** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Cloud Application Monitor

This feature may vary slightly on different platforms and not be available in VSYS on a part of platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

A cloud application is an application program that functions in the cloud. It resides entirely on a remote server and is delivered to users through the Internet.

Cloud application monitor page displays the statistics of cloud applications and users within a specified period (realtime, latest 1 hour, latest 1 day, latest 1 month), including application traffic, user number, and usage trend.

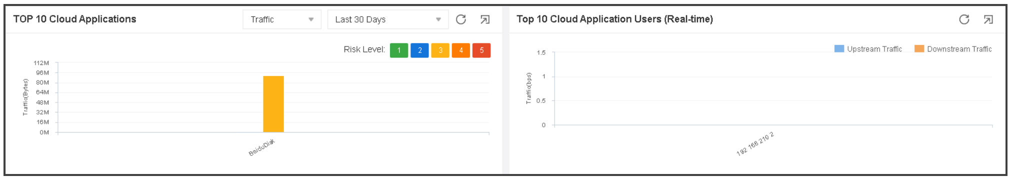
If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

The summary displays the following contents during a specified period:

- Top 10 cloud application rank by traffic/concurrent session number with in a specified period (realtime, latest 1 hour, latest 1 day, latest 1 month).
- Top 10 cloud application user rank by application number/traffic/concurrent session/new session.

Click **Monitor > Cloud Application Monitor> Summary**.

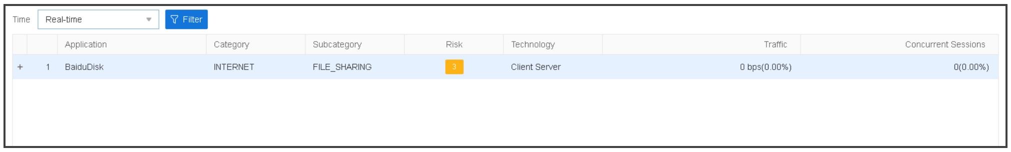


- By selecting different filters, you can view the statistics of different time period.
- By selecting the drop-down menu of trafficor concurrent sessions, you can view your intended statistics.

- Click the update ↻ icon to update the displayed data.
  - Hover your cursor over bar or pie chart to view exact data. Click the **Details** link on hover box, and you will jump to the **Cloud Application Details** page.

Cloud Application Details

Click **Monitor > Cloud Application Monitor>Cloud Application Details**.



Time Real-time Filter

		Application	Category	Subcategory	Risk	Technology	Traffic	Concurrent Sessions
+	1	BaiduDisk	INTERNET	FILE_SHARING	3	Client Server	0 bps(0.00%)	0(0.00%)

- Click the Time drop-down menu to select different time period to view the statistics in that period.
- Click the **Filter** button, and select **Application**. In the new text box, enter the name of your intended application.
- To view the detailed information of a certain application group, select the application group entry in the list and click + before it.
  - User(real-time): Select the Users(real-time)tab to display the detailed information of users who are using the selected application group. Click 🔍 in details column to see the trends of the upstream traffic, downstream traffic, total traffic .
  - Application(real-time): Select the Application(real-time) tab to display the detailed information of applications in use which belongs to the selected application . Click 🔍 in details column to see the trends of the upstream traffic, downstream traffic, total traffic of the selected application.
  - Traffic: Select the Traffic tab to display the traffic trends of selected application.

- Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application.
- Description: Select the Description tab to display the detailed description of the selected application.

Statistical Period

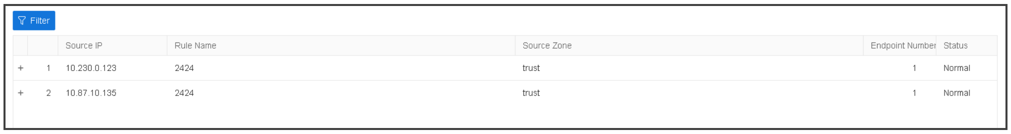
System supports the predefined time cycle and the custom time cycle. Click **Real-time** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Share Access Monitor

To detect the users' private behavior of shared access to the Internet, system supports to analyze the User-agent filed of HTTP packet, a share access detect method which is based on the application characteristic. The share access detect page can display the share access information with specified filter condition.

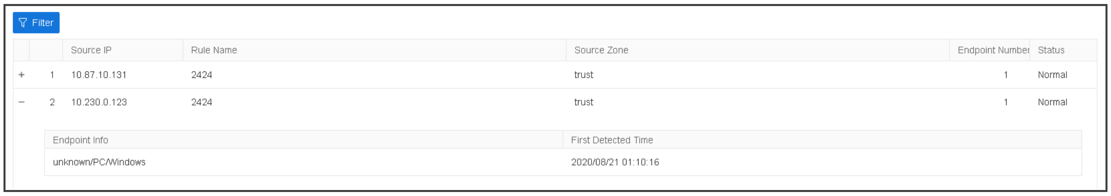
Click **Monitor> Share Access**.



		Source IP	Rule Name	Source Zone	Endpoint Number	Status
+	1	10.230.0.123	2424	trust	1	Normal
+	2	10.87.10.135	2424	trust	1	Normal

- Click Filter to select the condition in the drop-down list to search for the share access.
- Source IP: Displays the endpoints statistics of the specified source IP.
- Rule Name: Displays the endpoints statistics of the specified share access rule.
- Source Zone: Displays the endpoints statistics of the specified source zone.
- Endpoint Number: Displays the endpoints statistics of the specified endpoint number.
- Status: Displays the endpoints statistics of the specified status, including the normal status, logging status, warning status, and blocking status.

Move the mouse to **Endpoint Number** list, click + button, you will view the list of **Endpoint info** and **First Detection Time**.



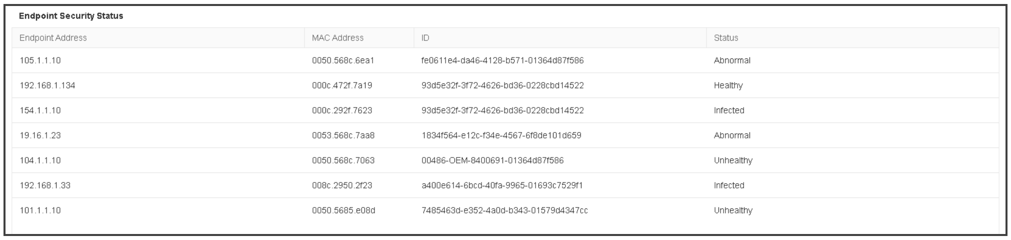
		Source IP	Rule Name	Source Zone	Endpoint Number	Status
+	1	10.87.10.131	2424	trust	1	Normal
−	2	10.230.0.123	2424	trust	1	Normal

Endpoint Info	First Detected Time
unknown/PC/Windows	2020/08/21 01:10:16

End Point Monitor

If system is configured with "Configuring End Point Security Control Center Parameters" on Page 753, the endpoint detect page displays the endpoint data information list synchronized with the endpoint security control center.

Click **Monitor** > **End Point Monitor**.



Endpoint Security Status

Endpoint Address	MAC Address	ID	Status
105.1.1.10	0050.568c.6ea1	fe0611e4-da46-4128-b571-01364d87f586	Abnormal
192.168.1.134	000c.472f.7a19	93d5e32f-3f72-4626-bd36-0228cbd14522	Healthy
154.1.1.10	000c.292f.7623	93d5e32f-3f72-4626-bd36-0228cbd14522	Infected
19.16.1.23	0053.568c.7aa8	1834f564-e12c-f34e-4567-6f8de101d659	Abnormal
104.1.1.10	0050.568c.7063	00486-OEM-8400691-01364d87f586	Unhealthy
192.168.1.33	008c.2950.2f23	a400e614-6bcd-40fa-9965-01693c7529f1	Infected
101.1.1.10	0050.5685.e08d	7485463d-e352-4a0d-b343-01579d4347cc	Unhealthy

iQoS Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

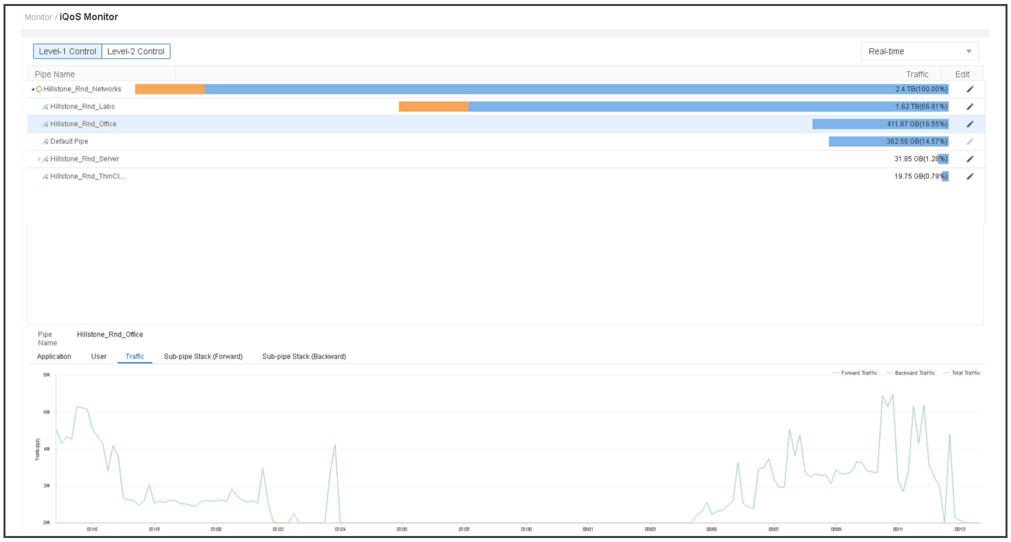
When the iQoS policy is configured and the function of iQoS is enabled, you can view the real-time traffic details or traffic trends of pipes and sub-pipes in Level-1 Control or Level-2 Control.

> **Notes:** The iQoS monitor function is controlled by license, To use the function, install the iQoS license.For more information on license, please refer to the License
> .

- Click the "Edit" button to edit the selected pipe.
- Mouse over the bar of the Traffic columns to see the forward and backward traffic of the pipe.

iQoS Details

Click **Monitor >iQoS Monitor** and enter the iQOS page. The pipe name and total traffic will be displayed in the list.



Monitor / **iQoS Monitor**

Pipe Name	Traffic	Edit
Hillstone_Rnd_Networks	2.4 TB(100.00%)	
Hillstone_Rnd_Labs	1.62 TB(66.81%)	
Hillstone_Rnd_Office	411.87 GB(16.55%)	
Default Pipe	362.58 GB(14.57%)	
Hillstone_Rnd_Server	31.85 GB(1.28%)	
Hillstone_Rnd_ThinCl...	19.75 GB(0.79%)	

Pipe Name: Hillstone_Rnd_Office

- Select the Level-1 Control or Level-2 Control button to display the pipe traffic of the selected level.
- In the Real-time ▾ drop-down list, select **Last 60 Minutes**, **Last 24 Hours, Last 7 Days** or **Last 30 Days** to display the pipe traffic of the selected period. The maximum period is 30 days.
- Click ◢ to expand sub-pipes.
- Click Edit to edit the selected pipe.
- Hover your mouse over the colorful lines of Traffic to view the forward traffic and backward traffic.

The traffic details of the selected pipe will be displayed at the bottom of the page, including traffic, sub-pipe stack (forward) and sub-pipe stack (backward).

- Traffic： Displays the trends of forward traffic, backward traffic and total traffic of pipes. Hover you mouse over the lines to view the forward traffic, backward traffic and total traffic in real time. When you click Forward Traffic, Backward Traffic or Total Traffic in the top right corner of trend chart, it will turn grey and the corresponded line will be hidden; when you click it again, it will turn black and the line will appear.
- Sub-pipe Stack (Forward)： Displays the trends of forward traffic of sub-pipes. Hover you mouse over the lines to view the top 5 traffic and other forward traffic of sub-pipes in real time. When you click the name of the specified sub-pipe in the top right corner of trend chart, it will turn grey and the corresponded line will be hidden; when you click it again, it will turn black and the line will appear.
- Sub-pipe Stack (Backward)： Displays the trends of backward traffic of sub-pipes. Hover you mouse over the lines to view the top 5 backward traffic and other backward traffic of sub-pipes in real time. When you click the name of the specified sub-pipe in the top right corner

of trend chart, it will turn grey and the corresponded line will be hidden; when you click it again, it will turn black and the line will appear.

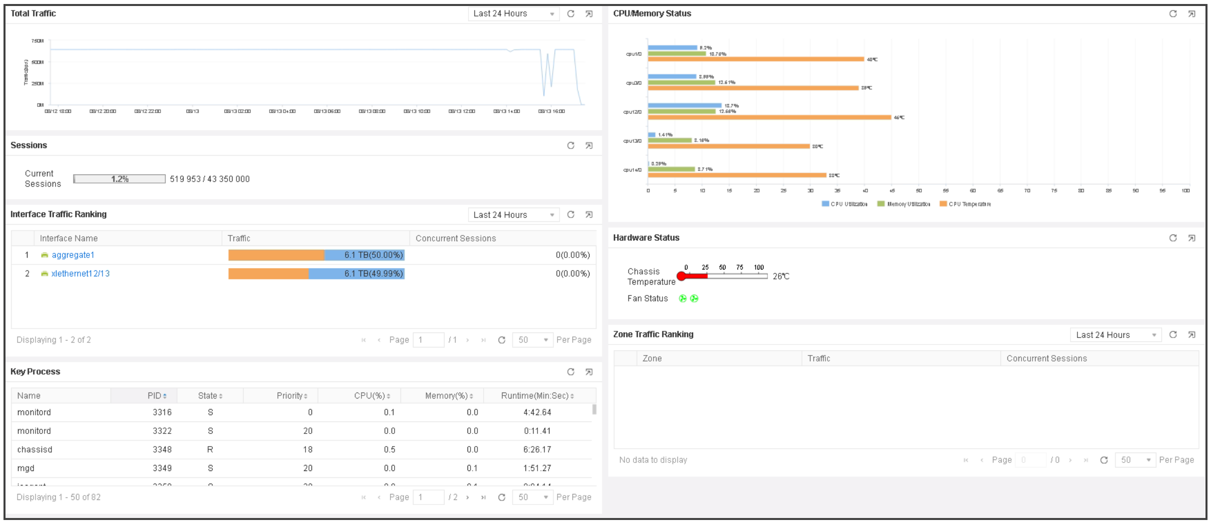
Device Monitor

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 Device page displays the device statistics within the specified period, including the total traffic, interface traffic, zone traffic, CPU/memory status, sessions, hardware status and online IP.

Summary

The summary displays the device statistics within last 24 hours. Click **Monitor>Device Monitor>Summary**.



Sessions

Current Sessions 1.2% 519 953 / 43 350 000

Interface Traffic Ranking Last 24 Hours

	Interface Name	Traffic	Concurrent Sessions
1	aggregate1	6.1 TB(50.00%)	0(0.00%)
2	xlethernet12/13	6.1 TB(49.99%)	0(0.00%)

Displaying 1 - 2 of 2 Page 1 / 1 50 Per Page

Key Process

Name	PID	State	Priority	CPU(%)	Memory(%)	Runtime(Min:Sec)
monitord	3316	S	0	0.1	0.0	4:42.64
monitord	3322	S	20	0.0	0.0	0:11.41
chassisd	3348	R	18	0.5	0.0	6:26.17
mgd	3349	S	20	0.0	0.1	1:51.27

Displaying 1 - 50 of 82 Page 1 / 2 50 Per Page

Hardware Status

Chassis Temperature 26℃

Fan Status

Zone Traffic Ranking Last 24 Hours

	Zone	Traffic	Concurrent Sessions

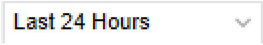
No data to display Page 0 / 0 50 Per Page

- Total traffic: Displays the total traffic within the specified statistical period.
    - Hover your mouse over the chart to view the total traffic statistics at a specific point in time.
    - Select a different Statistical Period to view the statistical information in that period of time.
    - If IPv6 is enabled, the device traffic will show the total traffic of IPv4 and IPv6.

- Interface traffic: Displays the upstream traffic, downstream traffic, total traffic and concurrent sessions of interface within the specified statistical period by rank.
    - Click **Traffic In**, **Traffic Out**, **Traffic**, or **Concurrent Sessions**. System displays the interface traffic according to the value(from large to small) of the specified object. By default, the interface traffic is displayed according to the total traffic value of interface.
    - Select a different Statistical Period to view the statistical information in that period of time.
    - Click the interface name to view the Detailed Information.
    - If IPv6 is enabled, the interface traffic will show the traffic of IPv4 and IPv6.
- Zone traffic: Displays the upstream traffic, downstream traffic, total traffic and concurrent sessions of zone within the specified statistical period by rank.
    - Click **Traffic In**, **Traffic Out**, **Traffic**, or **Concurrent Sessions**. System displays the zone traffic according to the value(from large to small) of the specified object. By default, the zone traffic is displayed according to the total traffic value of zone.
    - Select a different Statistical Period to view the statistical information in that period of time.
    - Click the zone name to view the Detailed Information.
- Hardware status: Displays the real-time hardware status, including storage, chassis temperature and fan status.
    - Storage: Displays the percentage of disk space utilization.
    - Internal Storage: Displays the percentage of hard disk utilization. Only E6368, E6168, E5568, E5268, E5168, E3968, E3668 and E2868 support this function.

        - Hover your mouse over the utilization to view the current utilization, the used storage size and the total storage size.
    - Chassis temperature: Displays the current CPU/chassis temperature.
    - Fan status: Displays the operation status of the fan. Green indicates normal, and red indicates error or a power supply module is not used.
- Sessions: Displays the current sessions utilization.
- CPU/memory status: Displays current CPU utilization, memory utilization and CPU temperature statistics.
    - Click legends of **CPU Utilization**, **Memory Utilization** or **CPU Temperature** to specify the histogram statistical objects. By default, it displays statistics of all objects.
- Key Process: Displays information about key processes on the device, including process name, PID, state, priority, and CPU percentage .

Statistical Period

System supports the predefined time cycle. Select statistical period from the drop-down menu 

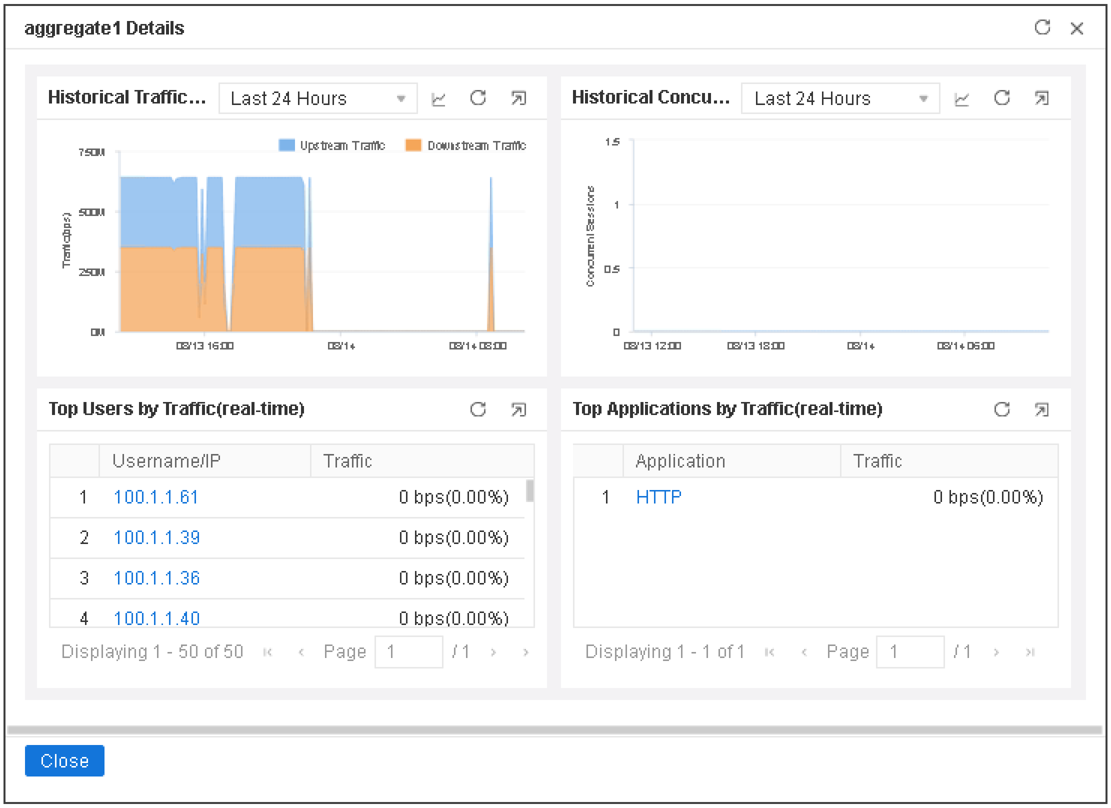
at the top right corner of some statistics page to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Detailed Information

The detailed information page displays detailed statistics of certain monitored objects. In addition, in the detailed information page, hover your mouse over the chart that represents a certain object to view the statistics of history trend and other information.

For example, click **agregate1** in the Interface Traffic , and the detailed information of ethernet0/0 appears.



aggregate1 Details

Historical Traffic... Last 24 Hours

Historical Concu... Last 24 Hours

Top Users by Traffic(real-time)

	Username/IP	Traffic
1	100.1.1.61	0 bps(0.00%)
2	100.1.1.39	0 bps(0.00%)
3	100.1.1.36	0 bps(0.00%)
4	100.1.1.40	0 bps(0.00%)

Displaying 1 - 50 of 50 Page 1 / 1

Top Applications by Traffic(real-time)

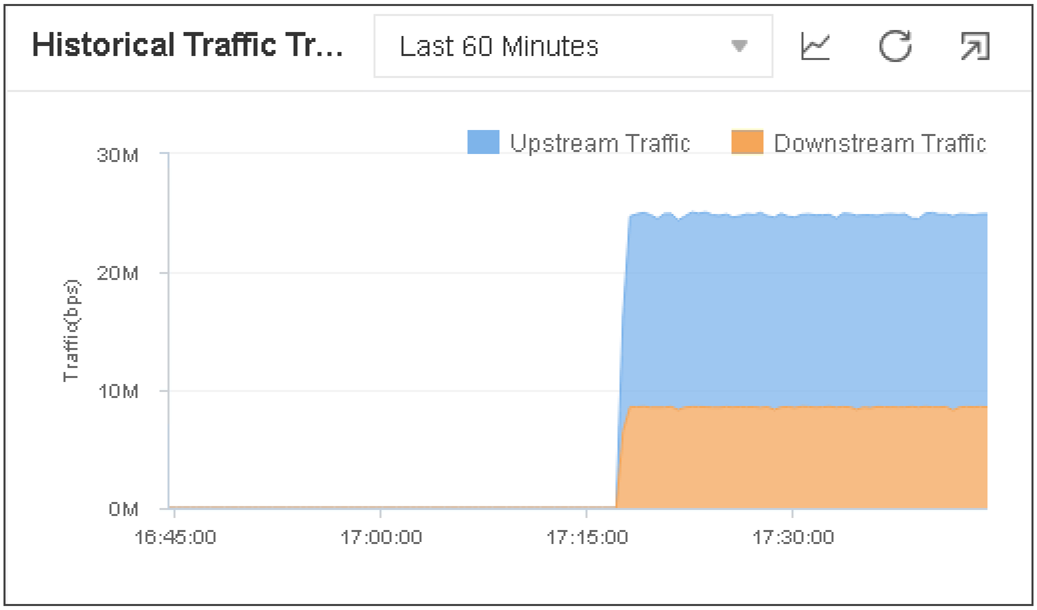
	Application	Traffic
1	HTTP	0 bps(0.00%)

Displaying 1 - 1 of 1 Page 1 / 1

Close

- Icon 📈 and 📊 are used to switch the line chart and stacked chart, which display the history trend of sessions and concurrent sessions.
- In traffic trend section, click legends of **Traffic In** or **Traffic Out** to specify the statistical objects. By default, it displays all statistical objects.

- In the User or Application section, click **Username/IP** or **Application** to display the real-time trend of the specified user or application. For example, the user traffic trend is shown as below.

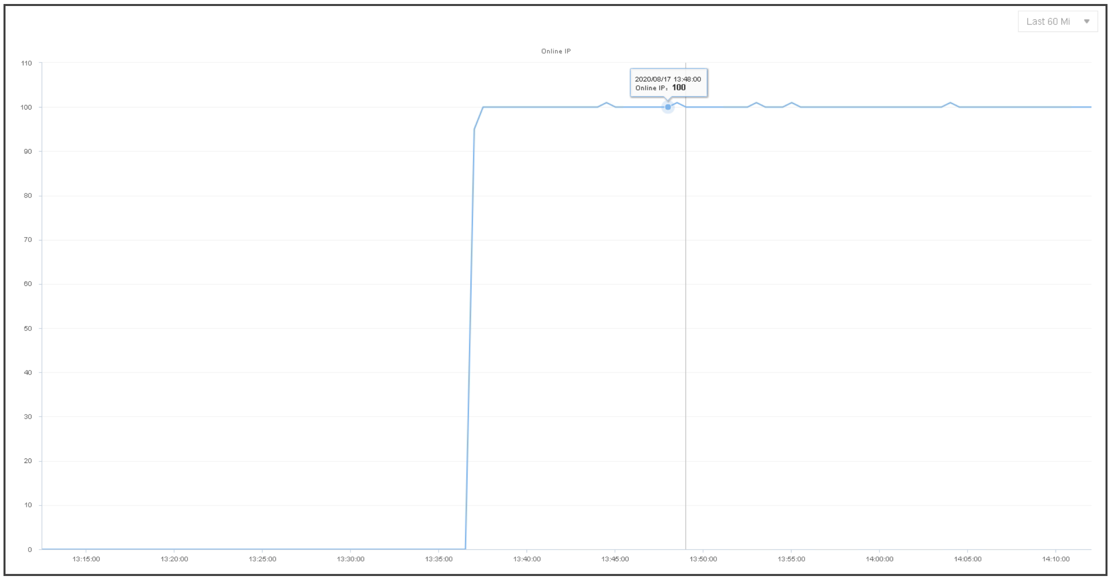


  - Select line chart or stacked chart from the pop-up menu Stacked Chart at the top right corner .

  - Hover your mouse over the chart to view the session statistics at a specific point in time.

Online IP

Click **Monitor>Device>Online IP** to view the historical trend of the number of online users. You can select the statistical period as last 60 minutes, last 24 hours or last 30 days.



- Hover your mouse over the line to view online users information.

URL Hit

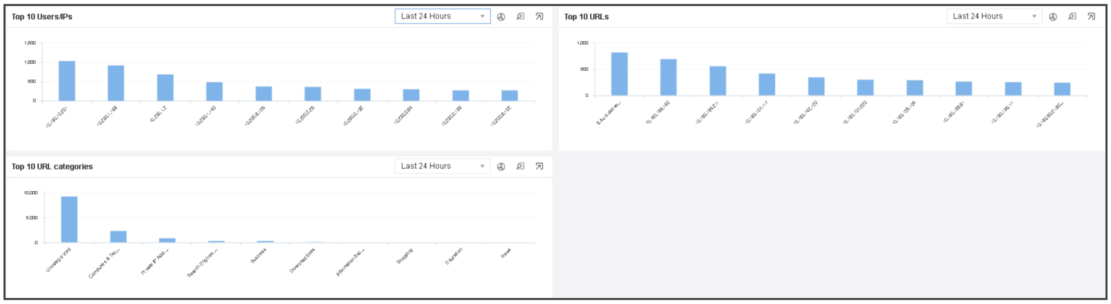
This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

If the " URL Filtering" on Page 659 function is enabled in the security policy rule, the predefined stat-set of URL filter can gather statistics on user/IPs, URLs and URL categories.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

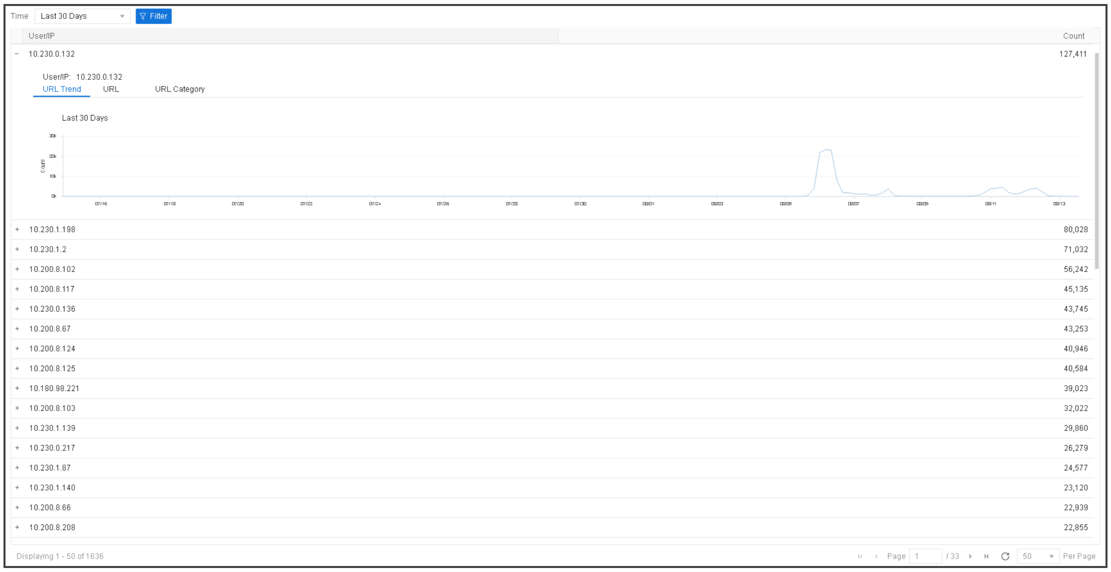
Click **Monitor> URL Hit>Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar, to view the hit count of User/IP, URL or URL Category .
- Click at top-right corner of every table and enter the corresponding details.
- Click and to switch between the bar chart and the pie chart.

User/IP

Click **Monitor> URL Hit>User/IP**.



User/IP: 10.230.0.132

User/IP	Count
− 10.230.0.132	127,411
+ 10.230.1.198	80,028
+ 10.230.1.2	71,032
+ 10.200.8.102	56,242
+ 10.200.8.117	45,135
+ 10.230.0.136	43,745
+ 10.200.8.67	43,253
+ 10.200.8.124	40,946
+ 10.200.8.125	40,584
+ 10.180.98.221	39,023
+ 10.200.8.103	32,022
+ 10.230.1.139	29,860
+ 10.230.0.217	26,279
+ 10.230.1.87	24,577
+ 10.230.1.140	23,120
+ 10.200.8.66	22,939
+ 10.200.8.208	22,855

Displaying 1 - 50 of 1636

Page 1 / 33 50 Per Page

- The User/IPs and detailed hit count are displayed in the list below.
- Click a User/IP in the list to display the corresponding URL hit statistics in the curve chart below.
    - Statistics: Displays the hit statistics of the selected User/IP, including the real-time statistics and statistics for the latest 1 hour, 24 hours 30 days .
    - URL(real-time): Displays the URLs' real-time hit count of selected User/IP. Click URL link ,you can view the corresponding URLs detailed statistics page. Click **Detail** link, you can view the URL hit trend of the selected User/IP in the **URL Filter Details**dialog .
    - URL category(real-time): Displays the URL categories' read-time hit count of selected User/IP. Click URL category link , you can view the corresponding URL categories' detailed statistics page. Click **Detail** link, you can view the URL category hit trend of the selected User/IP in the pop-up dialog .
- Click the **Filter** button at top-left corner. Select **User/IP** and you can search the User/IP hit count information by entering the keyword of the username or IP.

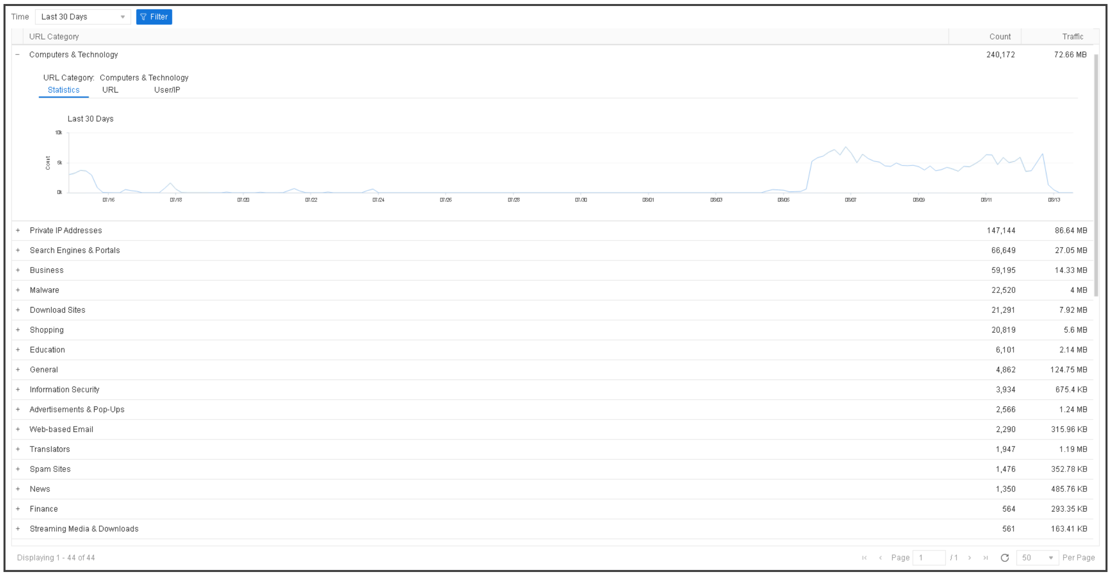
URL

Click **Monitor > URL Hit > URL**.

- The URL, URL category and detailed hit count are displayed in the list below.
- Click a URL in the list to view its detailed statistics.
  - Statistics: Displays the hit statistics of the selected URL, including the real-time statistics and statistics for the latest 1 hour, 24 hours 30 days .
  - User/IP(real-time): Displays the User/IP's real-time hit count of selected URL. Click the User/IP link and you can view the corresponding user/IPs detailed statistics page. Click the **Detail** link and you can view the URL hit trend of the selected user/IP in the **URL Filter Details** page.
- Click the **Filter** button at the top-left corner. Select **URL**and you can search the URL hit count information by entering the keyword of the URL.
- Click↻to refresh the real-time data in the list.

URL Category

Click **Monitor> URL Hit > URL Category**.



URL Category	Count	Traffic
− Computers & Technology	240,172	72.66 MB
+ Private IP Addresses	147,144	86.64 MB
+ Search Engines & Portals	66,649	27.05 MB
+ Business	59,195	14.33 MB
+ Malware	22,520	4 MB
+ Download Sites	21,291	7.92 MB
+ Shopping	20,819	5.6 MB
+ Education	6,101	2.14 MB
+ General	4,862	124.75 MB
+ Information Security	3,934	675.4 KB
+ Advertisements & Pop-Ups	2,566	1.24 MB
+ Web-based Email	2,290	315.96 KB
+ Translators	1,947	1.19 MB
+ Spam Sites	1,476	352.78 KB
+ News	1,350	485.76 KB
+ Finance	564	293.35 KB
+ Streaming Media & Downloads	561	163.41 KB

Displaying 1 - 44 of 44

- The URL category, count, traffic are displayed in the list.
- Click a URL category in the list to view its detailed statistics displayed in the Statistics, URL (real-time), User/IP(real-tiime) tabs.
  - Statistics: Displays the trend of the URL category visits, including the real-time trend and the trend in the last 60 minutes, 24 hours , 30 days.
  - URL(real-time): Displays the visit information of the URLs, contained in the URL category, that are being visited.
  - User/IP(real-time): Displays the visit information of the users or IPs that are visiting the URL category.
- Click ↻ to refresh the real-time data in the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click the time button on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

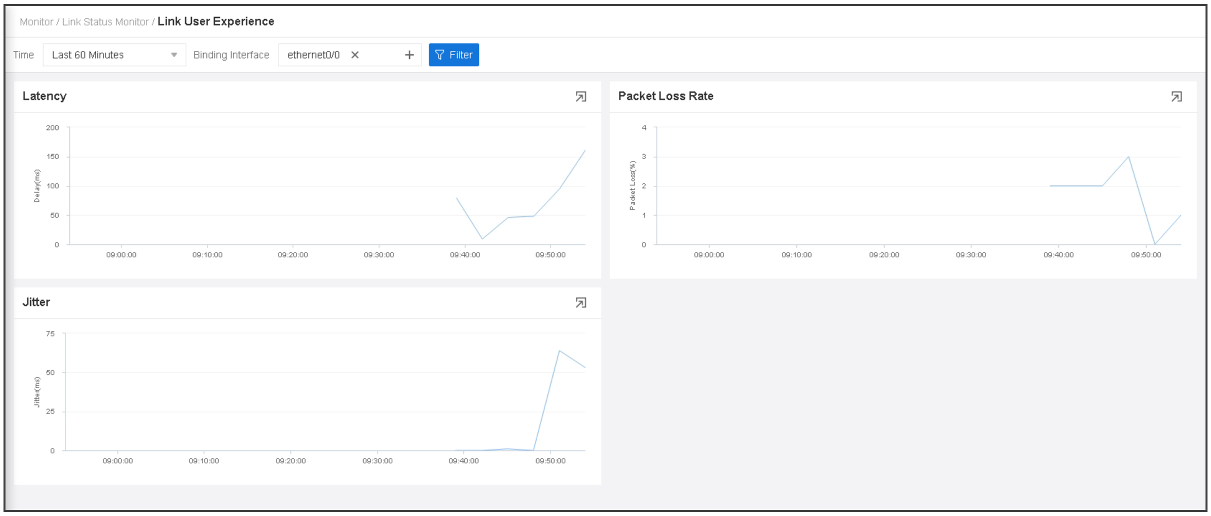
Link Status Monitor

Link status monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, and jitter, to monitor and display the overall status of the link. System also supports for link detection to calculate the traffic information of the specific destination IP address in the link, including latency, and jitter.

Link User Experience

The link user experience page displays the traffic statistics of the interfaces that have been bound within a specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month)

Click **Monitor > Link Status Monitor.** For more information about configuration of binding interfaces, refer to Link Configuration.



Monitor / Link Status Monitor / Link User Experience

Time: Last 60 Minutes
Binding Interface: ethernet0/0

- Select a different Statistical_Period to view the statistical information in that periods of time.

- Select the binding interface **Binding Interface** drop-down list, Click the **Binding Interface** drop-down menu and select the interface name to view the link status monitoring statistics for this interface. You can select multiple interfaces.

- Click Filter button and select **Application** in the drop-down menu. You can select the TOP 10 or Application / Application group name to view the link status monitoring statistics according to the specified application

Notes:

- "Time" and "Binding Interface" are required in the filter condition.
- If the application switch of the specified interface is not enabled in the link configuration, the **Application** filter condition cannot be added.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click **Last 60 Minutes** on the top right corner of each tab to set the time cycle.

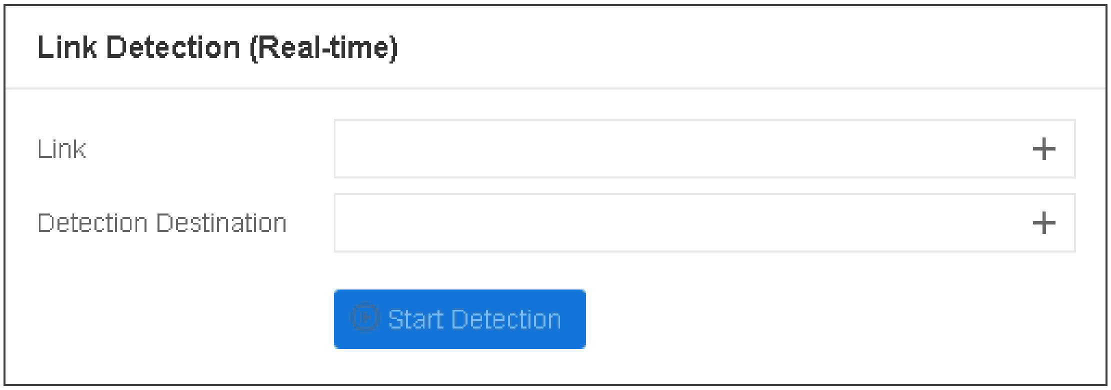
- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Link Detection

The link detection page displays real-time traffic statistics of specified detection destination IP to link or link to detection destination IP, include latency, and jitter.

To configure the link detection, take the following steps:

1. Click **Monitor** > **Link Status Monitor** > **Link Detection**.



2. Select the interface name to view the link status monitoring statistics for this interface, you can select up to 8 interfaces. Click **New** to add interfaces, you can add up to 16 interfaces. For more information about configuration of binding interfaces, refer to Link Configuration.

3. Select the IP address to view the link status monitoring statistics for this destination address, you can select up to 8 addresses. Click **New** to add destination address, you can add up to 32 addresses. For more information about configuration of destination addresses, refer to Detection Destination.

4. Click **Start Detection**, and view the statistics of the real-time link detection at the bottom of the page. Select **Detection Destination IP->Link** or **Link->Detection Destination IP** tab to view the trend chart of latency and jitter. Click Trend Chart and Table to switch between the trend chart and table.

5. Click **End Detection** to end the real-time link detection

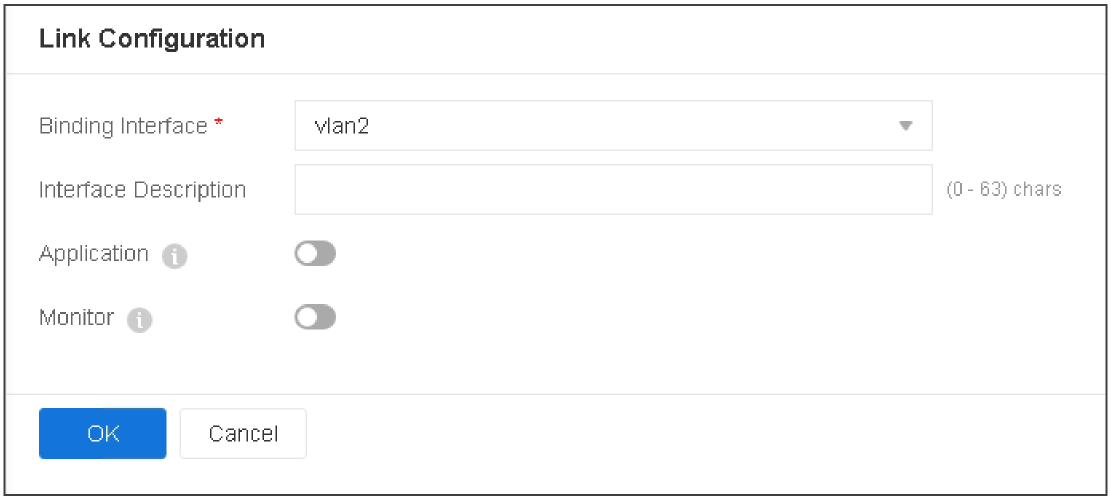
Link Configuration

In the link configuration page, you can configure the binding interface to monitor the link state and can enable the application switch and link user experience.

To configure the link, take the following steps:

1. Click **Monitor > Link Status Monitor > Link Configuration**.

2. Click **New**.



Link Configuration

Binding Interface * vlan2

Interface Description (0 - 63) chars

In the Link Configuration page, configure these values

Option	Description
Binding Interface	Select the interface in the drop down menu.
Interface Description	Type the description for the interface.
Application	Click the **Enable** button. After enabling, you can see details of the specific application in this interface.
Monitor	Click the **Enable** button. After enabling, you can see traffic statistics in this interface.

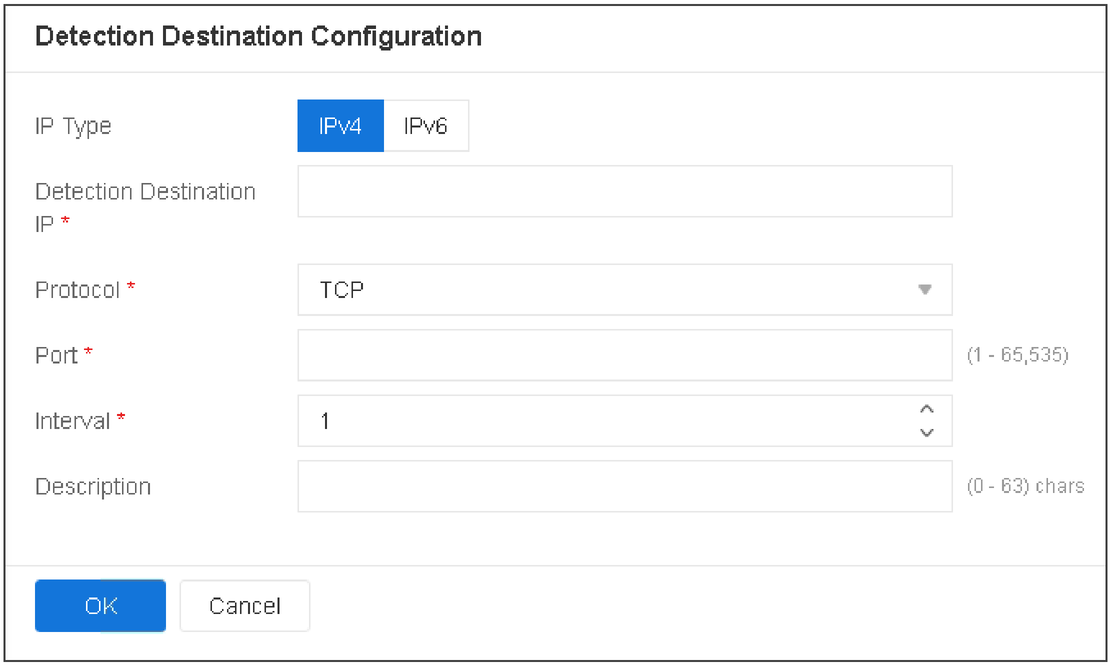
3. Click **OK**.

Detection Destination

In the detection destination page, you can configure the destination IP address to monitor the link state.

To configure the detection destination, take the following steps:

1. Click **Monitor** > **Link Status Monitor** > **Detection Destination**
2. Click **New**.



Detection Destination Configuration

IP Type: IPv4 | IPv6

Detection Destination IP *

Protocol *: TCP

Port *: (1 - 65,535)

Interval *: 1

Description: (0 - 63) chars

In the Detection Destination Configuration page, configure these values

Option	Description
IP Type	Select the IP address type, include IPv4 or IPv6.
Detection Destination IP	Specifies the IP address of the detection destination.

Option	Description
Protocol	Specifies the protocol of the detection destination, include TCP or ICMP.
Port	Specifies the port number of the detection destination.
Interval	Specifies the interval time of the detection packet. The value range is 1 to 5 seconds, the default value is 1.
Description	Type the description for the detection destination

3. Click **OK**.

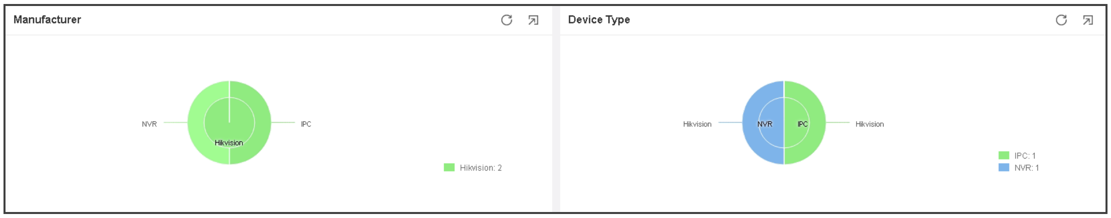
IoT Monitor

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.

Summary

On the Summary page, you can obtain the real-time distribution of manufacturers and device types.

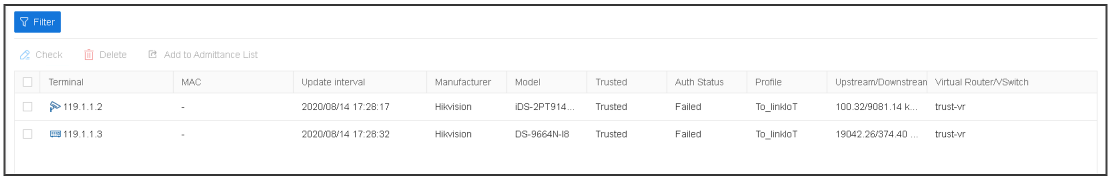
Click **Monitor** > **IoT Monitor** > **Summary**.



- Click the ↻ button to refresh the monitoring data.
- Hover your mouse over the bar chart to view the device number of different manufacturers and different device types.
- Different manufactures and devices are marked with different colors of legends. When your mouse hovers over an legend, the corresponded part will be highlighted on the bar chart.

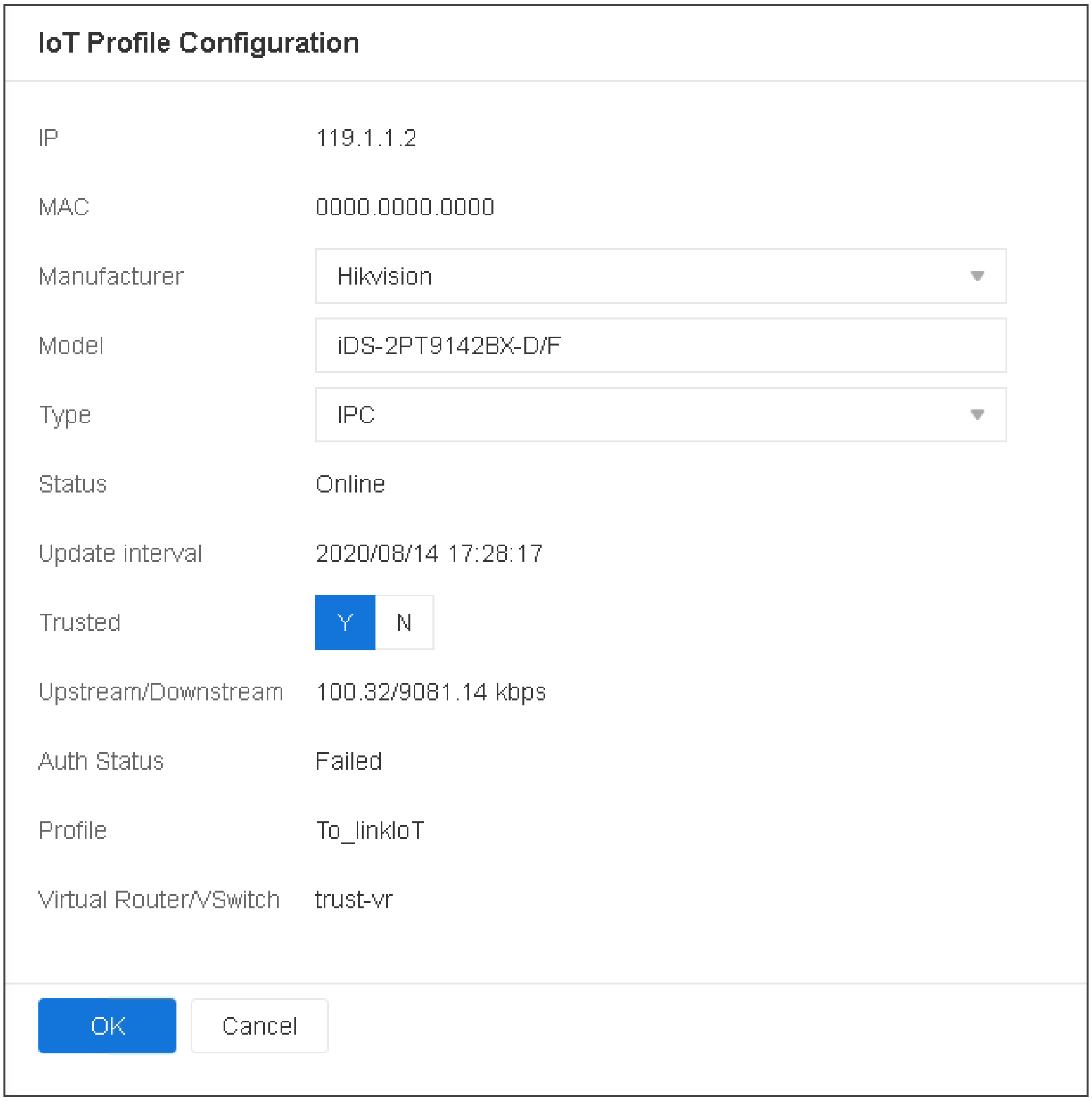
Details

Click **Monitor** > **IoT Monitor** > **Details** to view the detailed information of the network video monitoring devices.



□	Terminal	MAC	Update interval	Manufacturer	Model	Trusted	Auth Status	Profile	Upstream/Downstrean	Virtual Router/VSwitch
□	119.1.1.2	-	2020/08/14 17:28:17	Hikvision	iDS-2PT914...	Trusted	Failed	To_linkIoT	100.32/9081.14 k...	trust-vr
□	119.1.1.3	-	2020/08/14 17:28:32	Hikvision	DS-9664N-I8	Trusted	Failed	To_linkIoT	19042.26/374.40 ...	trust-vr

- 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 modify the manufacturer, model, type and trust status manually. The manually changed configuration is prior to the automatically detected result. When the device logs in again, the manually changed configurations will be cleared.



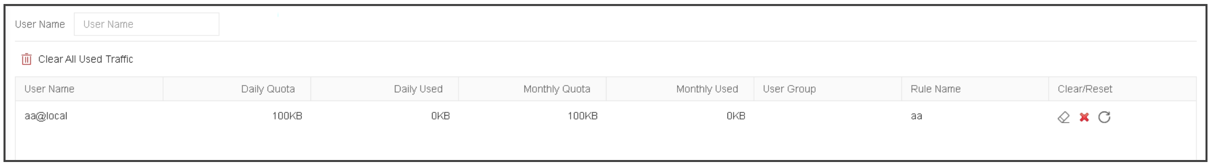
IoT Profile Configuration

IP	119.1.1.2
MAC	0000.0000.0000
Manufacturer	Hikvision
Model	iDS-2PT9142BX-D/F
Type	IPC
Status	Online
Update interval	2020/08/14 17:28:17
Trusted	[✓ Y] N
Upstream/Downstream	100.32/9081.14 kbps
Auth Status	Failed
Profile	To_linkIoT
Virtual Router/VSwitch	trust-vr

- 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.
- 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.

User Quota Monitor

After the "Traffic Quota" on Page 886 function is configured, the user quota detect page displays the user traffic quota statistics list, including the user's daily/ monthly quota, daily/ monthly used traffic value, the user group, and the corresponding traffic quota rule name.



User Name: User Name

Clear All Used Traffic

User Name	Daily Quota	Daily Used	Monthly Quota	Monthly Used	User Group	Rule Name	Clear/Reset
aa@local	100KB	0KB	100KB	0KB		aa	◇ ✖ ↻

- Type the user name into the **User Name** text box to filter the user traffic quota statistics for the specified name.
- Click ◇ in the **Clear/Reset** column of the list to clear the selected user daily used traffic.
- Click ✖ in the **Clear/Reset** column of the list to clear the selected user monthly used traffic.

- Click ↻ in the **Clear/Reset** column of the list to reset all used traffic for the selected user.
- Click **Clear All Used Traffic** to clear all used traffic of all users in the list.

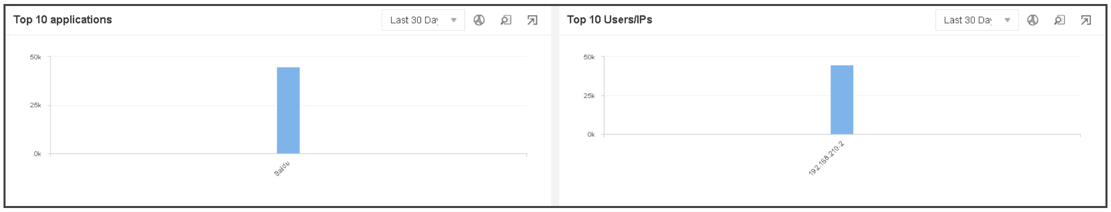
Application Block

If system is configured with "Security Policy" on Page 768 the application block can gather statistics on the applications and user/IPs.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

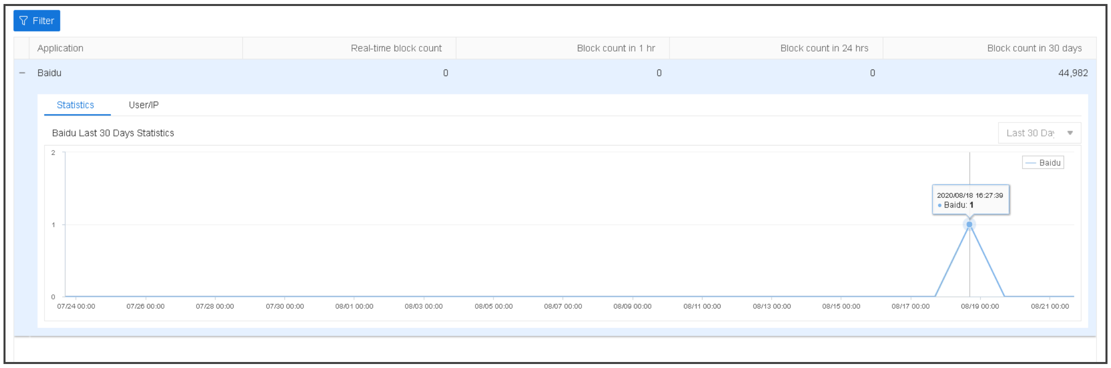
The summary displays the application block's statistics on the top 10 applications and top 10 user/IPs. Click **Monitor>Application Block> Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar to view the block count on the applications and user/IPs.
- Click to switch between the bar chart and the pie chart.
- Click to close the chart.
- Click at the top-right corner of every table and enter the corresponding details page.

Application

Click **Monitor>Application Block> Application**.



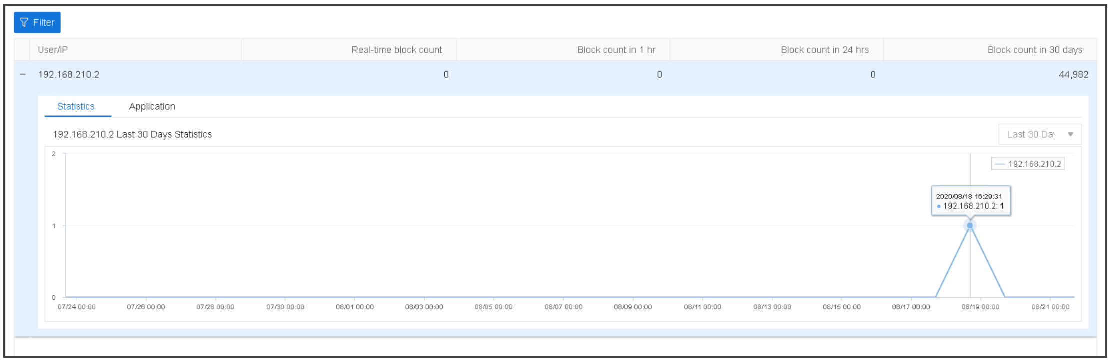
	Application	Real-time block count	Block count in 1 hr	Block count in 24 hrs	Block count in 30 days
−	Baidu	0	0	0	44,982

Baidu Last 30 Days Statistics

- The applications and detailed block count are displayed in the list.
- To view the corresponding information of application block on the applications and user/IPs, select the application entry in the list, and click "+".
    - Statistics: Displays the block count statistics of the selected application, including the real-time statistics and statistics for the latest 1 hour, 24 hours and 30 days.
    - User/IP: Displays the user/IPs that are blocked from the selected application. Click a user/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.
- Click Filter to select the condition in the drop-down list. You can search the application block information by entering the keyword of the application name.
- Click to refresh the real-time data in the list.

User/IP

Click **Monitor>Application Block> User/IP**.



Filter

	User/IP	Real-time block count	Block count in 1 hr	Block count in 24 hrs	Block count in 30 days
−	192.168.210.2	0	0	0	44,982

Statistics | Application

192.168.210.2 Last 30 Days Statistics

Last 30 Day

- The user/IP and detailed block count are displayed in the list.
- Click a user/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.
- Click Filter to select the condition in the drop-down list. You can search the users/IPs information.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click (Real-time ▾) on the top right corner of each tab to set the time cycle.

- Real-time: Displays the statistical information within the realtime.
- Last Hour: Displays the statistical information within the latest 1 hour.
- Last Day: Displays the statistical information within the latest 1 day.
- Last Month: Displays the statistical information within the latest 1 month.

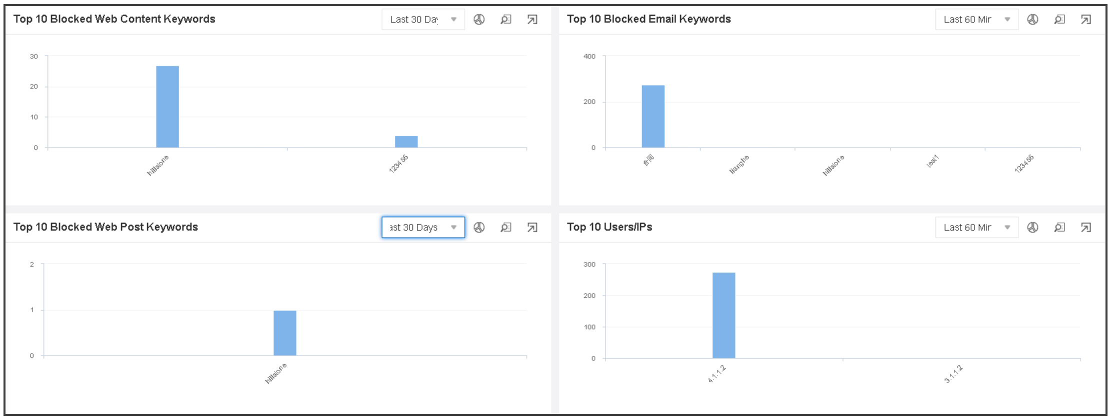
Keyword Block

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

If system is configured with "Web Content" on Page 712, "Email Filter" on Page 724, or "Web Posting" on Page 718, the predefined stat-set of the Keyword Block can gather statistics on the Web keyword, Web keywords, email keywords, posting keywords and users/IPs.

Summary

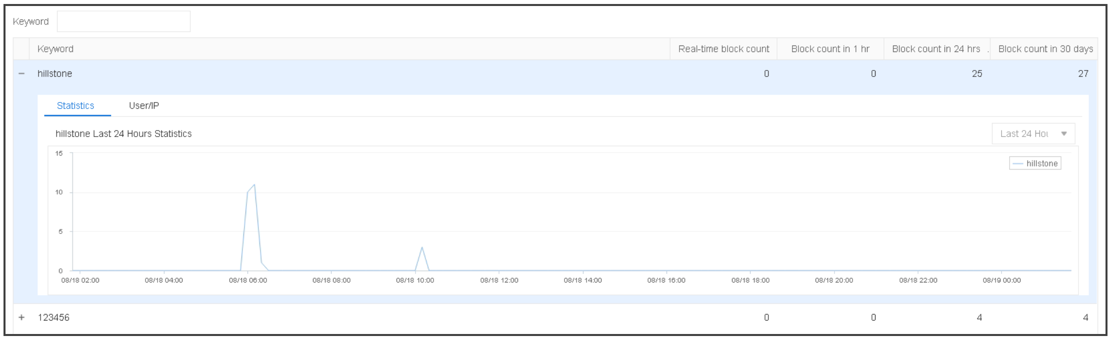
The summary displays the predefined stat-set of the Keyword Block that can gather statistics on the top 10 hit Web keywords, the top 10 hit email keywords, the top 10 posting keywords, and the top 10 users/IPs. Click **Monitor > Keyword Block > Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar to view the block count on the keywords .
- Click 🔍 at the top-right corner of every table and enter the corresponding details page.
- Click ☮ to switch between the bar chart and the pie chart.

Web Content

Click **Monitor>Keyword Block> Web Content**.



Keyword

	Keyword	Real-time block count	Block count in 1 hr	Block count in 24 hrs	Block count in 30 days
−	hillstone	0	0	25	27
+	123456	0	0	4	4

Statistics User/IP

hillstone Last 24 Hours Statistics

- The Web content and detailed block count are displayed in the list below.
- To view the corresponding information of keyword block on the Web content, select the keyword entry in the list.
  - Statistics: Displays the statistics of the selected keyword, including the real-time statistics and statistics for the latest 1 hour, 24 hours and 30 days.
  - User/IP: Displays the user/IPs that are blocked by the selected keyword. Click a user-/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.
- Click Filter to select the condition in the drop-down list. You can search the keyword block information by entering the keyword .
- Click ↻to refresh the real-time data in the list.

Email Content

Click **Monitor>Keyword Block> Email Content**.

For a page description, see Web_Content.

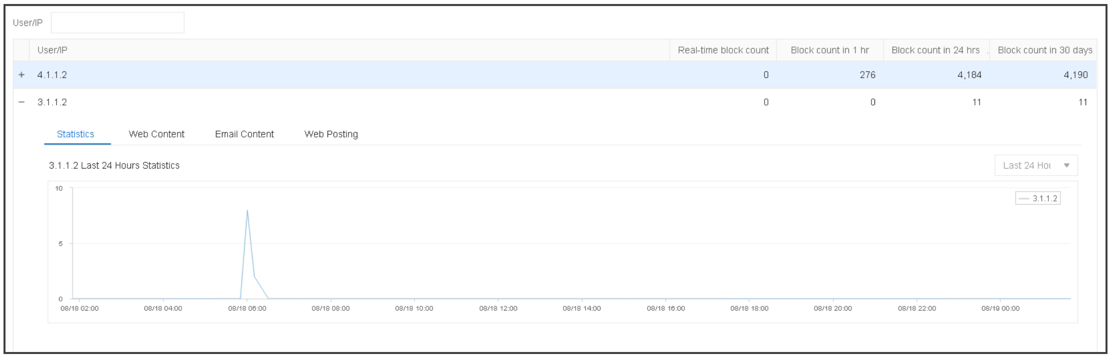
Web Posting

Click **Monitor>Keyword Block>Web Posting**.

For a page description, see Web_Content.

User/IP

Click **Monitor>Keyword Block>User/IP**.



User/IP

	User/IP	Real-time block count	Block count in 1 hr	Block count in 24 hrs	Block count in 30 days
+	4.1.1.2	0	276	4,184	4,190
−	3.1.1.2	0	0	11	11

- The user/IP and detailed block count are displayed in the list below.
- Click a user/IP in the list to display the corresponding statistics , Web content, Email Content, Web Posting in the curve chart below. Click to jump to the corresponding detail page.
- Click Filter to select the condition in the drop-down list. You can search the users/IPs information .

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click (Real-time ▾) on the top right corner of each tab to set the time cycle.

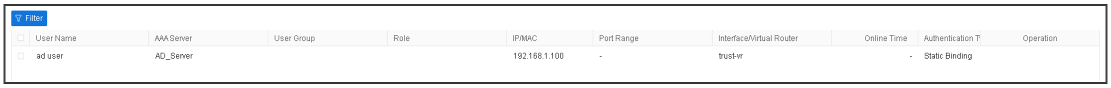
- Real-time: Displays the current statistical information.
- Last Hour: Displays the statistical information within the latest 1 hour.

- Last Day: Displays the statistical information within the latest 1 day.
- Last Month: Displays the statistical information within the latest 1 month.

Authentication User

If system is configured with"Web Authentication" on Page 302, "1Single Sign-On" on Page 314, "SSL VPN" on Page 410, "L2TP VPN" on Page 523 the authentication user can gather statistics on the authenticated users.

Click **Monitor>Authenticated User**.



□	User Name	AAA Server	User Group	Role	IP/MAC	Port Range	Interface/Virtual Router	Online Time	Authentication T	Operation
□	ad user	AD_Server			192.168.1.100	-	trust-vr	-	Static Binding	

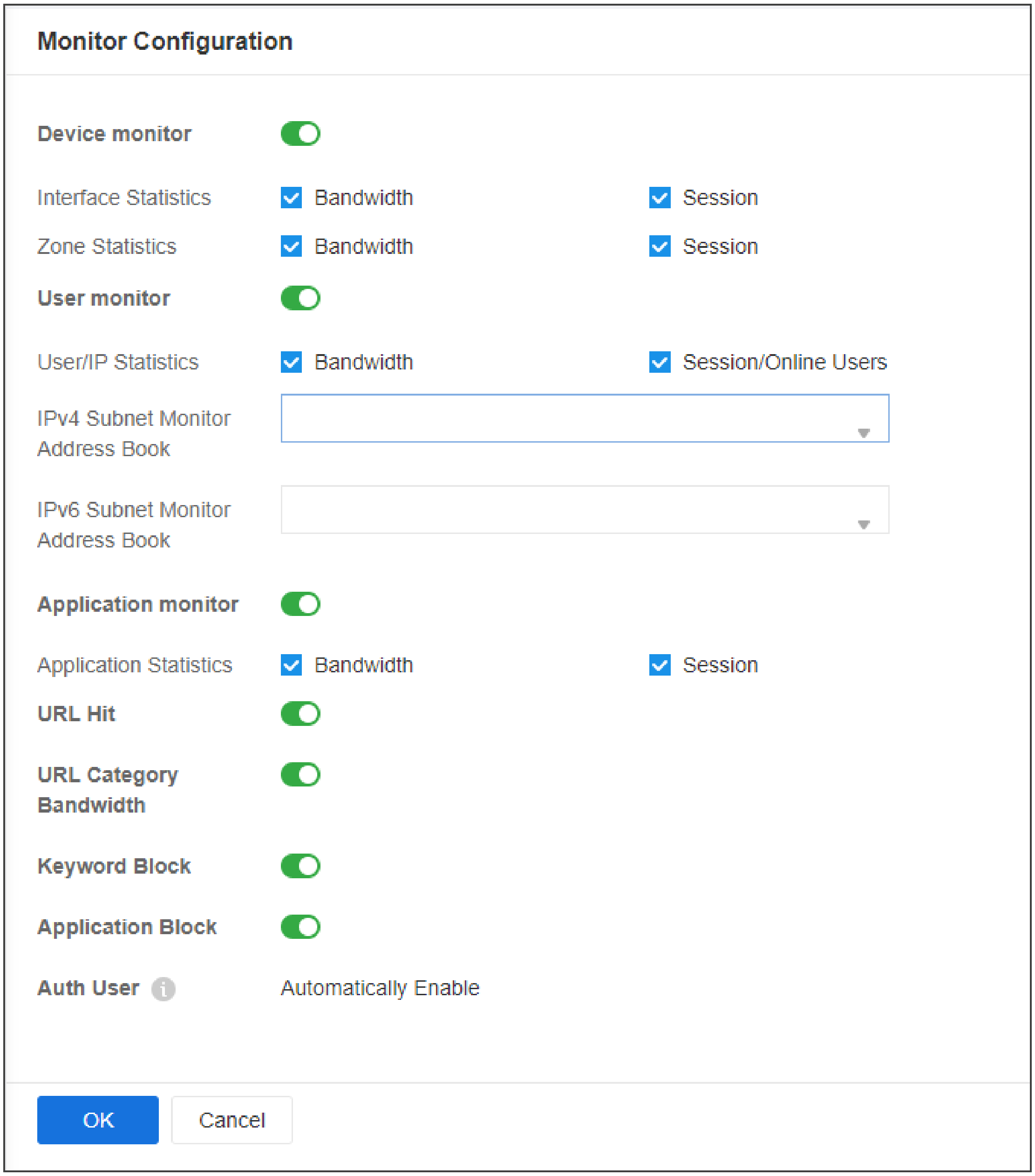
- Click Filter to select the condition in the drop-down list to filter the users.
- Click **Kick Out** under the Operation column to kick the user out.
- Click↻to refresh the real-time data in the list.

Monitor Configuration

You can enable or disable some monitor items as needed. The monitor items for Auth user are enabled automatically.

To enable/disable a monitor item, take the following steps:

1. Click **Monitor > Monitor Configuration**.



Monitor Configuration

Device monitor ●

Interface Statistics ☑ Bandwidth ☑ Session

Zone Statistics ☑ Bandwidth ☑ Session

User monitor ●

User/IP Statistics ☑ Bandwidth ☑ Session/Online Users

IPv4 Subnet Monitor Address Book

IPv6 Subnet Monitor Address Book

Application monitor ●

Application Statistics ☑ Bandwidth ☑ Session

URL Hit ●

URL Category Bandwidth ●

Keyword Block ●

Application Block ●

Auth User Automatically Enable

2. Select or clear the monitor item(s) you want to enable or disable.
3. Select subnet monitor address book in the IPv4 Subnet Monitor Address Book or IPv6 Subnet Monitor Address Book drop-down list. The system will match the traffic which is sent from the Internet to Subnet according to the specified address. If matched, the traffic will be counted to the Subnet side.
4. entry.
5. Click **OK**.

Notes: After a monitor item is enabled or disabled in the root VSYS, the item of all VSYSs will be enabled or disabled(except that the non-root VSYS does not support this monitor item). You can not enable or disable monitor item in non-root VSYSs.

User-defined Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

A user-defined stat-set provides a more flexible approach to view the statistics. You can view the statistics as needed. The statistical data may vary in the data types you have selected.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

The IP type-based statistical information table.

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
No direction	Initiator	Statistics on the traffic of the initiator's IP	Statistics on the session number of the initiator's IP	Statistics on the new sessions of the initiator's IP	Statistics on the URL hit count of the specified IPs	Statistics on the keyword block count of the specified IPs	Statistics on the application block count of the specified IPs
	Responder	Statistics on the traffic of the responder's IP	Statistics on the session number of the respon-	Statistics on the new sessions of the respon-			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
			der's IP	der's IP			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Belong to zone	Statistics on the traffic of an IP that belongs to a specific security zone	Statistics on the session number of an IP that belongs to a specific security zone	Statistics on the new sessions of an IP that belongs to a specific security zone			
	Not belong to zone	Statistics on the traffic of an IP that does not belong to a specific security zone	Statistics on the session number of an IP that does not belong to a specific security	Statistics on the new sessions of an IP that does not belong to a specific security			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
			zone	zone			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Belong to interface	Statistics on the traffic of an IP that belongs to a specific interface	Statistics on the session number of an IP that belongs to a specific interface	Statistics on the new sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the traffic of an IP that does not belong to a specific interface	Statistics on the session number of an IP that does not belong to a specific inter-	Statistics on the new sessions of an IP that does not belong to a specific inter-			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
			face	face			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
Bi-directional	Initiator	Statistics on the inbound and outbound traffic of the initiator's IP	Statistics on the number of received and sent sessions of the initiator's IP	Statistics on the new received and sent sessions of the initiator's IP			
	Responder	Statistics on the inbound and outbound traffic of the responder's IP	Statistics on the number of received and sent sessions of the responder's IP	Statistics on the new received and sent sessions of the responder's IP			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Belong to zone	Statistics on the inbound and outbound traffic of an IP that belongs to a specific security zone	Statistics on the number of received and sent sessions of an IP that belongs to a specific security zone	Statistics on the new received and sent sessions of an IP that belongs to a specific security zone			
	Not belong to zone	Statistics on the inbound and outbound traffic of an IP that	Statistics on the number of received and sent sessions of an IP	Statistics on the new received and sent sessions of an IP that			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		does not belong to a specific security zone	that does not belong to a specific security zone	does not belong to a specific security zone			
	Belong to interface	Statistics on the inbound and outbound traffic of an IP that belongs to a specific interface	Statistics on the number of received and sent sessions of an IP that belongs to a specific interface	Statistics on the new received and sent sessions of an IP that belongs to a specific interface			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Not belong to interface	Statistics on the inbound and outbound traffic of an IP that does not belong to a specific interface	Statistics on the number of received and sent sessions of an IP that does not belong to a specific interface	Statistics on the new received and sent sessions of an IP that does not belong to a specific interface			

The interface, zone, user, application, URL, URL category, VSYS type-based statistical information table.

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
Zone	No direction	Statistics on the traffic of the specified security zones	Statistics on the session number of the specified security zones	Statistics on the new sessions of the specified security zones	Statistics on the URL hit count of the specified security zones	N/A	N/A
	Bi-directional	Statistics on the inbound and outbound traffic of the specified security zones	Statistics on the number of received and sent sessions of the specified security zones	Statistics on the new received and sent sessions of the specified security zones			
Interface	No direction	Statistics on	Statistics on	Statistics on	Statistics	N/A	N/A

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		the traffic of the specified interfaces	the session number of the specified interfaces	the new sessions of the specified interfaces	on the URL hit count of the specified interfaces		
	Bi-directional	Statistics on the inbound and outbound traffic of the specified interfaces	Statistics on the number of received and sent sessions of the specified interfaces	Statistics on the new received and sent sessions of the specified interfaces			
Application	N/A	Statistics on the traffic	Statistics on the session	Statistics on the new sessions	N/A	N/A	Statistics on the block

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		of the specified applications	number of the specified applications	of the specified applications			count of the specified applications
User	No direction	Statistics on the traffic of the specified users	Statistics on the session number of the specified users	Statistics on the new sessions of the specified users	Statistics on the URL hit count of the specified users	Statistics on the keyword block count of the specified users	Statistics on the application block count of the specified users
	Bi-directional	Statistics on the inbound and outbound traffic of the specified users					

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
URL	N/A	N/A	N/A	N/A	Statistics on the hit count of the specified URLs	N/A	N/A
URL Category	N/A	N/A	N/A	N/A	Statistics on the hit count of the specified URL categories	N/A	N/A
VSYS	N/A	Statistics on the traffic	Statistics on the session	Statistics on the new sessions	Statistics on the URL	N/A	N/A

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		of the specified VSYSs	number of the specified VSYSs	of the specified VSYSs	hit count of the specified VSYSs		

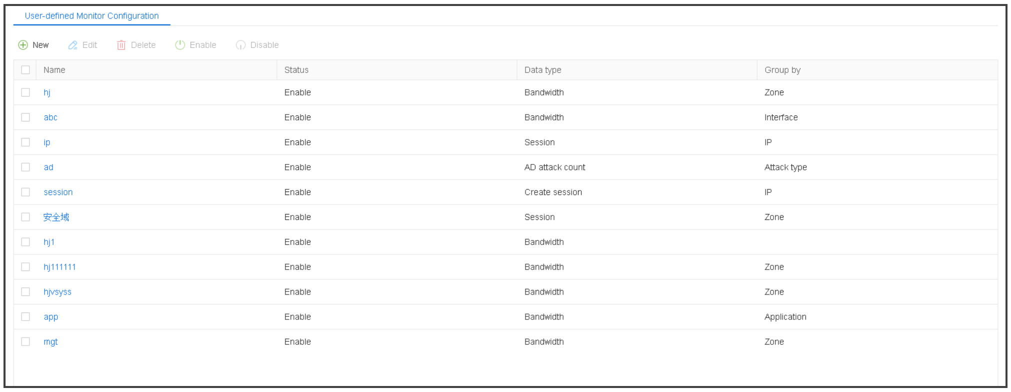
You can configure a filtering condition for the stat-set to gather statistics on the specified condition, such as statistics on the session number of the specified security zone, or the traffic of the specified IP.

The filtering conditions supported table.

Type	Description
filter zone	Data is filtered by security zone.
filter zone zone-name ingress	Data is filtered by ingress security zone.
filter zone zone-name egress	Data is filtered by egress security zone.
filter interface	Data is filtered by interface.
filter interface if-name ingress	Data is filtered by ingress interface.
filter interface if-name egress	Data is filtered by egress interface.
filter application	Data is filtered by application.
filter ip	Data is filtered by address entry.
filter ip add-entry source	Data is filtered by source address (address entry).

Type	Description
filter ip add-entry destination	Data is filtered by destination address (address entry).
filter ip A.B.C.D/M	Data is filtered by IP.
filter ip A.B.C.D/M source	Data is filtered by source IP.
filter ip A.B.C.D/M destination	Data is filtered by destination IP.
filter user	Data is filtered by user.
filter user-group	Data is filtered by user group.
filter severity	Data is filtered by signature severity.

Click **Monitor>User-defined Monitor**.



□	Name	Status	Data type	Group by
□	hj	Enable	Bandwidth	Zone
□	abc	Enable	Bandwidth	Interface
□	ip	Enable	Session	IP
□	ad	Enable	AD attack count	Attack type
□	session	Enable	Create session	IP
□	安全域	Enable	Session	Zone
□	hj1	Enable	Bandwidth	
□	hj111111	Enable	Bandwidth	Zone
□	hjvsyss	Enable	Bandwidth	Zone
□	app	Enable	Bandwidth	Application
□	mgt	Enable	Bandwidth	Zone

- Click **New**. For more information, see Creating_a_User-defined_Stat-set

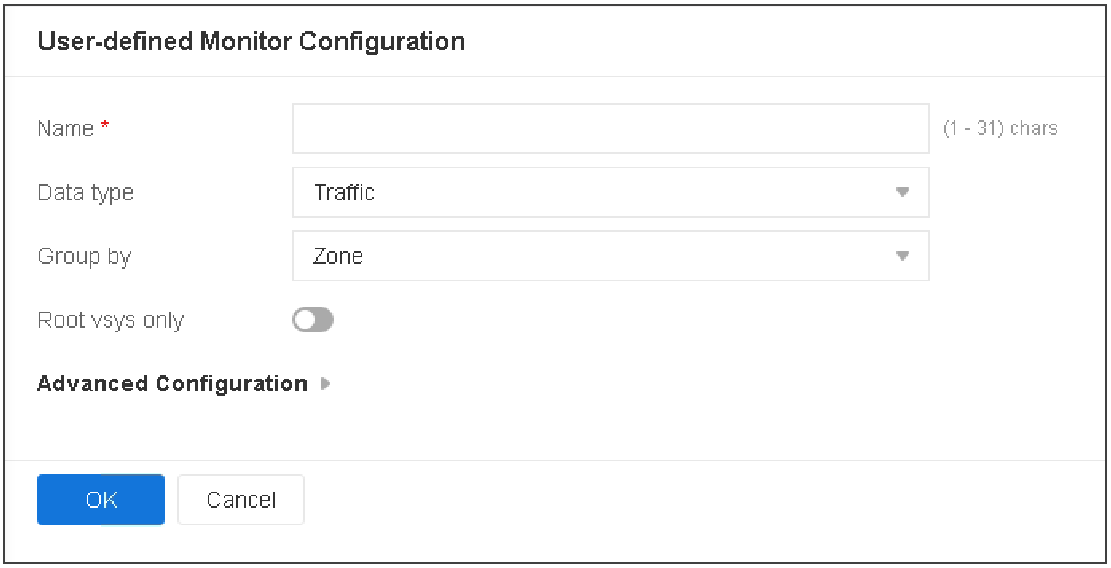
- Click the user-defined stat-set name link. For more information, see Viewing_User-defined_Stat-set_Statistics.

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**.



User-defined Monitor Configuration

Name * (1 - 31) chars

Data type: Traffic

Group by: Zone

Root vsys only

In the User-defined Monitor Configuration page, modify according to your needs.

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.
Root vsys only	If you only want to perform the data statistics for the root VSYS, click the **Enable** button. This button 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 button will be unavailable.
Advanced Configuration	To configure a filtering condition, expand Advanced Configuration. In the Advanced Configuration page, select a

Option	Description
	filter condition from the Type drop-down list. For more details about this option, see The_filtering_conditions_supported_table.

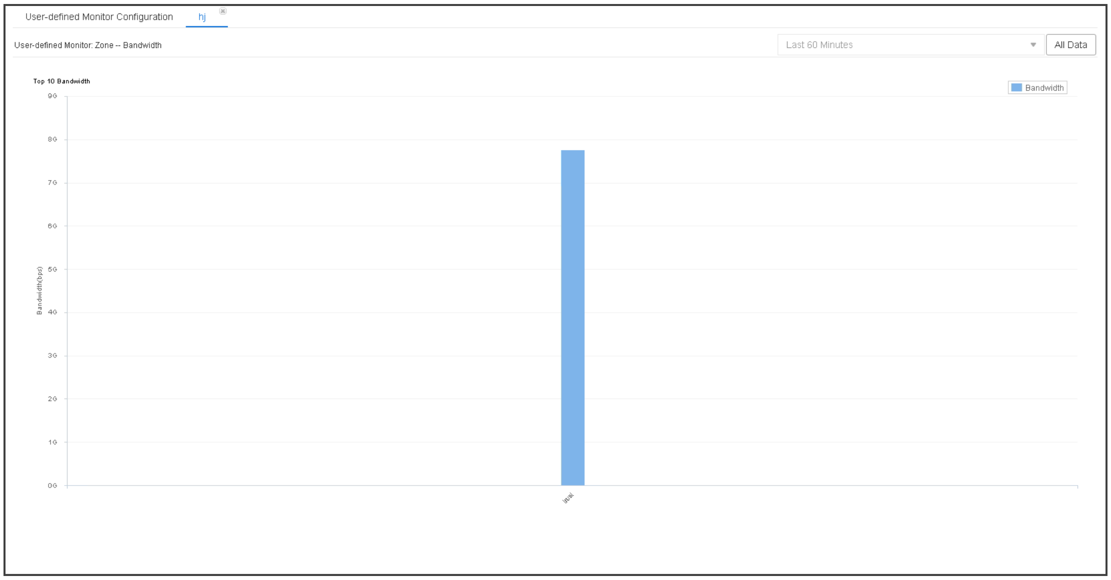
3. Click **OK** to save your settings . The configured stat-set will be displayed .

Notes: You need to pay attention to the following when configure a stat-set.

- The URL hit statistics are only available to users who have a URL license.
- 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

Click the user-defined stat-set name link, and then select the stat-set you want to view.



- Displays the top 10 statistical result from multiple aspects in forms of bar chart.
- 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.

Reporting

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

System provides rich and vivid reports that allow you to analyze network risk, network access and device status comprehensively by all-around and multi-dimensional statistics and charts.

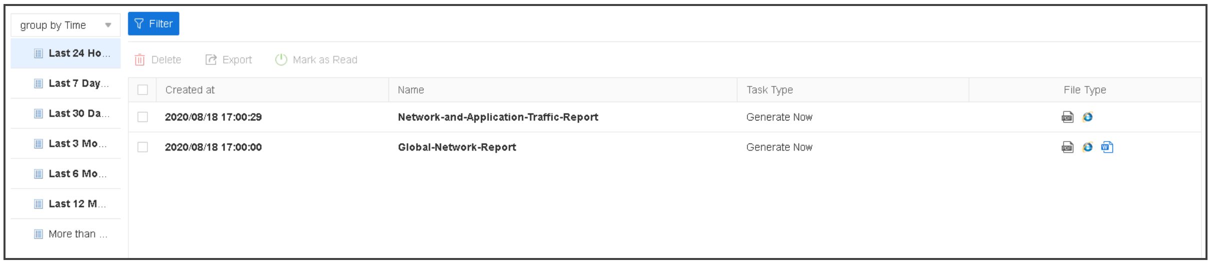
You can configure report task in "Report Template" on Page 1087 and "Report Task" on Page 1093, and view generated report files in "Report File" on Page 1085.

Related Topics:

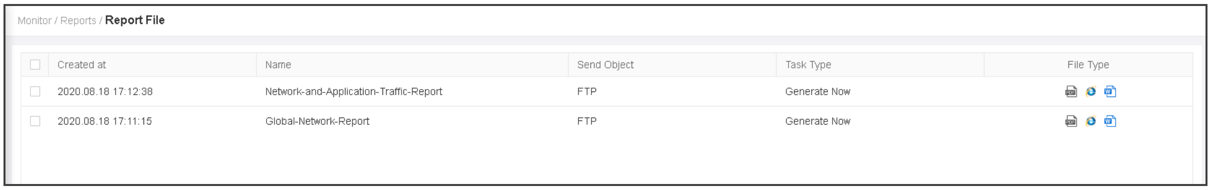
- "Report File" on Page 1085
- "Report Template" on Page 1087
- "Report Task" on Page 1093

Report File

Go to **Monitor > Reports > Report File** and the report file page shows all of the generated report files. The report file pages may vary slightly on different platforms, which are shown below.



□	Created at	Name	Task Type	File Type
□	**2020/08/18 17:00:29**	**Network-and-Application-Traffic-Report**	Generate Now	PDF 🌐
□	**2020/08/18 17:00:00**	**Global-Network-Report**	Generate Now	PDF 🌐 W


Monitor / Reports / **Report File**

□	Created at	Name	Send Object	Task Type	File Type
□	2020.08.18 17:12:38	Network-and-Application-Traffic-Report	FTP	Generate Now	PDF 🌐 W
□	2020.08.18 17:11:15	Global-Network-Report	FTP	Generate Now	PDF 🌐 W

- Sort report files by different conditions: Select **Group by Time**, **Group by Task** or **Group by Status** from the drop-down list, and then select a time, task or status from the selective table, and the related report files will be shown in the report file table.
- The bold black entry indicates that the report file status is "unread".
- Click **Delete** to delete the selected report files.
- Click **Export** , the browser launches the default download tool, and downloads the selected report file.
- Click **Mark as Read** to modify the status of the selected report files.
- Click Filter to select the condition in the drop-down list. Search for specific report files based on filter condition.

- In the File Type column, click the icon of the report file to preview the report file. Not all platforms support this function. The content of the security report varies slightly on different platforms.
- Hover your mouse over the Send Object column, and the system will prompt the Email addresses or FTP information about sending.The content of the security report varies slightly on different platforms.

Notes: If your browser has enabled "Blocking pop-up windows", you will not see the generated file. Make sure to set your browser "Always allow pop-up windows", or you can go to your blocked window history to find the report file.

Report Template

Report templates, define all the contents in the report files. To generate the report file, you need to configure the report template first.

Report templates are classified as predefined and user-defined templates, providing a variety of pre-categorized report items.

- Predefined Template: Predefined templates are built in system. By default, different report items have been selected for each predefined template category. The predefined template cannot be edited or deleted. The predefined template categories are as follows:

Category	Description
Global Network and Risk Assessment Report	Statistics of the global network and risk status, covering the overview, network and application traffic, network threats and host details.
Network and Application Traffic Report	Statistics of the current network situation, covering the network traffic, application traffic and URL hits.
Network Threat Report	Statistics of the threats in the current network, covering the threat trend, external attackers and threat categories.

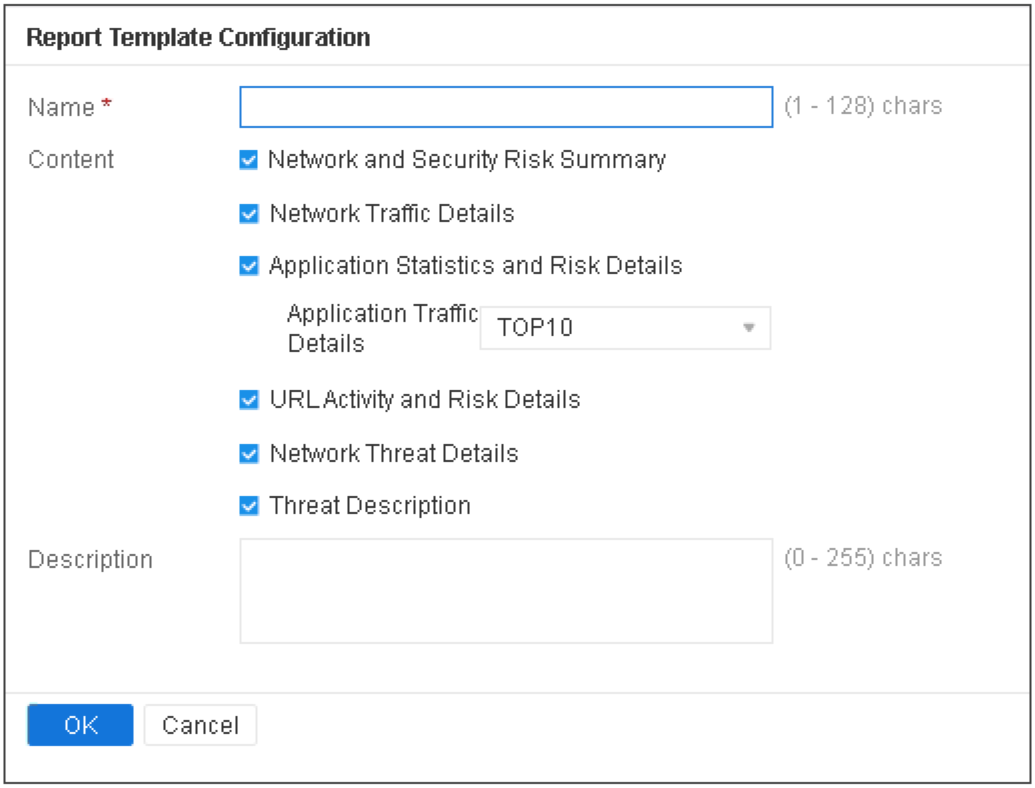
- User-defined Template: The report template created as needed. You can select the report items. Up to 32 user-defined templates can be created.

Creating a User-defined Template

To create a user-defined template, take the following steps:

1. Click **Monitor** > **Reports** > **Template**.

2. Click **New**.



Report Template Configuration

Name * (1 - 128) chars

Content

☑ Network and Security Risk Summary

☑ Network Traffic Details

☑ Application Statistics and Risk Details

Application Traffic Details: TOP10

☑ URL Activity and Risk Details

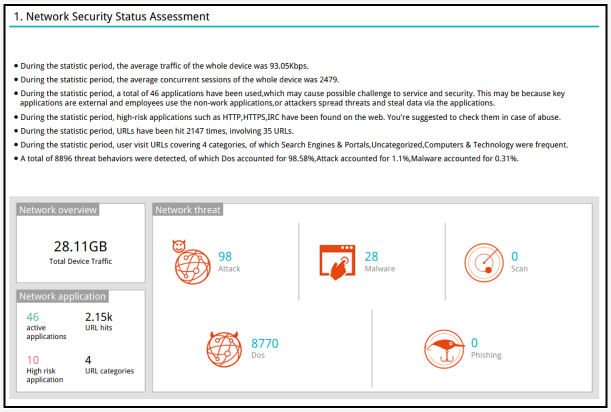
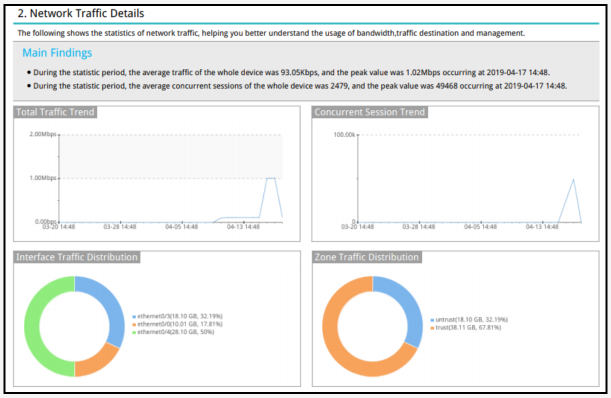
☑ Network Threat Details

☑ Threat Description

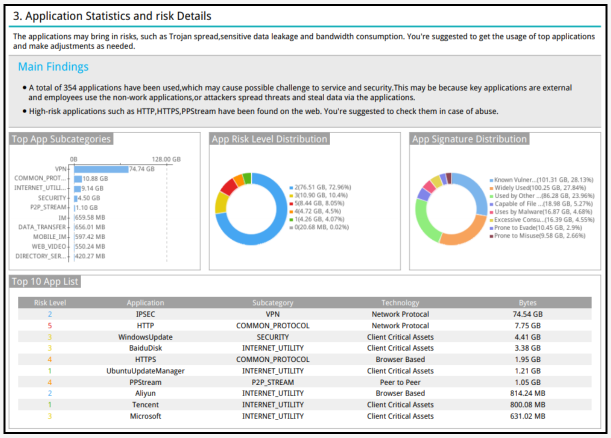
Description (0 - 255) chars

In the Report Template Configuration page, configure the following values.

Option	Description
Name	Specifies the name of the report template.
Content	Select the check box of the report item as needed. By default, all report items are selected. The report items are described as follows: • Network and Security Risk Summary: Statistics of the comprehensive and overall assessment for the health status and security risks of the entire net-

Option	Description
	work.  1. Network Security Status Assessment • During the statistic period, the average traffic of the whole device was 93.05Kbps. • During the statistic period, the average concurrent sessions of the whole device was 2479. • During the statistic period, a total of 46 applications have been used,which may cause possible challenge to service and security. This may be because key applications are external and employees use the non-work applications,or attackers spread threats and steal data via the applications. • During the statistic period, high-risk applications such as HTTP,HTTPS,IRC have been found on the web. You're suggested to check them in case of abuse. • During the statistic period, URLs have been hit 2147 times, involving 35 URLs. • During the statistic period, user visit URLs covering 4 categories, of which Search Engines & Portals,Uncategorized,Computers & Technology were frequent. • A total of 8896 threat behaviors were detected, of which Dos accounted for 98.58%,Attack accounted for 1.1%,Malware accounted for 0.31%. Network overview 28.11GB Total Device Traffic Network application 46 active applications 2.15k URL hits 10 High risk application 4 URL categories Network threat 98 Attack 28 Malware 0 Scan 8770 Dos 0 Phishing • Network Traffic Details: Statistics of network traffic, helping you better understand the usage of bandwidth, traffic destination and management.  2. Network Traffic Details The following shows the statistics of network traffic, helping you better understand the usage of bandwidth,traffic destination and management. Main Findings • During the statistic period, the average traffic of the whole device was 93.05Kbps, and the peak value was 1.02Mbps occurring at 2019-04-17 14:48. • During the statistic period, the average concurrent sessions of the whole device was 2479, and the peak value was 49468 occurring at 2019-04-17 14:48. Total Traffic Trend 2.00Mbps 1.00Mbps 0.00bps 03-20 14:48 03-28 14:48 04-05 14:48 04-13 14:48 Concurrent Session Trend 100.00k 0 03-20 14:48 03-28 14:48 04-05 14:48 04-13 14:48 Interface Traffic Distribution ethernet0/3(18.10 GB, 32.19%) ethernet0/0(10.01 GB, 17.81%) ethernet0/4(28.10 GB, 50%) Zone Traffic Distribution untrust(18.10 GB, 32.19%) trust(38.11 GB, 67.81%) • Application Statistics and Risk Details: Statistics of the traffic of all applications on the device and obtains the usage of the main service applications

Option	Description
	in the intranet. Click the **TOP** drop-down list to specify the number of applications that need to count the traffic for ranking, including TOP5, TOP10, TOP20 and TOP50.



3. Application Statistics and risk Details

The applications may bring in risks, such as Trojan spread,sensitive data leakage and bandwidth consumption. You're suggested to get the usage of top applications and make adjustments as needed.

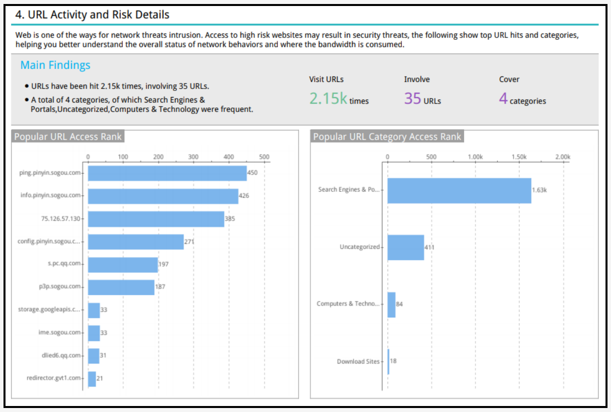
Main Findings

- A total of 354 applications have been used,which may cause possible challenge to service and security.This may be because key applications are external and employees use the non-work applications,or attackers spread threats and steal data via the applications.
- High-risk applications such as HTTP,HTTPS,PPStream have been found on the web. You're suggested to check them in case of abuse.

Top 10 App List

Risk Level	Application	Subcategory	Technology	Bytes
2	IPSEC	VPN	Network Protocal	74.54 GB
5	HTTP	COMMON_PROTOCOL	Network Protocal	7.75 GB
3	WindowsUpdate	SECURITY	Client Critical Assets	4.41 GB
3	BaiduDisk	INTERNET_UTILITY	Client Critical Assets	3.38 GB
4	HTTPS	COMMON_PROTOCOL	Browser Based	1.95 GB
1	UbuntuUpdateManager	INTERNET_UTILITY	Client Critical Assets	1.21 GB
4	PPStream	P2P_STREAM	Peer to Peer	1.05 GB
2	Aliyun	INTERNET_UTILITY	Browser Based	814.24 MB
1	Tencent	INTERNET_UTILITY	Client Critical Assets	800.08 MB
3	Microsoft	INTERNET_UTILITY	Client Critical Assets	631.02 MB

- URL Activity and Risk Details: Statistics of device URL access trends and rankings.



4. URL Activity and Risk Details

Web is one of the ways for network threats intrusion. Access to high risk websites may result in security threats, the following show top URL hits and categories, helping you better understand the overall status of network behaviors and where the bandwidth is consumed.

Main Findings

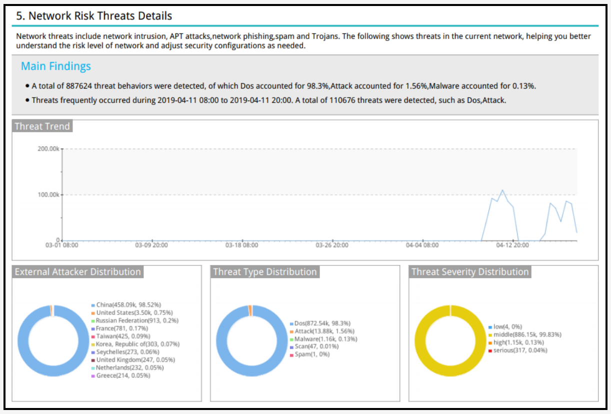
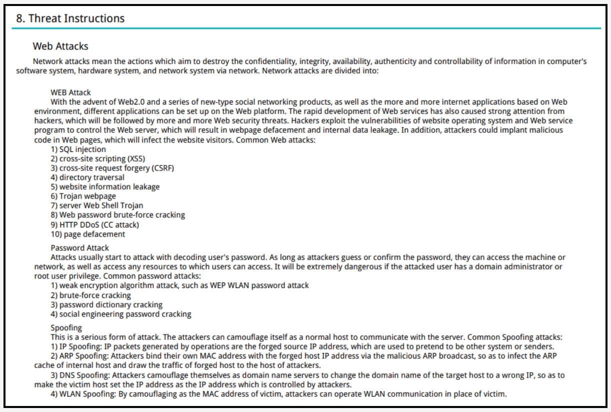
- URLs have been hit 2.15k times, involving 35 URLs.
- A total of 4 categories, of which Search Engines & Portals,Uncategorized,Computers & Technology were frequent.

Visit URLs 2.15k times

Involve 35 URLs

Cover 4 categories

- Network Threat Details: Statistics of the threat events detected by the device, the distribution of

Option	Description
	external attacks, etc., in order to know the network threats and risks existing in the current network.  5. Network Risk Threats Details Network threats include network intrusion, APT attacks,network phishing,spam and Trojans. The following shows threats in the current network, helping you better understand the risk level of network and adjust security configurations as needed. Main Findings • A total of 887624 threat behaviors were detected, of which Dos accounted for 98.3%,Attack accounted for 1.56%,Malware accounted for 0.13%. • Threats frequently occurred during 2019-04-11 08:00 to 2019-04-11 20:00. A total of 110676 threats were detected, such as Dos,Attack. Threat Trend External Attacker Distribution Threat Type Distribution Threat Severity Distribution 200.00k 100.00k 0 03-01 08:00 03-09 20:00 03-18 08:00 03-26 20:00 04-04 08:00 04-12 20:00 China(458.09k, 98.52%) United States(3.50k, 0.75%) Russian Federation(913, 0.2%) France(781, 0.17%) Taiwan(425, 0.09%) Korea, Republic of(303, 0.07%) Seychelles(273, 0.06%) United Kingdom(247, 0.05%) Netherlands(232, 0.05%) Greece(214, 0.05%) Dos(872.54k, 98.3%) Attack(13.88k, 1.56%) Malware(1.16k, 0.13%) Scan(47, 0.01%) Spam(1, 0%) low(4, 0%) middle(886.15k, 99.83%) high(1.15k, 0.13%) serious(317, 0.04%) • Threat Description: Display the detailed description of the threat, helping understand the threat information.  8. Threat Instructions Web Attacks Network attacks mean the actions which aim to destroy the confidentiality, integrity, availability, authenticity and controllability of information in computer's software system, hardware system, and network system via network. Network attacks are divided into: WEB Attack With the advent of Web2.0 and a series of new-type social networking products, as well as the more and more internet applications based on Web environment, different applications can be set up on the Web platform. The rapid development of Web services has also caused strong attention from hackers, which will be followed by more and more Web security threats. Hackers exploit the vulnerabilities of website operating system and Web service program to control the Web server, which will result in webpage defacement and internal data leakage. In addition, attackers could implant malicious code in Web pages, which will infect the website visitors. Common Web attacks: 1) SQL injection 2) cross-site scripting (XSS) 3) cross-site request forgery (CSRF) 4) directory traversal 5) website information leakage 6) Trojan webpage 7) server Web Shell Trojan 8) Web password brute-force cracking 9) HTTP DDoS (CC attack) 10) page defacement Password Attack Attacks usually start to attack with decoding user's password. As long as attackers guess or confirm the password, they can access the machine or network, as well as access any resources to which users can access. It will be extremely dangerous if the attacked user has a domain administrator or root user privilege. Common password attacks: 1) weak encryption algorithm attack, such as WEP WLAN password attack 2) brute-force cracking 3) password dictionary cracking 4) social engineering password cracking Spoofing This is a serious form of attack. The attackers can camouflage itself as a normal host to communicate with the server. Common Spoofing attacks: 1) IP Spoofing: IP packets generated by operations are the forged source IP address, which are used to pretend to be other system or senders. 2) ARP Spoofing: Attackers bind their own MAC address with the forged host IP address via the malicious ARP broadcast, so as to infect the ARP cache of internal host and draw the traffic of forged host to the host of attackers. 3) DNS Spoofing: Attackers camouflage themselves as domain name servers to change the domain name of the target host to a wrong IP, so as to make the victim host set the IP address as the IP address which is controlled by attackers. 4) WLAN Spoofing: By camouflaging as the MAC address of victim, attackers can operate WLAN communication in place of victim.
Description	Specifies the description of the report template.

3. Click **OK** to complete user-defined template configurations.

Editing a User-defined Template

To edit a user-defined report template, take the following steps:

1. Click **Monitor** > **Reports** > **Template**.

2. In the templates list, select the user-defined report template entry that needs to be edited.

3. Click **Edit**.

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

Deleting a User-defined Template

To delete a user-defined report template, take the following steps:

1. Click **Monitor** > **Reports** > **Template**.

2. In the templates list, select the user-defined report template entry that needs to be deleted.

3. Click **Delete**.

Cloning a Report Template

System supports the rapid clone of a report template. You can clone and generate a new report template by modifying some parameters of one current report template.

To clone a report template, take the following steps:

1. Click **Monitor** > **Reports** > **Template**.

2. In the templates list, select a report template that needs to be cloned.

3. Click the **Clone** button above the list, and in the **Report Template Configuration** page, enter the newly cloned report template name into the "Name" .

4. The cloned report template will be generated in the list.

Report Task

The report task is the schedule related to report file. It defines the report template, generation period, generation time, and the output method of report files.

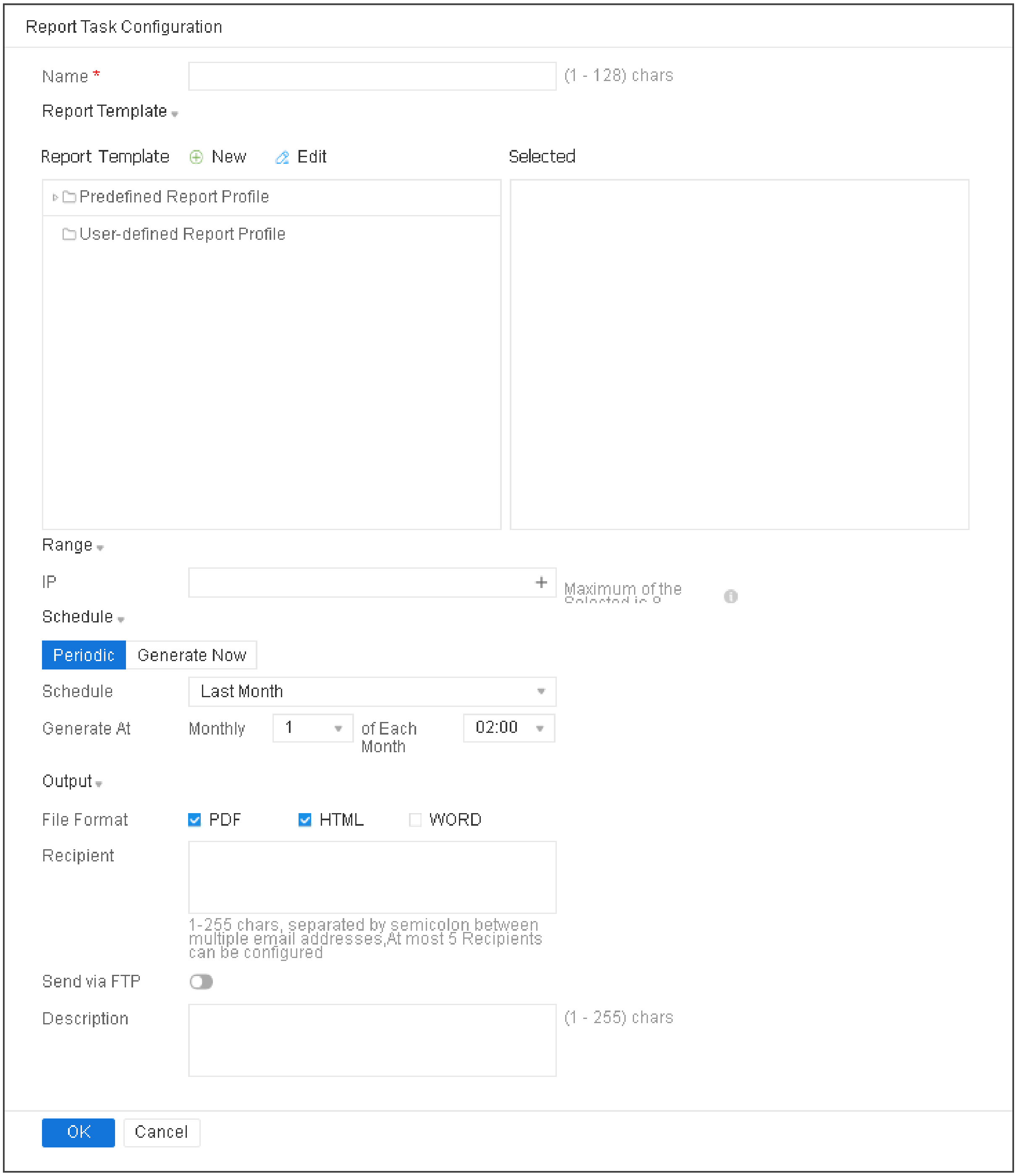
You can configure report tasks and generate report files on the device according to your needs.

Creating a Report Task

To create a report task, take the following steps:

1. Select **Monitor> Reports> Report Task**.

2. Click **New**.



Report Task Configuration

Name * (1 - 128) chars

Report Template

Report Template ⊕ New Edit

Selected

Predefined Report Profile

User-defined Report Profile

Range

IP + Maximum of the Selected is 8

Schedule

Periodic | Generate Now

Schedule: Last Month

Generate At: Monthly 1 of Each Month 02:00

Output

File Format: ☑ PDF ☑ HTML □ WORD

Recipient

1-255 chars, separated by semicolon between multiple email addresses,At most 5 Recipients can be configured

Send via FTP

Description (1 - 255) chars

OK Cancel

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 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 Schedule, configure the running time of the report task.

Option	Description
Schedule	The schedule specifies the running time of the report

Option	Description
	task. The report task can be run periodically or run immediately. Periodic: Generates report files as planned. • Schedule: Specifies the statistical period. • Generate At: Specifies the generation time. Generate Now: Generates report files immediately. • Type: Generates report file based on the data in the specified statistical period.

Expand Output, configure the output mode information of the report.

Option	Description
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.

Option	Description
	• Username: Specifies the username used to log on to the FTP server. • Password: Enter the password of the FTP username. • 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** to complete report task configuration.

Editing the Report Task

To edit the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.
2. In the report task list, select the report task entry that needs to be edited.
3. Click the **Edit** button on the top to open the **Report Task Configuration** page to edit the selected report task.
4. Click **OK** to save the settings.

Deleting the Report Task

To delete the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.

2. In the report task list, select the report task entry that needs to be deleted.

3. Click the **Delete** button on the top to delete the selected report task.

Enabling/Disabling the Report Task

To enable or disable the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.

2. Select the task, and click the **Enable** or **Disable** button on the top.

   By default, the user-defined task is enabled.

Logging

Logging is a feature that records various kinds of system logs, including device log, threat log, session log, NAT log, Content filter log,File filter log, Network Behavior Record logshare access logs, and URL logs.

- Device log
  - Event - includes 8 severity levels: debugging, information, notification, warning, error, critical, alert, emergency.
  - Network - logs about network services, like PPPoE and DDNS.
  - Configuration - logs about configuration on command line interface, e.g. interface IP address setting.
- Share Access Logs - logs about share access rule.
- Threat - logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- Session - Session logs, e.g. session protocols, source and destination IP addresses and ports.
- NAT - NAT logs, including NAT type, source and destination IP addresses and ports.
- EPP - logs related with end point protection function.
- File Filter - logs related with file filter function.
- Content filter logs － logs related with content filter function, e.g. Web content filter, Web posting, Email filter and HTTP/FTP control.
- Network behavior record logs － Logs related with network behavior record function, e.g. IM behavior ,etc.

- URL - logs about network surfing, e.g. Internet visiting time, web pages visiting history, an URL filtering logs.
- PBR - logs about policy-based route.
- CloudSandBox - logs about sandbox.

The system logs the running status of the device, thus providing information for analysis and evidence.

Log Severity

Event logs are categorized into eight severity levels.

Severity	Level	Description	Log Definition
Emergencies	0	Identifies illegitimate system events.	LOG_EMERG
Alerts	1	Identifies problems which need immediate attention such as device is being attacked.	LOG_ALERT
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_

Severity	Level	Description	Log Definition
			INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_ DEBUG

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 - Sends logs to UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Local database - Sends logs to the local database of the device.

Log Format

To facilitate the access and analysis of the system logs, StoneOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**.See the example below:

2000-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

Event Log

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

To view event logs, select **Monitor > Log > Event Log**.

In this page, you can perform the following actions:

- Configure: Click to jump to the configuration page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Modify Log Parameter: Click to modify parameter of specified log, including the description, level of the log, and enabling/disabling the log generation.
- Filter: Click Filter to add conditions to show logs that march your filter.

Network Log

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

To view network logs, select **Monitor > Log > Network Log**.

In this page, you can perform the following actions:

- Configure: Click to jump to the configuration page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT file.
- Modify Log Parameter: Click to modify parameter of specified log, including the description, level of the log, and enabling/disabling the log generation.
- Filter: Click Filter to add conditions to show logs that march your filter.

Configuration Log

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

To view configuration logs, select **Monitor > Log > Configuration Log**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the configuration page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Modify Log Parameter: Click to modify parameter of specified log, including the description, level of the log, and enabling/disabling the log generation.
- Filter: Click Filter to add conditions to show logs that march your filter.

Share Access Logs

To view share access logs, select **Monitor > Log > Share Access Log**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the Log Management page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT file.
- Add to My Log: Click to add the current filtered results to MyLog list.
- Filter: Click Filter to add conditions to show logs that march your filter.

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 "Log Configuration" on Page 1115.
- You have enabled one or more of the following features: "Anti-Virus" on Page 915, " Intrusion Prevention System" on Page 927, "Attack-Defense" on Page 981 or "Perimeter Traffic Filtering" on Page 1001 .

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

In this page, you can perform the following actions:

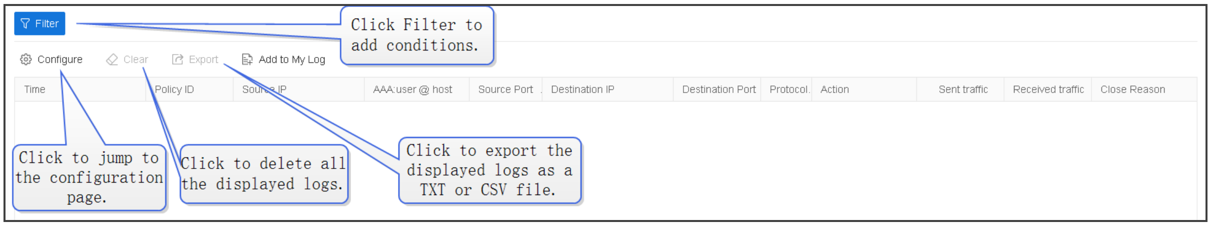
- Configure: Click to jump to the configuration page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click Filter to add conditions to show logs that march your filter.You can enter the IPv4 or IPv6 address if the filter condition is selected as source or destination IP.
- View the details of selected log in the Log Details tab. In the Log Details tab, you can click "View Pcap" "Download" "Add Whitelist" "Disable Signatures" to quickly link to the relevant page.

Session Log

Session logs can be generated under the conditions that:

- Session logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- The logging function has been enabled for policy rules. Refer to "Security Policy" on Page 768.

To view session logs, select **Monitor > Log > Session log**.



Click Filter to add conditions.

Click to jump to the configuration page.

Click to delete all the displayed logs.

Click to export the displayed logs as a TXT or CSV 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.

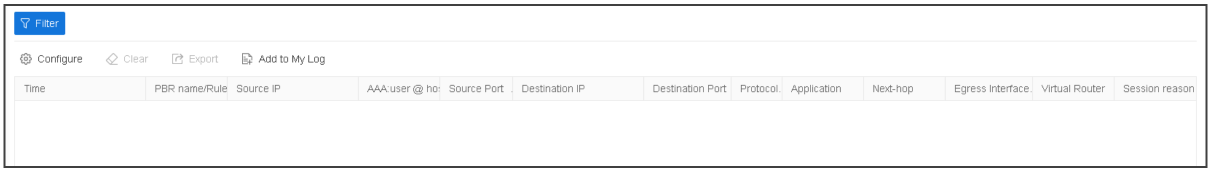
PBR Log

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

PBR logs can be generated under the conditions that:

- PBR logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- You have enabled logging function in PBR rules. Refer to "Creating a Policy-based Route Rule" on Page 264 .

To view PBR logs, select **Monitor > Log > PBR Log**.



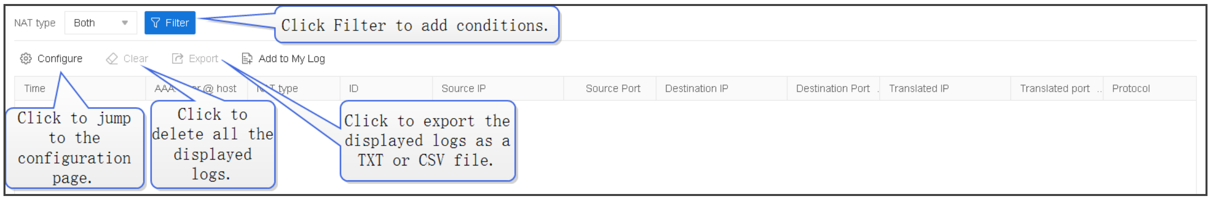
Time	PBR name/Rule	Source IP	AAA:user @ ho:	Source Port	Destination IP	Destination Port	Protocol.	Application	Next-hop	Egress Interface.	Virtual Router	Session reason

NAT Log

NAT logs are generated under the conditions that:

- NAT logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- NAT logging of the NAT rule configuration is enabled. Refer to"Configuring SNAT" on Page 852 and"Configuring DNAT" on Page 864.

To view NAT logs, select **Monitor > Log > NAT Log**.



Click Filter to add conditions.

Click to jump to the configuration page.

Click to delete all the displayed logs.

Click to export the displayed logs as a TXT or CSV file.

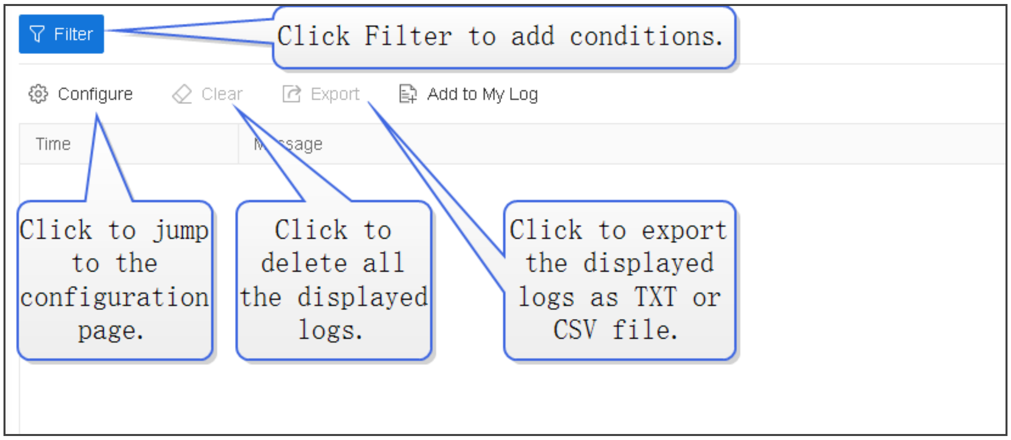
URL Log

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 "Log Configuration" on Page 1115.
- You have enabled logging function in URL rules. Refer to " URL Filtering" on Page 659

To view URL logs, select **Monitor > Log > URL Log**.



Click Filter to add conditions.

Click to jump to the configuration page.

Click to delete all the displayed logs.

Click to export the displayed logs as TXT or CSV file.

EPP Log

To view EPP logs, select **Monitor > Log > EPP**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the EPP page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click Filter to add conditions to show logs that march your filter.

IoT Log

You can view, configure, clear or export IoT logs.

The following condition should be met before log's generation:

- The IoT logging function has been enabled on the device. For the detailed configurations, refer to Log Management.

Click **Monitor** > **Log** > **IoT Log** to enter the <IoT Log> page.

- Click the Filter button to add filter conditions and the required information will be filtered out in the following list.
- Configure: Click the **Configure** button and enter the **Log Management** page.
- Clear: Click the **Clear** button to delete all the filtered IoT logs in system.
- Export: Click the **Export** button to export part or all logs in the format of TXT or CSV.

File Filter 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.

File Filter logs can be generated under the conditions that:

- File Filter logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- You have enabled the function of "File Filter" on Page 705.

To view File Filter logs, select **Monitor > Log > File Filter**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file.

Content Filter 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.

Content Filter logs can be generated under the conditions that:

- Content Filter logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- You have enabled one or more of the following features: "Web Content" on Page 712, "Web Posting" on Page 718, "Email Filter" on Page 724 and"APP Behavior Control" on Page 730 function.

To view Content Filter logs, select **Monitor > Log > Content Filter**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file.

Network Behavior Record 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.

Network Behavior Record logs can be generated under the conditions that:

- Network Behavior Record logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 1115.
- You have enabled the function of"Network Behavior Record" on Page 737.

To view Network Behavior Record logs, select **Monitor > Log > Network Behavior Record**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file.

CloudSandBox Log

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

To view sandbox logs, select **Monitor > Log > Cloud SandBox Log**.

In this page, you can perform the following actions:

- Configure: Click to jump to the CloudSandBox page.
- Clear: Click to clear the selected logs.
- Export: Click to export the displayed logs as a TXT or CSV file.
- Filter: Click Filter to add conditions to show logs that march your filter.You can enter the IPv4 or IPv6 address if the filter condition is selected as source or destination IP.

Log Configuration

You can create log server, set up log email address, and add UNIX servers.

Creating a Log Server

To create a log server, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **Log Server Configuration** tab.
3. Click **New**.

In the Log Server Configuration page, configure these values.

Option	Description
Hostname	Enter the name or IP of the log server.
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. 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.
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 log servers.

Configuring Log Encoding

The default encoding format for the log information that is output to the log 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 log server will be GBK encoding. To enable the GBK encoding :

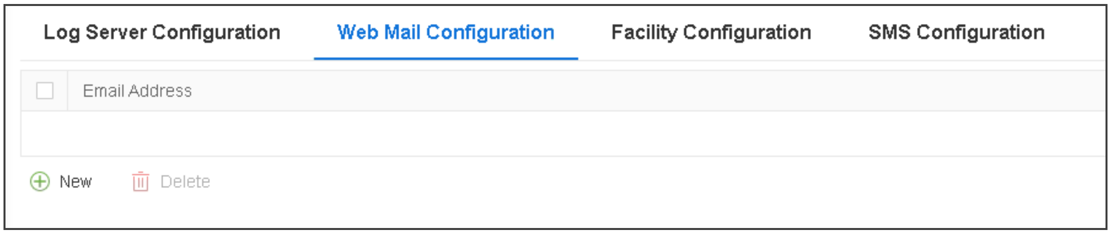
1. Select **Monitor > Log > Log Configuration**.
2. Click **Log Server Configuration** tab.
3. Click the **Log Encoding Configuration** button in the upper right corner to open the Log Encoding Configuration page.
4. Click the button to enable the GBK Encoding.
5. .Click **OK** to save the settings.

Adding Email Address to Receive Logs

An email in the log management setting is an email address for receiving log messages.

To add an email address, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **Web Mail Configuration** tab.



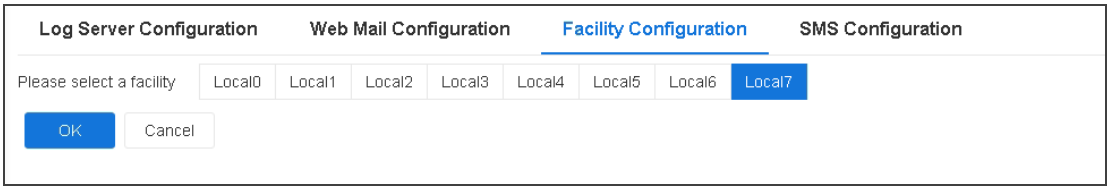
3. Enter an email address and click **New**.
4. If you want to delete an existing email, click **Delete**.

Notes: You can add at most 3 email addresses.

Specifying a Unix Server

To specify a Unix server to receive logs, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click the **Facility Configuration** tab.



3. Select the device you want and the logs will be exported to that Unix server.
4. Click **OK**.

Specifying a Mobile Phone

To specify a mobile phone to receive logs, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **SMS Configuration** tab.
3. Enter a mobile phone number and click **New**.
4. If you want to delete an existing mobile phone number, click **Delete**.

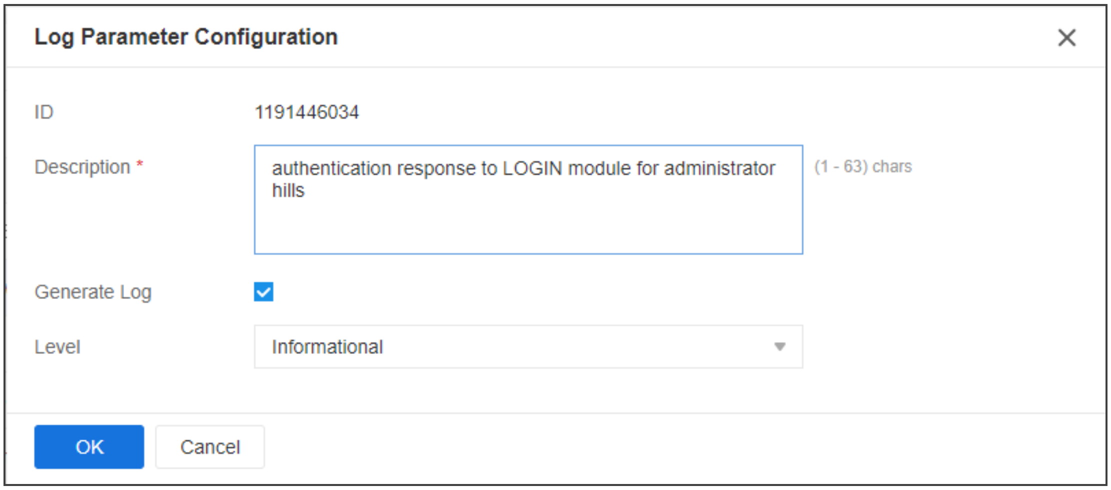
Notes: You can add at most 3 mobile phone numbers.

Log Parameter Configuration

The system supports to modify parameter of the event log, network log, and configuration log, including the description, level of the log, and enabling/disabling the log generation. You can modify the parameters of the specified log through the corresponding log page, and view it through the log parameter configuration page, edit or delete log entries on the log parameter configuration page.

To edit the log parameter, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration** > **Log Parameter Configuration**.
2. Select the log entry that needed to be edited, click **Edit**, modify the description, level in the Log Parameter Configuration page.



Log Parameter Configuration

ID 1191446034

Description * authentication response to LOGIN module for administrator hills (1 - 63) chars

Generate Log ☑

Level Informational

3. Click **OK**.

Managing Logs

You can configure system to enable the logging function, including enabling various logs.

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.
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.

Option	Description
	- 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.
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.
Log Server	Select the check box to export event logs to the syslog server. - View Log 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

Option	Description
	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. - 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.
Log Server	Select the check box to export network logs to the syslog

Option	Description
	server. - View Log Server - Click to see all existing syslog servers or to add a new server.

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.
Log 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).

Session Log

Option	Description
Enable	Click the button to enable the session logging function.

Option	Description
	• 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.
Log Server	Select the check box to export session logs to the syslog 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.

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

Option	Description
	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.
Log Server	Select the check box to export PBR logs to the syslog 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 plain 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.

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.

Option	Description
	The default value may vary for different hardware platforms.
Log Server	Select the check box to export NAT logs to log servers. • 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.

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.
Log Server	Select the check box to export IoT logs to log servers. • View Log Server - Click to see all existing 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

Option	Description
	servers, which will relieve the pressure of a single log 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. • 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.

Option	Description
Log Server	Select the check box to export EPP logs to log servers. - View Log Server - Click to see all existing 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 log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.
Email Address	Select the check box to send EPP 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.

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.

Option	Description
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.
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.

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.
Log Server	Select the check box to export File Filter logs to log server. • View Log 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 log servers, which will relieve the pressure of a single log 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.
Log Server	Select the check box to export Content Filter logs to 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.

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.
Log Server	Select the check box to export Network Behavior Record logs to 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.

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

Option	Description
	CloudSandBox logs.
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.
Log Server	Select the check box to export CloudSandBox logs to log server. • View Log 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.
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.
File	Select to export threat logs as a file to USB.

Option	Description
	- 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.
Terminal	Select to send logs to terminals.
Log Server	Select the check box to export threat logs to 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.
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

Option	Description
	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.
Log Server	Select the check box to export Share Access logs to log server. - View Log Server - Click to see all existing syslog servers or to add a new server.

Chapter 13 Diagnostic Tool

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

System supports the following diagnostic methods:

- Test Tools: DNS Query, Ping and Traceroute can be used when troubleshooting the network.

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.

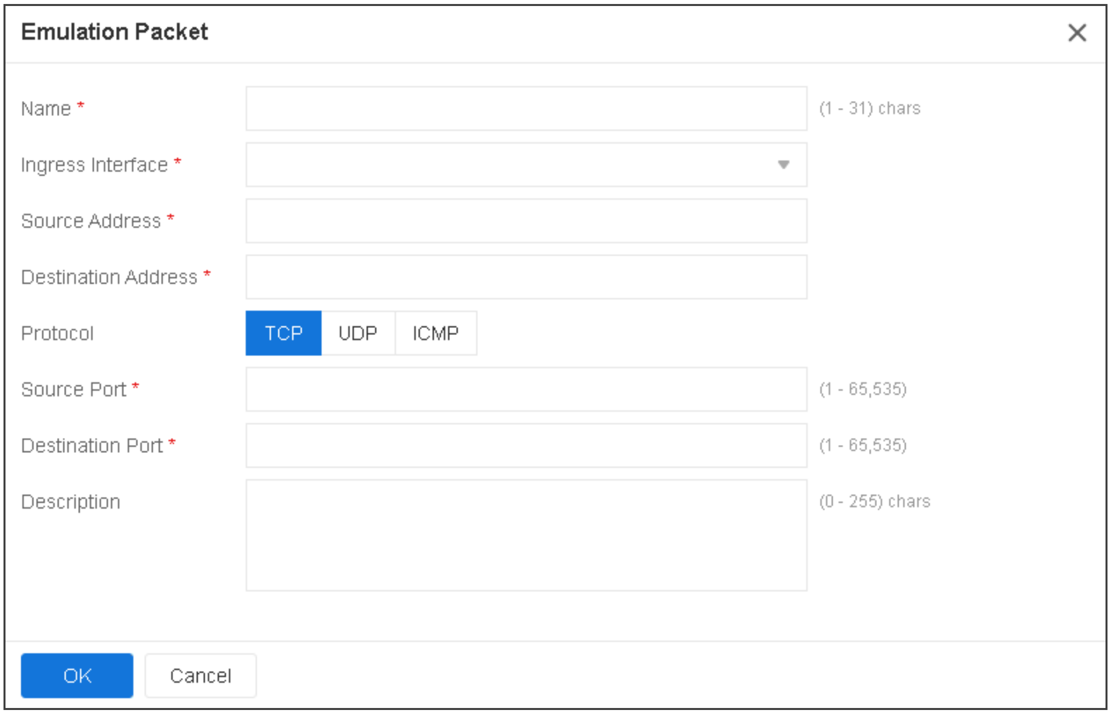
Configuring Packet Path Detection

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 Tool > Packet Path Detection**.
2. Click **Choose Detected Source**.
3. Click **New** , in the drop-down list, select **Emulation Packet** tab.



Emulation Packet

Name *		(1 - 31) chars
Ingress Interface *		
Source Address *		
Destination Address *		
Protocol	TCP UDP ICMP	
Source Port *		(1 - 65,535)
Destination Port *		(1 - 65,535)
Description		(0 - 255) chars

Configure options as follows.

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.
Source Address	Specifies the source IP address of the emulation packet in the text box.
Destination Address	Specifies the destination IP address of the emulation packet in the text box.
Protocol	Select the protocol of the emulation packet from the drop-down list. When selecting TCP or UDP, specify the source and destination ports in the Source Port and

Option	Description
	Destination Port text boxes; when selecting ICMP, enter the ICMP type and code in the Type and Value text boxes.
Description	Specifies the description for this emulation packet.

4. 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.

5. 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

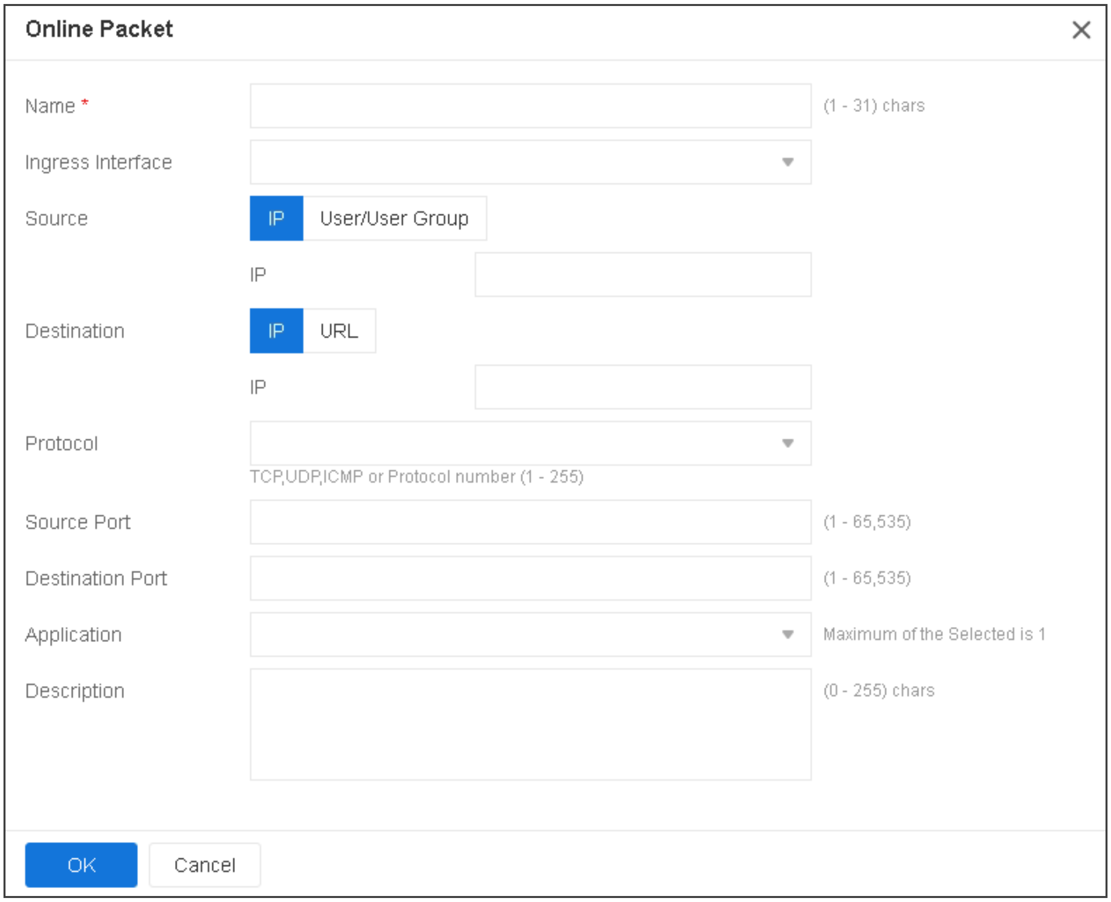
click the **View Details** link to view the detailed detection report. The meanings of status indicators are as follows:

- 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 Tool > Packet Path Detection**.
2. Click **Choose Detected Source**.
3. Click **New** , in the drop-down list, select **Online Packet** tab.



Online Packet

Name *		(1 - 31) chars
Ingress Interface		
Source	IP / User/User Group IP	
Destination	IP / URL IP	
Protocol	TCP,UDP,ICMP or Protocol number (1 - 255)	
Source Port		(1 - 65,535)
Destination Port		(1 - 65,535)
Application		Maximum of the Selected is 1
Description		(0 - 255) chars

Configure options as follows.

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. • Address: Select the Address radio button and enter the IP address in the text box.

Option	Description
	- User/User Group: Select the User/User Group radio button and select the user/user group from the drop-down list.
Destination	Specifies the destination IP address of the online packet. - Address: Select the radio button and enter the IP 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.
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. If needed, specify the detecting duration in the Detecting Duration section. After reaching the specified duration, system will automatically stop the detection. The default value is 30 minutes.

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.

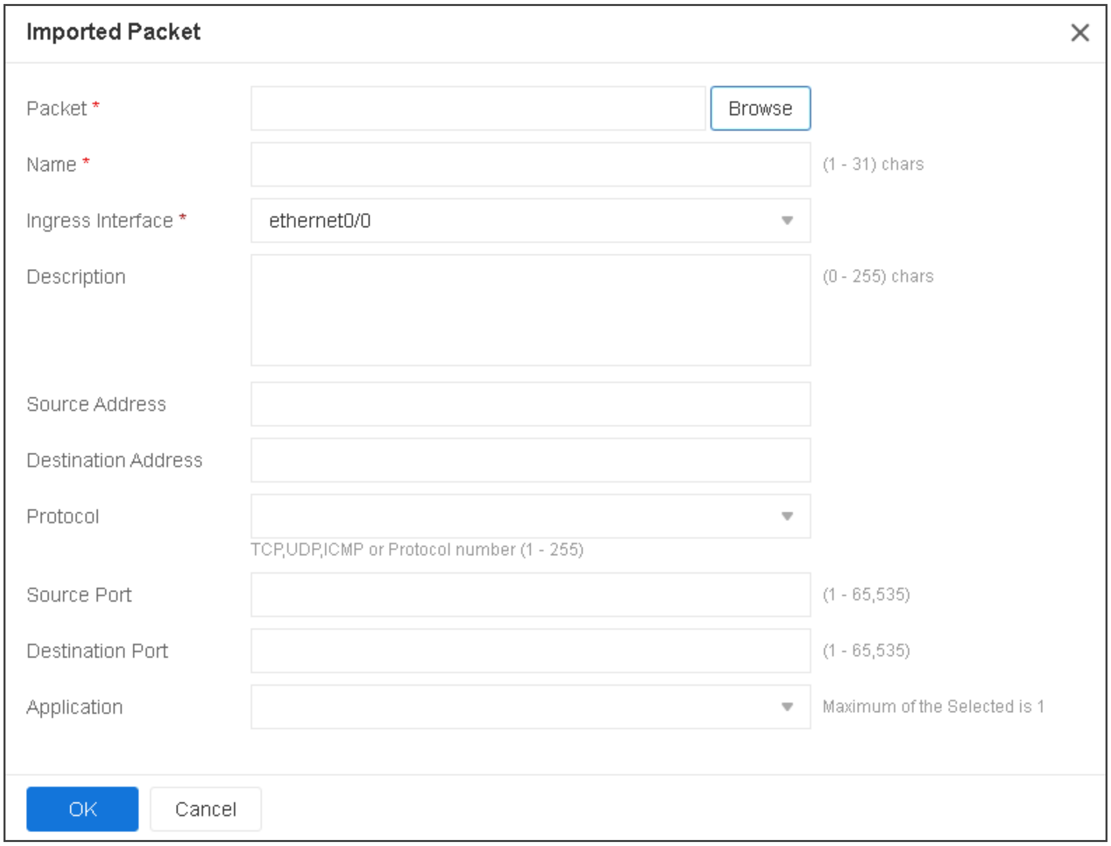
Notes: If one of the following situations happens during the detection, the system will stop the detection.

- 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.

Imported Detection

To perform the imported detection, take the following steps:

1. Select **System > Diagnostic Tool > Packet Path Detection**.
2. Click **Choose Detected Source**.
3. Click **New** , in the drop-down list, select **Imported Packet** tab.



Imported Packet

Packet *

Name * (1 - 31) chars

Ingress Interface * ethernet0/0

Description (0 - 255) chars

Source Address

Destination Address

Protocol

TCP,UDP,ICMP or Protocol number (1 - 255)

Source Port (1 - 65,535)

Destination Port (1 - 65,535)

Application Maximum of the Selected is 1

Configure options as follows.

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.
Name	Specifies the name of the imported packet.
Ingress Interface	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.

Option	Description
Advanced	
Source Address	Specifies the source IP address of the imported packet.
Destination Address	Specifies the destination IP address of the imported packet.
Protocol	Specifies the protocol type or the protocol number of the imported packet.
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. 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

The detected sources dialog box lists all detected sources in the system, including the emulation packet, online packet, and imported packet.

Click **Choose Detected Source**. In the Choose Detected Source dialog box, select the **Detected Sources** tab. You can then perform the following actions:

- Click **Details** in the Result column to view the detection report of the detected source.
- Click **Export** in the Export Packet column to export the detected packet to the desired directory.
- 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.

Packet Capture Tool

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

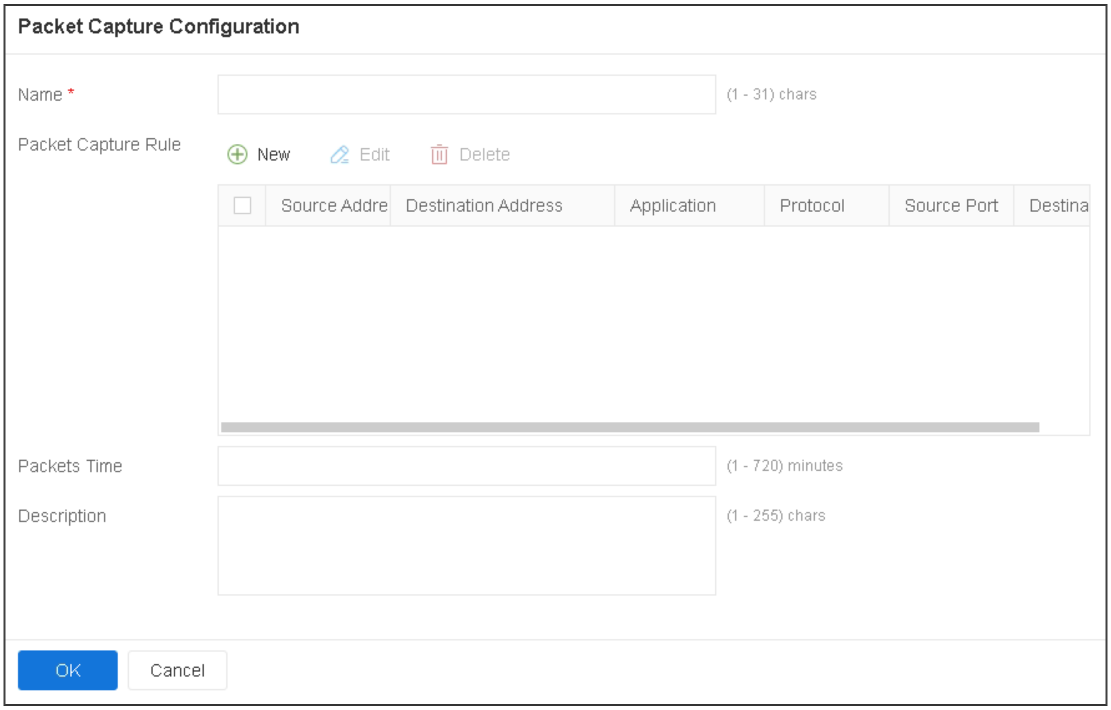
You can capture packets in the system with multiple capture tasks by Packets Capture Tools. With one or more packets capture rules in the task, and system will capture packages with multiple conditions in real time. At the same time, you can view the current captured and lost packages at any time. The captured packages can be downloaded or exported to a local location and then viewed through a third-party packet capture tool.

Configuring Packet Capture Tools

To capture packets, take the following steps:

1. Select **System > Diagnostic Tool > Packet Capture Tool**.

2. Click **New**.



Packet Capture Configuration

Name * (1 - 31) chars

Packet Capture Rule

□	Source Addre	Destination Address	Application	Protocol	Source Port	Destina

Packets Time (1 - 720) minutes

Description (1 - 255) chars

In the Packet Capture Configuration page, configure as follows.

Option	Description
Name	Enter the name of the packets capture entry.
Packet Capture Rule	Click **New**, and configure the packet capture rules in the **Packet Capture Rules** page. For the configuration method, refer to the 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.
Packets Time	Enter the packets time in the text box.
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: The system allows you to create at most 5 packets capture tasks.

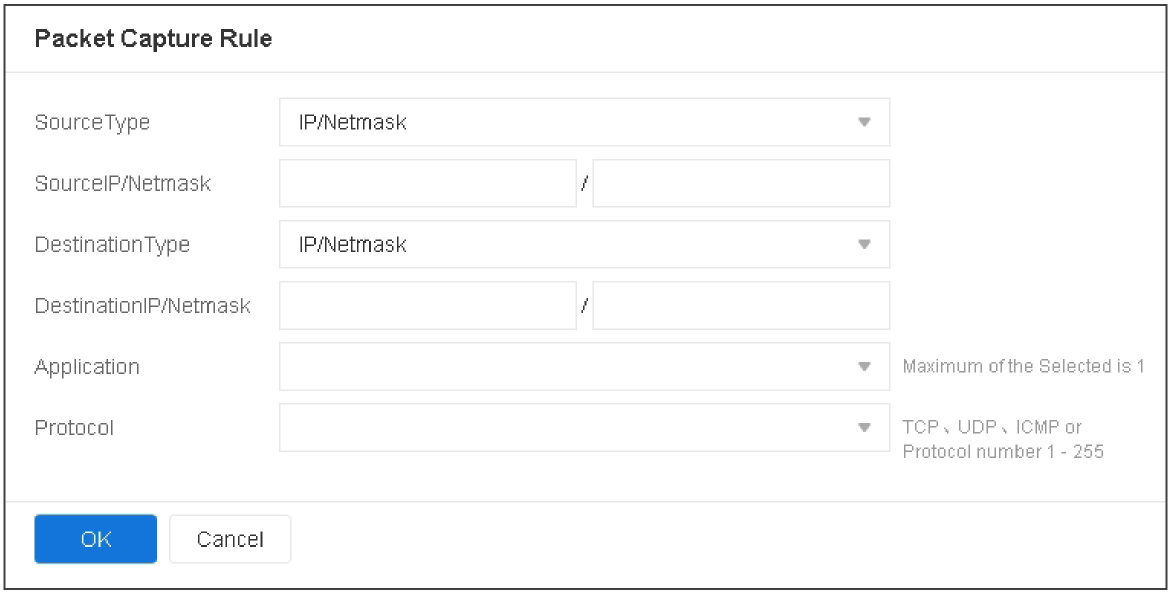
Create a Packet Capture Rule

To create a packet capture rule, take the following steps:

1. Select **System > Diagnostic Tool > Packet Capture Tool**.

2. Click **New**.

3. Click **New** at **Package Capture Rule** to open the **Packet Capture Rule** page.



Packet Capture Rule

SourceType	IP/Netmask	
SourceIP/Netmask	/	
DestinationType	IP/Netmask	
DestinationIP/Netmask	/	
Application		Maximum of the Selected is 1
Protocol		TCP、UDP、ICMP or Protocol number 1 - 255

In the Packet Capture Rule page, configure as follows.

Option	Description
Source Type	Specify the source IP address/range or the user/user group of the packet. • IP/Netmask: Enter the IPv4 address and its mask in the text box.

Option	Description
	- IP Range: Enter the IPv4 range in the text box. - IPv6/Prefix: Enter the IPv6 address and its prefix in the text box. - IPv6 Range: Enter the IPv6 range in the text box. - User/User Group: Select the user/user group from the drop-down list.
Destination Type	Specify the destination IP address/range of the packet. - IP/Netmask: Enter the IPv4 address and its mask in the text box. - IP Range: Enter the IPv6 address and its range in the text box - IPv6/Prefix: Enter the IPv6 address and its prefix in the text box. - IPv6 Range: Enter the IPv6 range in the text box. - URL: Enter the URL in the text box.
Application	Specifies the application type of the packet.
Protocol	Specifies the protocol type or the protocol number of the packet.
Source Port	When the protocol is TCP or UDP, the source port number can be specified. Specifies the source port of the packet.

Option	Description
Destination Port	When the protocol is TCP or UDP, the destination port number can be specified. Specifies the destination port of the packet.

4. Click **OK**.

Notes: A maximum of 8 packet capture rules can be created in the same packet capture task.

Packet Capture Global Configuration

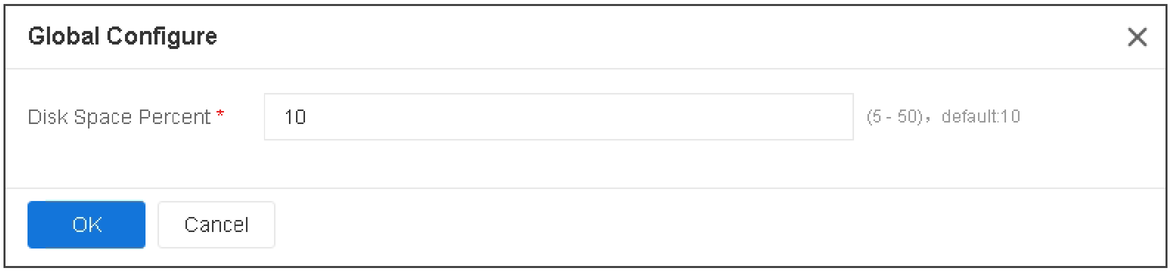
The global configuration items of packet capture vary according to the type of device:

- For devices with hard disks, you can configure the percentage of the packet capture files to the total hard disk size.
- For devices without hard disks, you can configure the packet capture file save percent and the packet capture file save time.

To configure the global configuration, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Packet Capture Tool**.
2. Click the **Global Configuration** button in the upper right corner of the page to open the **Global Configuration** page.

3. The global configuration page of the device with hard disk is as follows:

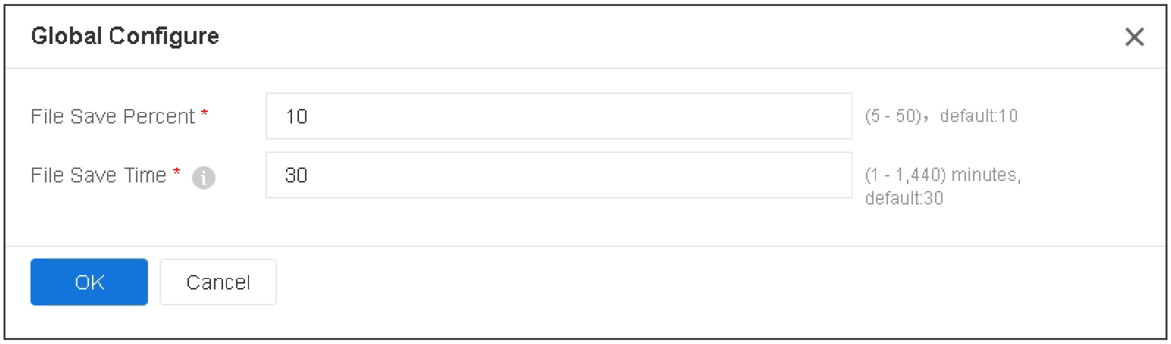


Global Configure

Disk Space Percent * 10 (5 - 50)，default:10

Option	Description
Disk Space Percent	Enter the percentage of the packet capture file to the total hard disk size in the text box. The range is 5%-50%. The default value is 10%.

4. The global configuration page of packet capture for devices without hard disk is as follows:



Global Configure

File Save Percent * 10 (5 - 50)，default:10

File Save Time * 30 (1 - 1,440) minutes, default:30

Option	Description
File Save Percent	Enter the maximum percentage of the remaining memory allowed by the packet capture file in the text box, the range is 5%-50%, and the default value is 10%.
File Save Time	Enter the length of time the packet capture file is saved in the text box, the unit is minutes, the range is 1-1440 minutes, and the default value is 30 minutes.

5. Click **OK**.

Test Tools

DNS Query, Ping and Traceroute can be used when troubleshooting the network.

DNS Query

To check the DNS working status of the device, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type a domain name into the **DNS Query** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Ping

To check the network connecting status, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type an IP address into the **Ping** box.
3. Click **Test**, and the testing result will be displayed in the list below.
4. The testing result contains two parts:
    - The Ping packet response. If there is no response from the target after timeout, it will print Destination Host Not Response, etc. Otherwise, the response contains sequence of packet, TTL and the response time.
    - Overall statistics, including number of packet sent, number of packet received, percentage of no response, the minimum, average and maximum response time.

Traceroute

Traceroute is used to test and record gateways the packet has traversed from the originating host to the destination. It is mainly used to check whether the network connection is reachable, and analyze the broken point of the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet can not be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As the result, the path from the originating host to the destination is identified. The system supports IPv4 and IPv6 peer addresses.

To test and record gateways the packet has traversed by Traceroute, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Select the VR in the Virtual Router drop-down list.
3. Select **IPv4** or **IPv6**.
4. Type an IP address into the **Traceroute** box.
5. Click **Test**, and the testing result will be displayed in the list below.

Chapter 14 High Availability

HA, the abbreviation for High Availability, provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network. To implement the HA function, you need to configure the two devices as HA clusters, using the identical hardware platform and firmware version, both enabling Virtual Router and AV functions, with anti-virus license installed. When one device is not available or can not handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

System supports three HA modes: Active-Passive (A/P), Active-Active (A/A), and Peer.

- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a primary device and the other acting as its backup device. The primary device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the primary device fails, the backup device will be promoted to primary and takes over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage.

- Active-Active (A/A) mode: When the security device is in NAT mode, routing mode or a combination of both, you can configure two Hillstone devices in the HA cluster as active, so that the two devices are running their own tasks simultaneously, and monitoring the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. This mode is known as the Active-Active mode. The A/A mode has the advantage of high-performance, as well as load-balancing.

- Peer mode: the Peer mode is a special HA Active-Active mode. In the Peer mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer mode is more flexible and is suitable for the deployment in the asymmetric routing environment.

HA Active-Active (A/A) and Peer mode may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Basic Concepts

HA Cluster

For the external network devices, an HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying an HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the primary and backup device of the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The primary device is in the active state and processes network traffic. When the primary device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0. In Active-Active (A/A) mode, the latest Hillstone version supports two HA groups, i.e., Group 0 and Group 1.

HA Node

To distinguish the HA devices in an HA group, you can use the value of HA Node to mark the devices. StoneOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, this does not make sense because both times is HA Node value of 0

Virtual Forward Interface and MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as the Virtual Forward Interface. The primary device of each HA group manages a virtual MAC (VMAC) address which is corresponding with its interface, and the traffic is forwarded on the interface. Different HA groups in an HA cluster cannot forward data among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In an HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the primary device.

HA Synchronization

To ensure the backup device can take over the work of the primary device when it fails, the primary device will synchronize its information with the backup device. There are three types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- SCVPN information
- DNS cache mappings
- ARP table
- PKI information
- DHCP information

- MAC table
- WebAuth information

System supports two methods to synchronize: real-time synchronization and batch synchronization. When the primary device has just been selected successfully, the batch synchronization will be used to synchronize all information of the primary device to the backup device. When the configurations change, the real-time synchronization will be used to synchronize the changed information to the backup device. Except for the HA related configurations and local configurations (for example, the host name), all the other configurations will be synchronized.

Configuring HA

This feature may vary slightly on different platforms, if there is a conflict between this guide and the actual page, the latter shall prevail.

To configure the HA function, take the following steps:

1. Configure an HA Virtual Forward Interface. For more information on configuring the interface, see "Creating a PPPoE Interface" on Page 81.

2. Configure an HA link interface which is used for the device synchronization and HA packets transmission.

    - Configure an HA cluster. Specify the HA VMAC prefix(optional) and ID of HA cluster to enable the HA function.

    - Configure an HA group. Specify the priority for devices and HA messages parameters.

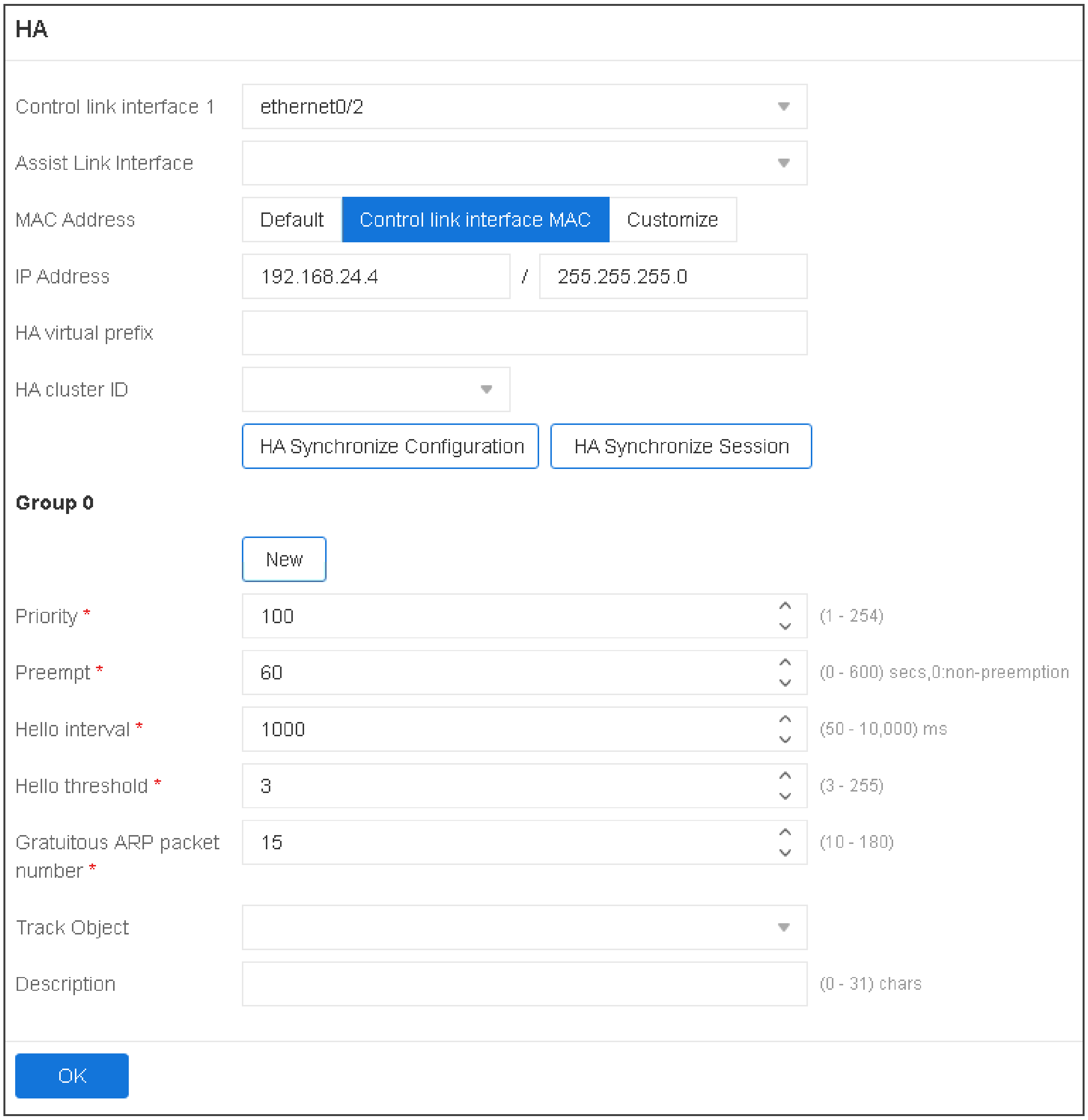
3. Configure an HA cluster. Specify the HA VMAC prefix(optional) and ID of HA cluster to enable the HA function.

4. Configure an HA group. Specify the priority for devices and HA messages parameters.

You need to configure the HA data link interface when configuring the HA function, and make sure the HA group interface 0 and interface 1 can be configured as an HA control link interface, but not an HA data link interface.

To configure HA, take the following steps:

1. Go to **System > HA**.



HA

Control link interface 1	ethernet0/2	
Assist Link Interface		
MAC Address	Default ● Control link interface MAC Customize	
IP Address	192.168.24.4 / 255.255.255.0	
HA virtual prefix		
HA cluster ID		
	HA Synchronize Configuration HA Synchronize Session	

Group 0

New

Priority *	100	(1 - 254)
Preempt *	60	(0 - 600) secs,0:non-preemption
Hello interval *	1000	(50 - 10,000) ms
Hello threshold *	3	(3 - 255)
Gratuitous ARP packet number *	15	(10 - 180)
Track Object		
Description		(0 - 31) chars

OK

Option	Description
Control link interface 1	Specifies the name of the HA control link interface. 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 (Backup device).

Option	Description
Control link interface 5	Specifies the name of interface on I/O module interface as the HA control link interface. For X10800 device, the system supports to configure the interface on I/O module as the HA control link interface in order to avoid the abnormal HA heartbeat and synchronization message due to the abnormal link of the interface on the control module. By default, the HA control link interface is on the control module.
Control link interface 6	Specifies the name of HA control link interface (Backup device).
Assist link interface	Specifies the name of the HA assist link interface. In the Active-Passive (A/P) mode, you can specify the HA assist link interface to receive and send heartbeat packets (Hello packets), and ensure the main and backup device of HA switches normally when the HA link fails. **Note**: • 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.

Option	Description
	- 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. 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. Note: 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.
Data link interface 2	Specifies the name of the HA data link interface 2. The data link interface is used to synchronize the data packet 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. Note: 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.
IP address	Specifies the IP address and netmask of the HA link interface, which can be an IPv4 address or an IPv6 address. When an IPv4 address is specified, the input format is A.B.C.D/M (e.g. 1.1.1.1/24). When an IPv6 address is

Option	Description
	specified, the input format is X.X.X.X::X/M (e.g. 2001::1/64). *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 VMAC 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. 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**: With the HA function enabled, if you want to modify the HA virtual MAC prefix, you may need to disable the HA function first.
HA cluster ID	Specifies an ID for HA cluster. 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. None indicates to disable the HA function.
Node ID	After enabling the HA function, specify the Node ID

Option	Description
	(HA Node) for the device. The IDs for two devices must be different. The range is 0 to 1. If you do not specify this value, the devices will obtain the Node ID by automatic negotiation.
Peer-mode	Selects the **Enable** checkbox to enable the HA Peer mode and specifies the role of this device in the HA cluster. The range is 0 to 1. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is will be in the disabled status.
Symmetric-routing	Select Symmetric-routing to make the device work in the symmetrical routing environment.
HA Synchronize Configuration	In some exceptional circumstances, the master and backup configurations may not be synchronized. In such a case you need to manually synchronize the configuration information of the master and backup device. Click **HA Synchronize Configuration** to synchronize the configuration information of the master and backup device.
HA Synchronize Session	By default the system will synchronize sessions between HA devices automatically. Session synchronization will generate some traffic, and will possibly impact device performance when the device is overloaded. You can enable automatic HA session synchronization according to the

Option	Description
	device workload to assure stability. Click **HA Synchronize Session** to enable automatic HA session synchronization.
New	After specifying the HA cluster ID, the system will create the HA group 0 automatically. Click New to create the HA group 1.
Delete	Click **Delete** to remove HA group 1 if needed.
Priority	Specifies the priority for the device. The device with higher priority (smaller number) will be selected as the primary device.
Preempt	Configure the preempt mode. When the preempt mode is enabled, once the backup device finds that its own priority is higher than the primary device, it will upgrade itself to become the primary device and the original primary device will become the backup device. The value of 0 indicates to disable the preempt mode. When the preempt mode is disabled, even if the device's priority is higher than the primary device, it will not take over the primary device unless the primary device fails.
Hello interval	Specifies the Hello interval value. The Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical.

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.
Gratuitous ARP packet number	Specifies the number of gratuitous ARP packets. When the backup device is selected 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.
Track object	Specifies the track object you have configured. 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	Type the descriptions of HA group into the box.

2. Click **OK**.

Chapter 15 System Management

The device's maintenance and management include:

- " System Information" on Page 1167
- "Device Management" on Page 1169
- "Configuration File Management" on Page 1194
- "Warning Page Management" on Page 1198
- "SNMP" on Page 1210
- "Upgrading System" on Page 1223
- "License" on Page 1230
- "Mail Server" on Page 1237
- "SMS Parameters" on Page 1240
- Extended Services
- "Test Tools" on Page 1152
- "VSYS (Virtual System)" on Page 1246

System Information

Users can view the general information of the system in the System Information page, including Serial Number, Hostname, Platform, System Time, System Uptime, HA State, Firmware, Boot File, Signature Database and so on.

Viewing System Information

To view system information, select **System** > **System And Database**.

System Information	
Serial Number	Show the serial number of device.
Hostname	Show the name of device.
Platform	Show the platform model of device.
System Time	Show the system date and time of device.
System Uptime	Show the system uptime of device.
HA State	Show the HA status of device. • Standalone: Non-HA mode that represents HA is disabled. • Init: Initial state. • Hello: Negotiation state that represents the device is consulting the relationship between the master and backup. • Master: Master state that represents the current device is the master. • Backup: Backup state that represents the current device

System Information	
	is the backup. - Failed: Fault state that represents the device has failed.
Firmware	Show the current firmware version of the device.
Boot File	Show the current boot file of the device.
Signature DB Information	
Application Identification Signature	Show the current version of the application signature database and the date of the last update.
URL Category Signature	Show the current version of the URL signature database and the date of the last update.
IP Reputation Database	Show the current version of the perimeter traffic filtering signature database and the date of the last update.
Anti-Virus Signature	Show the current version of the antivirus signature database and the date of the last update.
IPS Signature	Show the current version of the IPS signature database and the date of the last update.
Botnet Prevention Signature	Show the current version of the Botnet Prevention signature database and the date of the last update.
Sandbox Whitelist DB	Show the current version of the Sandbox Whitelist DB and the date of the last update.

Notes: The signature is all license controlled, so you need to make sure that your system has installed that license. Refer to "License" on Page 1230.

Device Management

Introduces how to configure the Administrator, Trust Host, MGT Interface, System Time, NTP Key and system options.

Administrators

Device administrators of different roles have different privileges. The system supports predefined administrator roles and customized administrator roles. By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information.
- **admin-read-only**: Permission for reading and executing. You can view the current or historical configuration information.
- **operator**: Permission for reading, executing and writing. You have the authority over all features except modify the Administrator's configuration, view the current or historical configuration information , but no permission to check the log information.
- **auditor**: You can only operate on the log information, including view, export and clear.

The following table shows the permissions to different types of administrators.

Operation	Administratior	Administratior (read-only)	Auditor	Operator
Configure (including saving configuration)	√	χ	χ	√
Configure administrator	√	χ	χ	χ
Restore factory	√	χ	χ	χ

Operation	Administrator	Administrator (read-only)	Auditor	Operator
default				
Delete configuration file	√	χ	χ	√
Roll back configuration	√	χ	χ	√
Reboot	√	χ	χ	χ
View configuration information	√	√	χ	√
View log information	√	√	√	χ
Modify current admin password	√	√	χ	√
ping/traceroute	√	√	χ	√

Notes:

- The device ships with a default administrator named hillstone. You can modify the setting of hillstone. However, this account cannot be deleted.
- Other administrator roles (except default administrator) cannot configure the admin settings, except modifying its own password.
- The system auditor can manage one or more logs, but only the system administrator can manage the log types.

VSYS Administrator

Administrators in different VSYSs are independent from each other. Administrators in the root VSYS are known as root administrators and administrators in the non-root VSYS are known as non-root administrators. The system supports four types of administrator, including Administrators, Administrator(read-only), Operator, and Auditor.

When creating VSYS administrators, you must follow the rules listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into the non-root VSYS.
- After logging into the root VSYS, the root administrators can switch to the non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after a successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in form of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The following table shows the permissions to different types of VSYS administrators.

Operation	Root VSYS Administratior	Root VSYS Administratior (read-only)	Root VSYS Auditor	Root VSYS Operator	Non-root VSYS Administratior	Non-root VSYS Administratior (read-only)	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including saving configuration)	√	χ	χ	√	√	χ	√	χ
Configure administrator	√	χ	χ	χ	√	χ	χ	χ
Restore factory default	√	χ	χ	χ	χ	χ	χ	χ
Delete configuration file	√	χ	χ	√	√	χ	√	χ
Roll back configuration	√	χ	χ	√	√	χ	√	χ

Operation	Root VSYS Administratior	Root VSYS Administratior (read-only)	Root VSYS Auditor	Root VSYS Operator	Non-root VSYS Administratior	Non-root VSYS Administratior (read-only)	Non-root VSYS Operator	Non-root VSYS Auditor
Reboot	√	χ	χ	χ	χ	χ	χ	χ
View configuration information	√	√	χ	√	View information in current VSYS	View information in current VSYS	View information in current VSYS	χ
View log information	√	√	√	χ	√	√	χ	√
Modify current admin password	√	√	√	√	√	√	√	√
ping/traceroute	√	√	χ	√	χ	χ	χ	χ

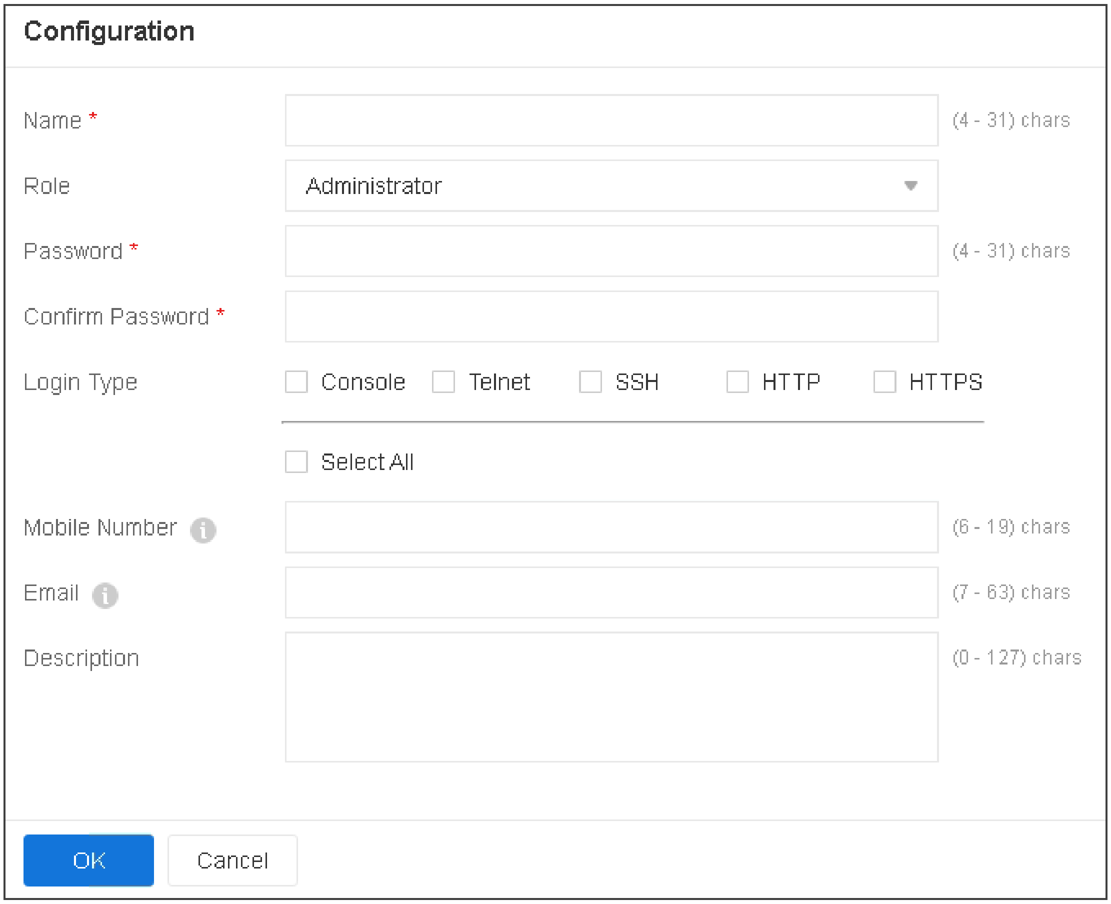
Creating an Administrator Account

To create an administrator account, take the following steps:

1. Select **System** > **Device Management** > **Administrators**.

2. Click **New**.

3. In the Configuration dialog box, configure the following.



Configuration

Name *		(4 - 31) chars
Role	Administrator	
Password *		(4 - 31) chars
Confirm Password *		
Login Type	□ Console □ Telnet □ SSH □ HTTP □ HTTPS □ Select All	
Mobile Number		(6 - 19) chars
Email		(7 - 63) chars
Description		(0 - 127) chars

Configure the following options.

Option	Description
Name	Type a name for the system administrator account.
Role	From the **Role** drop-down list, select a role for the administrator account. Different roles have different privileges. • Administrator: Permission for reading, executing

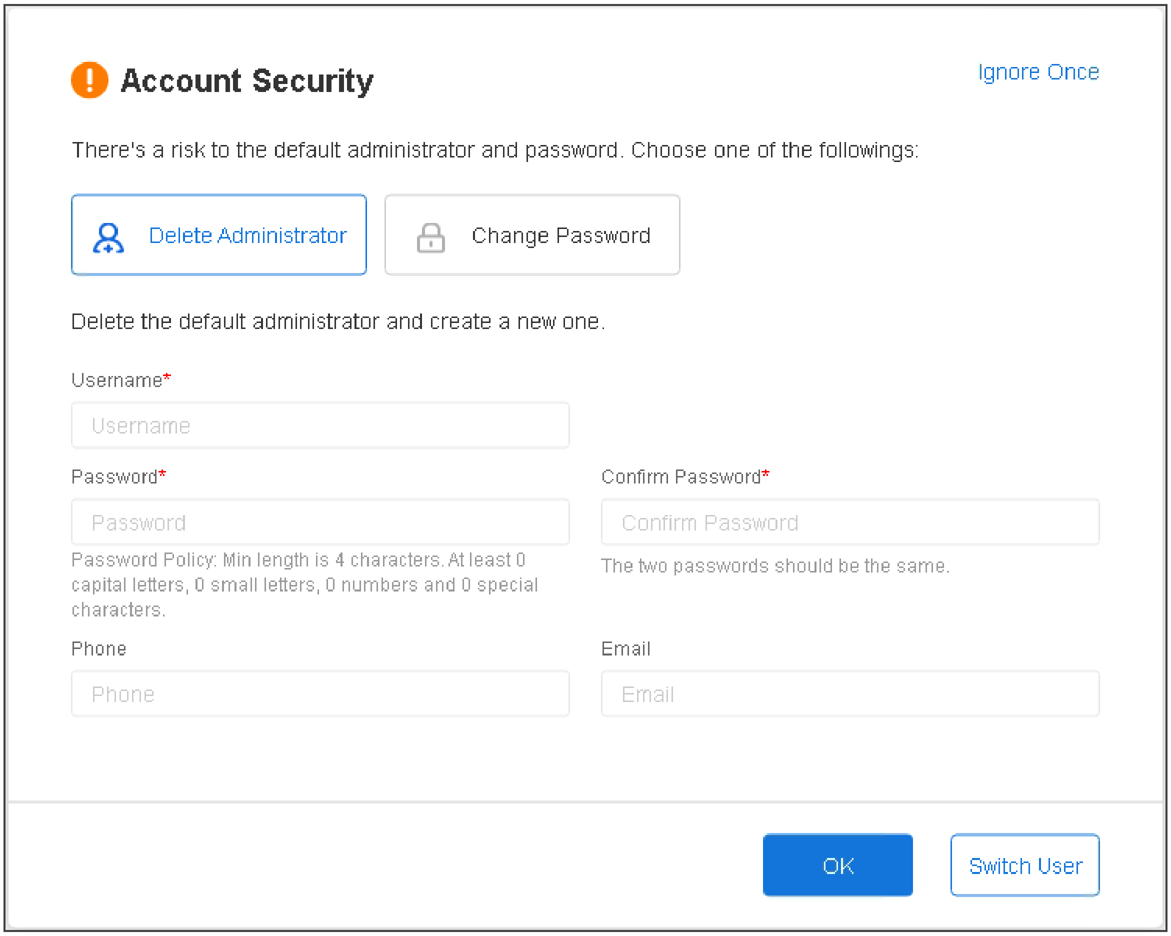
Option	Description
	and writing. This role has the authority over all features. - Operator: YThis role has the authority over all features except modifying the Administrator's configurations, and has no permission to check the log information - Auditor: You can only operate on the log information, including the view, export and clear. - Administrator-read-only: Permission for reading and executing. You can view the current or historical configuration information.
Password	Type a login password for the admin into the **Password** box. The password should meet the requirements of Password Strategy.
Confirm Password	Re-type the password into the **Confirm Password** box.
Login Type	Select the access method(s) for the admin, including Console, Telnet, SSH, HTTP and HTTPS. If you need all access methods, select **Select All**.
Description	Enter descriptions for the administrator account.

4. Click **OK**.

Configuring Login Options for the Default Administrator

System has a default administrator "hillstone" and a default password "hillstone". However, there is a risk that the default username and password may be cracked. To avoid that risk, when you logs in with the default username and password, the system will prompt the following information:

- Delete Default Administrator: Click the **Delete Administrator** radio button to delete the default administrator (hillstone), and then specify a new username , password and other information in respective textboxes to create a new administrator account. After creating the new administrator account, you can log in again with the new username and password.



Account Security

There's a risk to the default administrator and password. Choose one of the followings:

Delete the default administrator and create a new one.

Username*

Password*

Password Policy: Min length is 4 characters. At least 0 capital letters, 0 small letters, 0 numbers and 0 special characters.

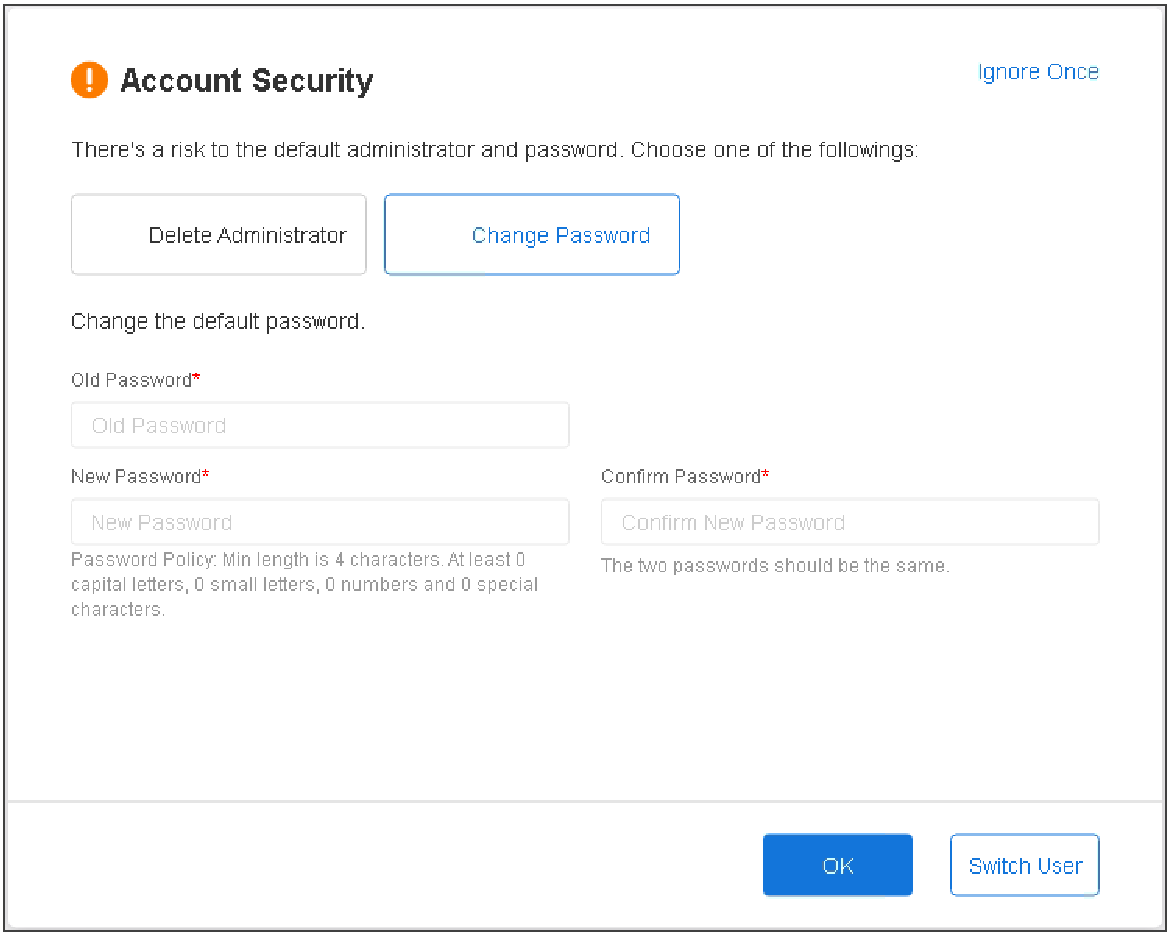
Confirm Password*

The two passwords should be the same.

Phone

Email

- Change Default Password: Click the **Change Password** radio button, and specify a new password for the default user in the textbox. Then, you can log in again with the new password.



There's a risk to the default administrator and password. Choose one of the followings:

Change the default password.

Password Policy: Min length is 4 characters. At least 0 capital letters, 0 small letters, 0 numbers and 0 special characters.

The two passwords should be the same.

- Ignore Once: Click the **Ignore Once** radio button, and you will immediately log in with the default username (hillstone) and password (hillstonae). You will be prompted again when log in with the default username and password next time.

Notes: In the HA Active-Passive (A/P) mode, the backup device does not support this function, and you can log in with the default username and password.

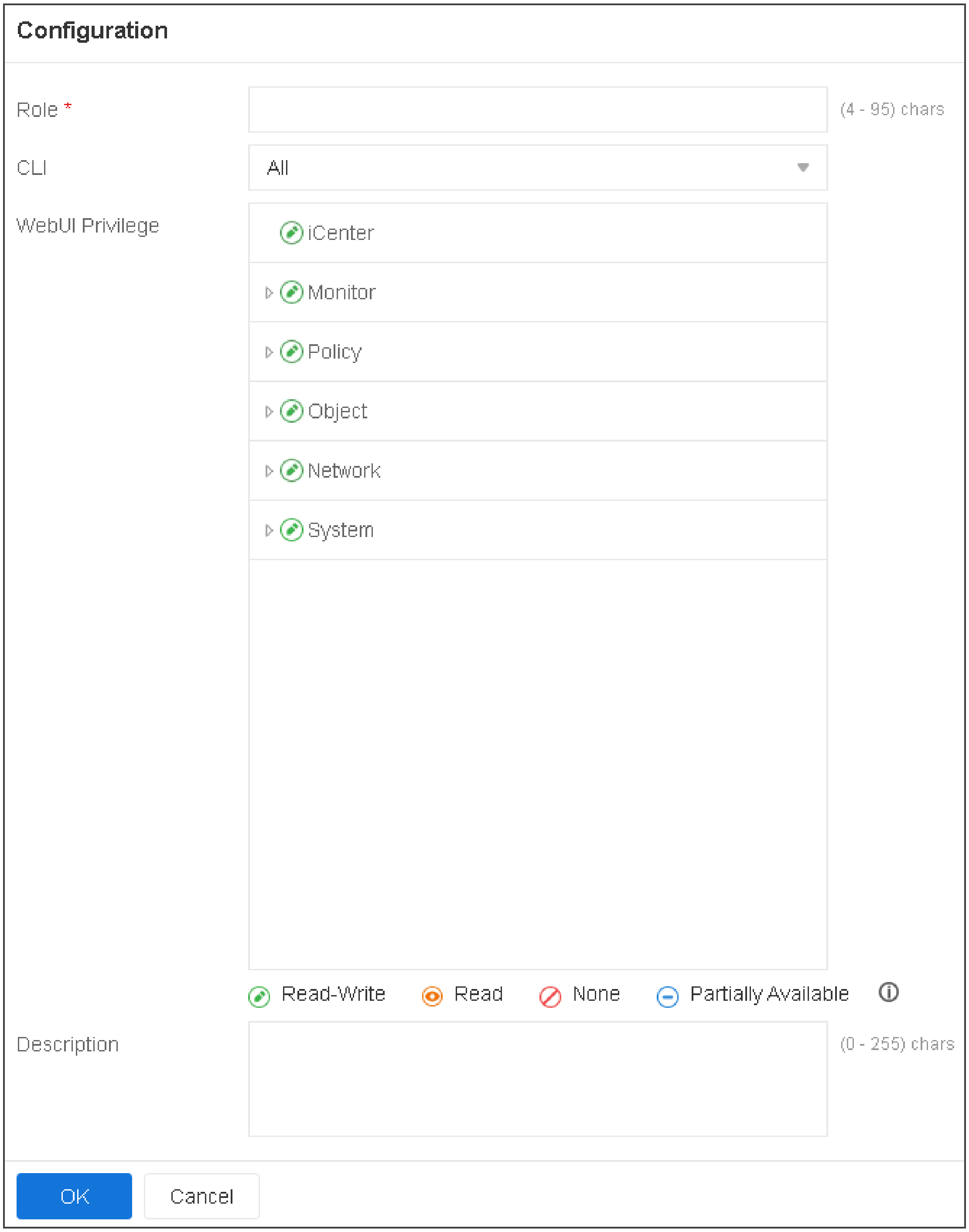
Admin Roles

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles. The pre-defined administrator role cannot be deleted or edited. You can customize administrator roles according to your requirements:

To create a new administrator role, take the following steps:

1. Select **System > Device Management > Admin Roles**.

2. Click **New**.



Configuration

Role * (4 - 95) chars

CLI: All

WebUI Privilege

- iCenter
- ▷ Monitor
- ▷ Policy
- ▷ Object
- ▷ Network
- ▷ System

Read-Write · Read · None · Partially Available ⓘ

Description (0 - 255) chars

OK · Cancel

3. In the Configuration dialog box, configure the following:

Option	Description
Role	Enter the role name.
CLI	Specify the administrator role's privileges of CLI.
WebUI Privilege	Click module name to set the administrator role's privilege. ⊘ represents the administrator role does not have privilege of the specified module, and cannot read and edit the configurations of the specified module. ◉ represents the administrator role has the read privilege of the specified module, and cannot edit the configurations. ✎ represents the administrator role can read and edit the configurations of the specified module.
Description	Specify the description for this administrator role.

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

Trusted Host

The device only allows the trusted host to manage the system to enhance the security. Administrator can specify an IP range, MAC address or MAC range, and the hosts in the specified range are the trusted hosts. Only trusted hosts could access the management interface to manage the device.

Notes: If system cannot be managed remotely, check the trusted host configurations.

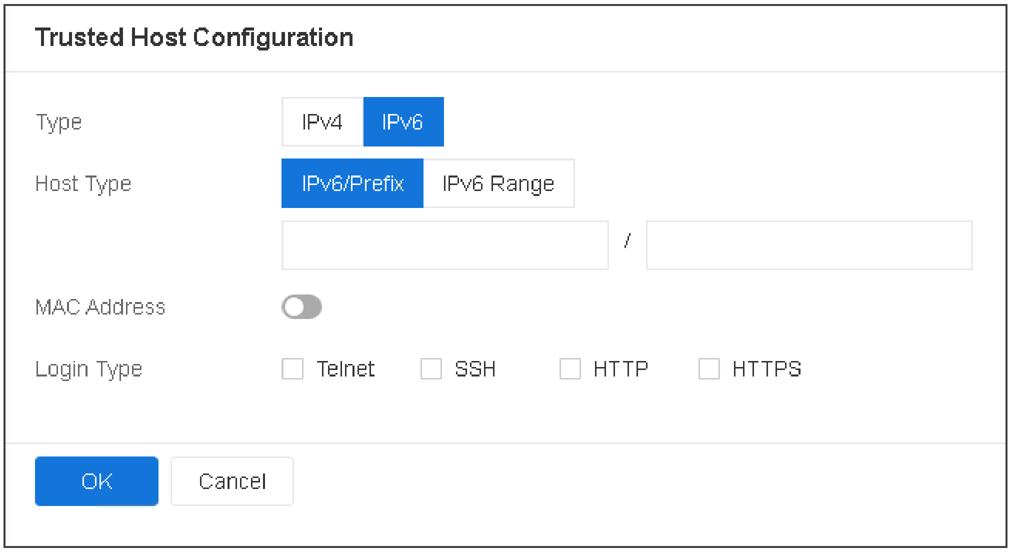
Creating a Trusted Host

To create a trust host, take the following steps:

1. Select **System** > **Device Management** > **Trusted Host**.

2. Click **New**.

3. In the Trusted Host Configuration dialog box, configure these values.



Configure the following options.

Option	Description
Match Address Type	Select the address type to match the trusted host. When "IPv4" is selected, you need to specify the IP range, and only the hosts in the IP range can be the trust hosts; when "IPv4&MAC" is selected, you need to specify the IP range or MAC address/range, and only the hosts in the specified IP range and MAC range can be the trust hosts.
IP Type	Specify the IP range of the trusted hosts: • IP/Netmask: Type the IP address and netmask of the trusted hosts. • IP Range: Type the start IP and end IP of the trus-

Option	Description
	ted hosts.
MAC Type	Specifies theMAC address or MAC range of the trust hosts: - MAC Address: Type the MAC address of the trusted hosts. - MAC Range: Type the start IP and end IP of the trusted hosts.
Login Type	Select the access methods for the trust host, including Telnet, SSH, HTTP and HTTPS.

4. Click **OK**.

Management Interface

The device supports the following access methods: Console, Telnet, SSH and WebUI. You can configure the timeout value, port number, PKI trust domain of HTTPS,and PKI trust domain of certificate authentication. When accessing the device through Telnet, SSH, HTTP or HTTPS, if login fails three times in one minute, the IP address that attempts the login will be blocked for 2 minutes during which the IP address cannot connect to the device.

To configure the access methods:

1. Select **System** > **Device Management** > **Management Interface**.

2. In the Management Interface tab, configure these values.

   Configure the following options.

Option	Description
Console	Configure the Console access method parameters.

Option	Description
	- Timeout: Type the Console timeout value into the **Timeout** box. The value range is 0 to 60. The default value is 10. The value of 0 indicates never timeout. If there is no activity until the timeout, system will drop the console connection.
Telnet	Configure the Telnet access method parameters. - Timeout: Specifies the Telnet timeout value. The value range is 1 to 60. The default value is 10. - Port: Specifies the Telnet port number. The value range is 1 to 65535. The default value is 23.
SSH	Configure the SSH access method parameters. - Timeout: Specifies the SSH timeout value. The value range is 1 to 60. The default value is 10. - Port: Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.
Web	Configure the WebUI access method parameters. - Multiple Login with Same Account: Select the check box and users are allowed to log in to devices with the same account simultaneously. By default, the function is disabled. In the default situation, when a same account is used to log in again, the previous login account will be kicked out.

Option	Description
	- Timeout: Specifies the WebUI timeout value. The value range is 1 to 1440. The default value is 10. - HTTP Port: Specifies the HTTP port number. The value range is 1 to 65535. The default value is 80. - HTTPS Port: Specifies the HTTPS port number. The value range is 1 to 65535. The default value is 443. - HTTPS Trust Domain: Select the trust domain existing in the system from the drop-down list. When HTTPS starts, HTTPS server will use the certificate with the specified trusted domain. By default, the trust domain trust_domain_default will be used. - Certificate Authentication: With this checkbox selected, system will start the certificat authentication. The certificate includes the digital certificate of users and secondary CA certificate signed by the root CA.Certificate authentication is one of two-factor authentication. The two-factor authentication does not only need the user's name and password authentication, but also needs other authentication methods, like a certificate or fingerprint.

Option	Description
	- Certificate Trust Domain: After enabling the certificate authentication and logging into the device over HTTPS, HTTPS server will use the certificate with the specified trusted domain.Make sure that root CA certificate is imported into it. - CN Check： After the CN check is enabled, the name of the root CA certificate is checked and verified when the user logs in. Only the certificate and the user can be consistent, and the login succeeds.

3. Click **OK**.

Notes: When changing HTTP port, HTTPS port or HTTPS Trust Domain, the web server will restart. You may need to log in again if you are using the Web interface.

System Time

You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.

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.
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**.

Configuring NTP

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 configure NTP:

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 . • 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.

Option	Description
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**.

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.

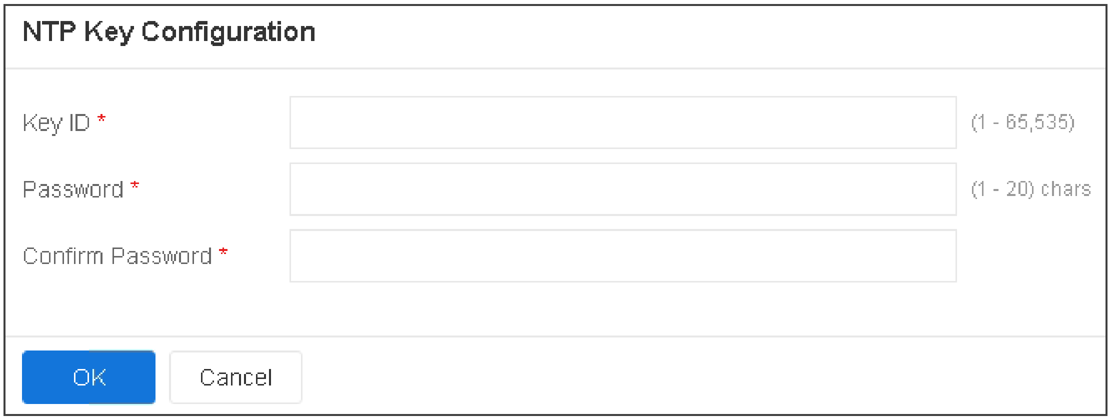
Creating a NTP Key

To create an NTP key:

1. Select **System** > **Device Management** > **NTP Key**.

2. Click **NEW**.

3. In the NTP Key Configuration dialog box, configure these values.



NTP Key Configuration

Key ID * (1 - 65,535)

Password * (1 - 20) chars

Confirm Password *

Configure the following options.

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.

4. Click **OK**.

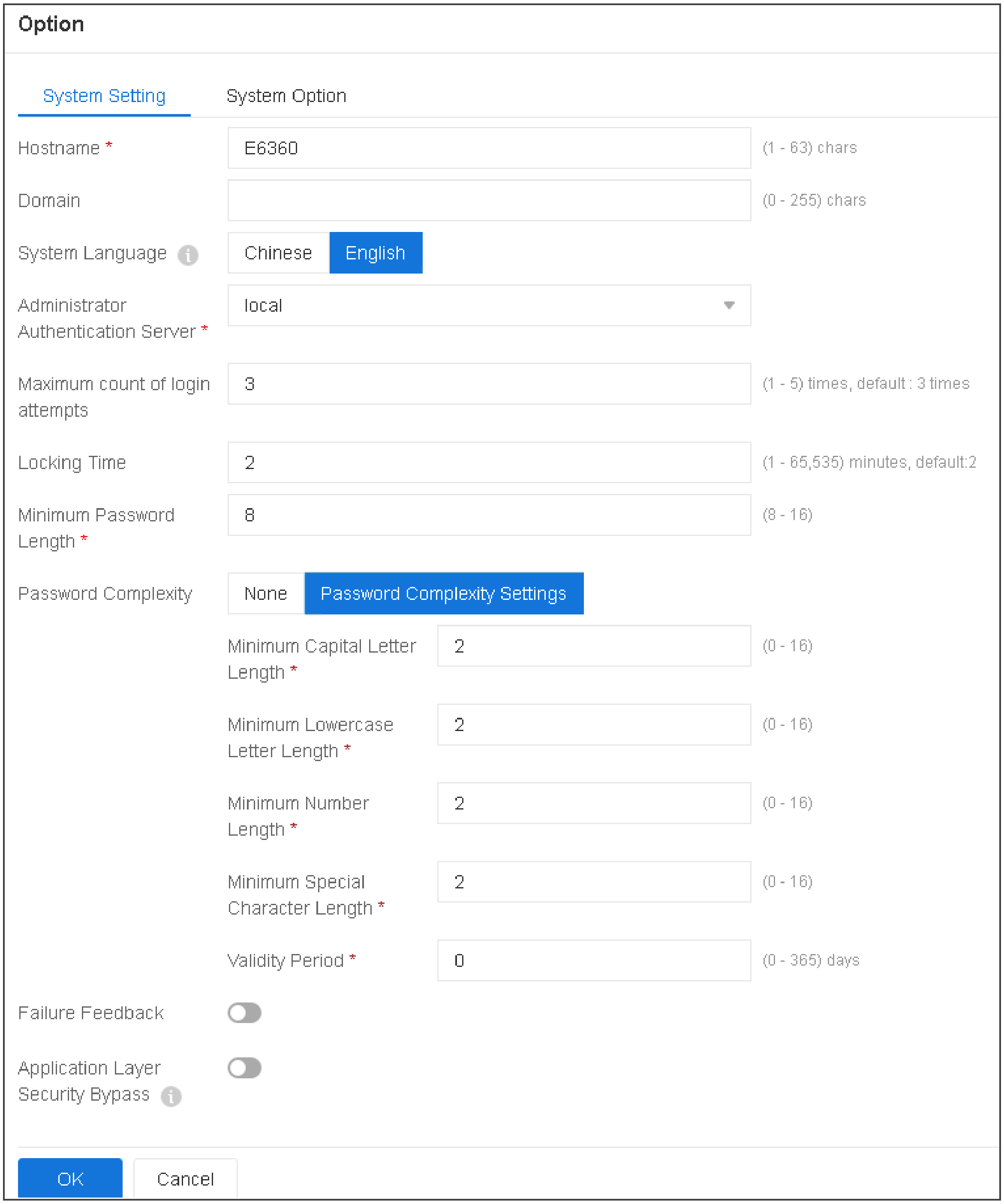
Option

Specifies system options, including system language, administrator authentication server, host name, password strategy, reboot and exporting the system debugging information.

To change system option, take the following steps:

1. Select **System** > **Device Management** > **Option**.

2. Select **System Setting** .Configure the following.



Option

System Setting | System Option

Hostname *	E6360	(1 - 63) chars
Domain		(0 - 255) chars
System Language	Chinese [✓ English]	
Administrator Authentication Server *	local	
Maximum count of login attempts	3	(1 - 5) times, default : 3 times
Locking Time	2	(1 - 65,535) minutes, default:2
Minimum Password Length *	8	(8 - 16)
Password Complexity	None [✓ Password Complexity Settings]	
Minimum Capital Letter Length *	2	(0 - 16)
Minimum Lowercase Letter Length *	2	(0 - 16)
Minimum Number Length *	2	(0 - 16)
Minimum Special Character Length *	2	(0 - 16)
Validity Period *	0	(0 - 365) days
Failure Feedback	○	
Application Layer Security Bypass	○	

Option	Description
Hostname	Type a host name you want to change into the **Host-**

Option	Description
	name box.
Domain	Type a domain name you want to specify into the **Domain** box.
System Language	You can select **Chinese** or **English** according to your own requirements.
Administrator1. Authentication Server	Select a server to authenticate the administrator from the drop-down list.
Minimum Password Length	Specifies the minimum length of password. The value range is 4 to 16 characters. The default value is 4.
Password Complexity	**None** means no restriction on the selection of password characters.You can select **Password Complexity Settings** to enable password complexity checking and configure password complexity. • Minimum Capital letters length: The default value is 2 and the range is 0 to 16. • Minimum Lowercase Letter Length: The default value is 2 and the range is 0 to 16. • Minimum Number Length: The default value is 2 and the range is 0 to 16. • Minimum Special Character Length: The default value is 2 and the range is 0 to 16.

Option	Description
	- Validity Period: The unit is day.The range is 0 to 365.The default value is 0, which indicates that there is no restriction on validity period of the password.

3. Click **OK**.

Rebooting the System

Some operations like license installation or image upgrading will require the system to reboot before it can take effect.

To reboot a system, take the following steps:

1. Go to **System** > **Device Management** > **Option** .
2. Click **Reboot**, and select **Yes** in the prompt.
3. The system will reboot. You need to wait a while before it can start again.

System Debug

System debug is supported for you to check and analyze the problems.

Failure Feedback

To enable the failure feedback function, take the following steps:

1. Select **System** > **Device Management**> **Option**.
2. In the System Tools dialog box, select the **Enable** check box for Failure feedback, and then system will automatically send the technical support file to the manufacturer.

System Debug Information

System debugging helps you to diagnose and identify system errors by the exported file.

To export the system debugging information, take the following steps:

1. Select **System > Device Management> Option**.
2. Click **Export**, system will pack the file in /etc/local/core and prompt to save tech-support file. After selecting the saved location and click **OK**, you can export the file successfully.

Application Layer Security Bypass

System supports to bypass the application layer functions, including Intrusion Prevention System, Anti Virus, and other application layer security protection function.

To enable application layer security bypass, take the following steps:

1. Select **System > Device Management> Option**.

2. In the System Setting page, select the **Enable** button for application layer security bypass， and click **OK**.

Configuration File Management

System configuration information is stored in the configuration file, and it is stored and displayed in the format of command line. The information that is used to initialize the Hillstone device in the configuration file is known as the initial configuration information. If the initial configuration information is not found, the Hillstone device will use the default parameters for the initialization. The information being taking effect is known as the current configuration information.

System initial configuration information includes current initial configuration information (used when the system starts) and backup initial configuration information. System records the latest ten saved configuration information, and the most recently saved configuration information for the system will be recorded as the current initial configuration information. The current configuration information is marked as Startup; the previous nine configuration information is marked with number from 0 to 8, in the order of save time.

You can not only export or delete the saved configuration files, but also export the current system configurations.

Managing Configuration File

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

To manage the system configuration files, take the following steps:

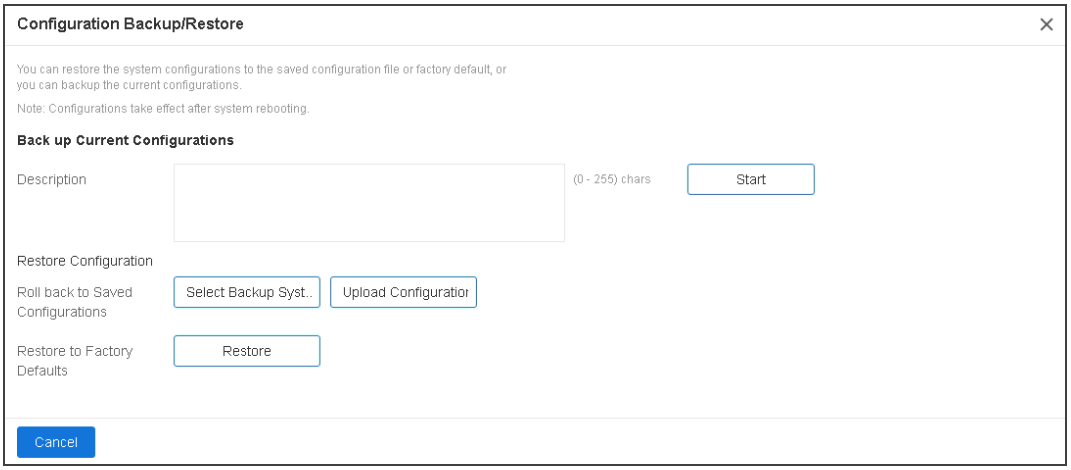
1. Select **System** > **Configuration File Management** > **Configuration File List**.

2. In the Configuration File List page, configure the following.

   - Export: Select the configuration file you want to export, and click **Export**.

   - Delete: Select the configuration file you want to delete, and click **Delete**.

   - Backup Restore: You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.



Configuration Backup/Restore

You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.

Note: Configurations take effect after system rebooting.

Back up Current Configurations

Description (0 - 255) chars

Option	Description
Back up Current Configurations	Type descriptions for the configuration file into **Description** box. Click **Start** to backup.
Restore Configuration	Roll back to Saved Configurations: • Select Backup System Configuration File: Click this button, then select Backup Configuration File from the list. Click **OK**. • Upload Configuration File: Click this button. In the Importing Configuration File dialog box, click **Browse** and choose a local configuration file you need in your PC. If you need to make the configuration file take effect, select the check box. Click **OK**. Restore to Factory Defaults: • Click **Restore**, in the Restore to Factory

Option	Description
	Defaults dialog box, click **OK**.

Notes: Device will be restored to factory defaults. Meanwhile, all the system configurations will be cleared, including backup system configuration files.

Viewing the Current Configuration

To view the current configuration file:

1. Select **System** > **Configuration File Management** > **Current Configurations**.

2. Click **Export** to export the current configuration file.

Importing/Exporting the Configuration of All VSYS

You can export the current configuration file of VSYS, and import the saved configuration file of VSYS.

To export the current configuration file of VSYS, take the following steps:

1. Select **System > Configuration File Management > Configuration File List**.

2. Click **Export All Vsys Configuration** to export the current configuration file of VSYS.

To import the saved configuration file of VSYS, take the following steps:

1. Select **System > Configuration File Management > Configuration File List**.

2. Click **Import All Vsys Configuration** .

3. Click **Brown** to select the configuration file needed to be imported. The file type can be GZ and ZIP.

4. After importing the configuration file, you need to reboot to take effect. Select the **Restart now**, make the new configuration take effect checkbox to reboot immediately.

5. Click **OK**.

Warning Page Management

Warning page management includes picture management and page management of user-defined warning pages.

Related links :

- Configuring URL Filtering Objects -Warning Page
- Configuring Content Filtering Objects - Warning Page

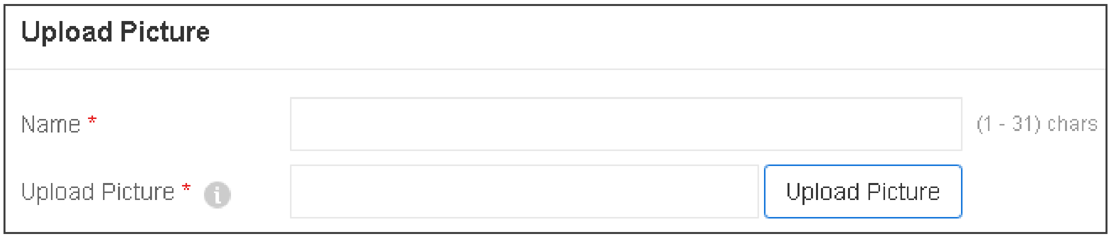
Page Management

You can upload the required pictures and reference the picture in the user-defined warning page as needed. In the picture management page, the name , previews and the last modification time of uploaded picture will be displayed in a list.

Uploading the Picture

To upload the picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.
2. Click **New** to open the **Upload Picture Configuration** dialog.



Upload Picture

Name * (1 - 31) chars

Upload Picture *

3. Type the name of the user-defined picture into the **Name** box.
4. Click **Upload Picture** and select the local picture file to be uploaded.

5. After uploading, the picture will be previewed in the dialog.

6. Click **OK** to save the configuration.

Notes: Only the following types of pictures can be uploaded: jpeg, jpg, png, gif, jfif; the size of uploaded pictures is limited to 24KB; the system allows up to 32 picture files to be uploaded.

Editing the Picture

To replace and modify the uploaded picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.

2. Select the check box of the picture to be edited in the list and click the **Edit**.

3. In the **Upload Picture Configuration** dialog, click the **Upload Picture** button to upload the picture file.

4. Click **OK** to save the configuration.

Deleting the Picture

To delete the picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.

2. Select the check box of the picture to be deleted in the list and click the **Delete**.

3. In the delete confirmation dialog, click the **Yes** button to complete the deletion.

Notes: Before deleting the picture, please make sure that the picture is not referenced by the user-defined warning page, otherwise it cannot be deleted.

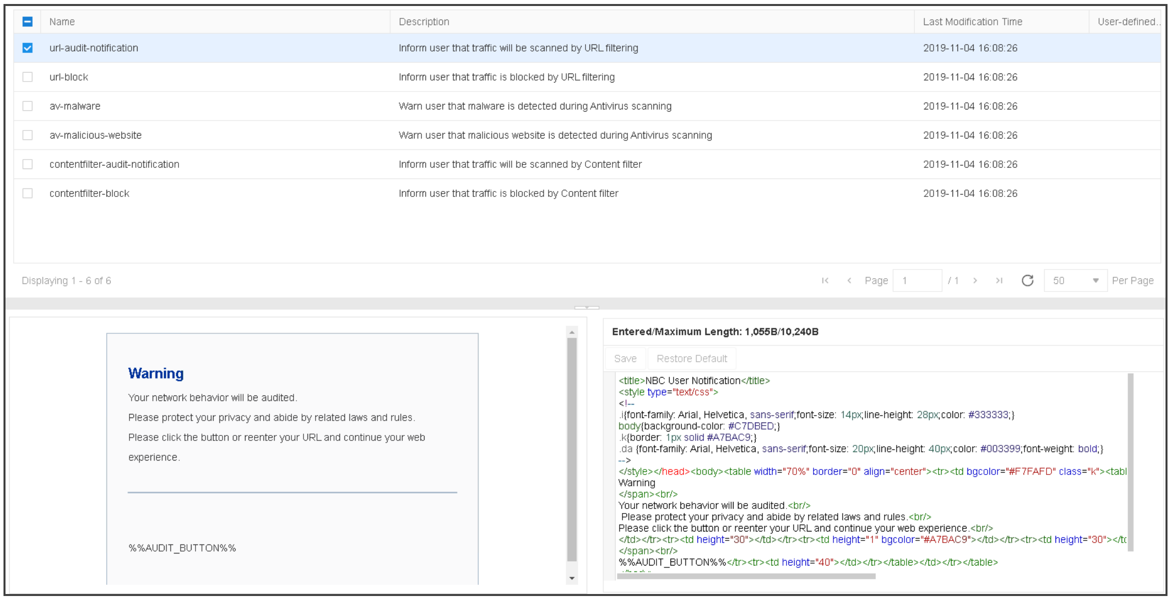
Page Management

System supports 6 types of user-defined warning pages, and the user-defined warning page already contains the reference string and warning information content displayed by default. You can add or modify the reference string by using html encoding to customize the warning message text, pictures and other content.

- url-adudit-notification: Inform user that traffic will be scanned by URL filtering.
- url-block: Inform user that traffic is blocked by URL filtering.
- av- malware: Warn user that malware is detected during Antivirus scanning.
- av-malicious-website: Warn user that malicious website is detected during Antivirus scanning.
- ontentfilter-audit-notification: Inform user that traffic will be scanned by Content filter.
- contentfilter-block: Inform user that traffic is blocked by Content filter.

To configure the user-defined warning page, take the following steps:

1. Select **System** > **Warning Page Management** > **Page Management**.



▬	Name	Description	Last Modification Time	User-defined...
☑	url-audit-notification	Inform user that traffic will be scanned by URL filtering	2019-11-04 16:08:26	
□	url-block	Inform user that traffic is blocked by URL filtering	2019-11-04 16:08:26	
□	av-malware	Warn user that malware is detected during Antivirus scanning	2019-11-04 16:08:26	
□	av-malicious-website	Warn user that malicious website is detected during Antivirus scanning	2019-11-04 16:08:26	
□	contentfilter-audit-notification	Inform user that traffic will be scanned by Content filter	2019-11-04 16:08:26	
□	contentfilter-block	Inform user that traffic is blocked by Content filter	2019-11-04 16:08:26	

Displaying 1 - 6 of 6

Warning

Your network behavior will be audited.

Please protect your privacy and abide by related laws and rules.

Please click the button or reenter your URL and continue your web experience.

%%AUDIT_BUTTON%%

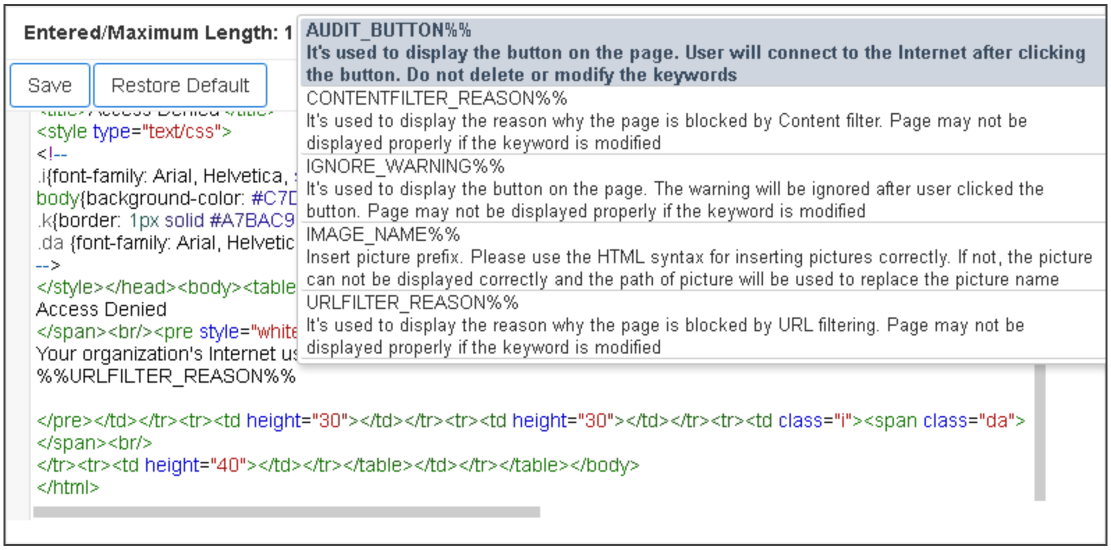
Entered/Maximum Length: 1,055B/10,240B

```
<title>NBC User Notification</title>
<style type="text/css">
<!--
.i{font-family: Arial, Helvetica, sans-serif;font-size: 14px;line-height: 28px;color: #333333;}
body{background-color: #C7DBED;}
.k{border: 1px solid #A7BAC9;}
.da {font-family: Arial, Helvetica, sans-serif;font-size: 20px;line-height: 40px;color: #003399;font-weight: bold;}
-->
</style></head><body><table width="70%" border="0" align="center"><tr><td bgcolor="#F7FAFD" class="k"><tabl
Warning
</span><br/>
Your network behavior will be audited.<br/>
 Please protect your privacy and abide by related laws and rules.<br/>
Please click the button or reenter your URL and continue your web experience.<br/>
</td></tr><tr><td height="30"></td></tr><tr><td height="1" bgcolor="#A7BAC9"></td></tr><tr><td height="30"></tc
</span><br/>
%%AUDIT_BUTTON%%</tr><tr><td height="40"></td></tr></table></td></tr></table>
```

In the Page Management page, view the details of user-defined warning page.

- The list at the top of the page shows the name, description, last modification time and the enable status of 6 types of user-defined warning pages supported by system.
- In the lower left part of the page, a page preview showing the selected user-defined warning page.
- In the lower right part of the page, the default html encoding of the user-defined warning page is displayed, and you can use the html encoding method to customize the page content in this part.

2. In the list above, select the check box of the warning page that needs to be customized.
3. In the html encoding page below, modify the content of the warning message, or enter "%%" to select the reference string to be added and reference the corresponding content or picture.



```
<style type="text/css">
<!--
.i{font-family: Arial, Helvetica,
body{background-color: #C7D
.k{border: 1px solid #A7BAC9
.da {font-family: Arial, Helvetic
-->
</style></head><body><table
Access Denied
</span><br/><pre style="white
Your organization's Internet us
%%URLFILTER_REASON%%

</pre></td></tr><tr><td height="30"></td></tr><tr><td height="30"></td></tr><tr><td class="i"><span class="da">
</span><br/>
</tr><tr><td height="40"></td></tr></table></td></tr></table></body>
</html>
```

AUDIT_BUTTON%%
It's used to display the button on the page. User will connect to the Internet after clicking the button. Do not delete or modify the keywords

CONTENTFILTER_REASON%%
It's used to display the reason why the page is blocked by Content filter. Page may not be displayed properly if the keyword is modified

IGNORE_WARNING%%
It's used to display the button on the page. The warning will be ignored after user clicked the button. Page may not be displayed properly if the keyword is modified

IMAGE_NAME%%
Insert picture prefix. Please use the HTML syntax for inserting pictures correctly. If not, the picture can not be displayed correctly and the path of picture will be used to replace the picture name

URLFILTER_REASON%%
It's used to display the reason why the page is blocked by URL filtering. Page may not be displayed properly if the keyword is modified

User-defined warning page can contain the following reference strings.

Reference String	Description
%%AUDIT_ BUTTON%%	It's used to display a button on the page. When you click the button, you can connect to the Internet. **Note**: This reference string is required in the "url-adudit-notification" and "contentfilter-audit-notification" pages. Please do not delete or modify this keyword.
%%IGNORE_ WARNING%%	It is used to display a button on the page. You can click the button to ignore the prompt and continue browsing. **Note**: This reference string is the default reference string displayed on the page. After modification, it may cause ignore prompts and buttons to be displayed normally.
%%IMAGE_NAME%%	Picture prefix, which is used to reference a picture uploaded in Picture Management, and output the picture on the user-defined warning page.
%%URLFILTER_ REASON%%	It's used to display the reason for URL filtering blocking on the "url-block" page. **Note**: This reference string is the default reference string displayed on the page. After modification, the reason may not be displayed normally.

Reference String	Description
%%VIRUS_NAME%%	It's used to display the virus name on the "av- malware" page. **Note**:This reference string is the default reference string displayed on the page. After modification, the virus name may not be displayed normally.
%%CONTENTFILTER_ REASON%%	It's used to display the reason for content filtering blocking on the "contentfilter-block" page. **Note**:This reference string is the default reference string displayed on the page. After modification, the reason may not be displayed normally.

4. After modifying the html encoding, click **Save** to save the configuration. At the same time, the user-defined warning page will be enabled, and ⏻ will be displayed in the "User-defined" column of the upper list.

5. If you need to restore the default content of the cuser-defined warning page, click the **Restore Default**.

Extended Services

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

System supports to connect to other Hillstone products to provide more services. Currently, the extended services include connecting Hillstone Security Management (HSM) and Hillstone Cloud. For specific configurations, refer to one of the following topics:

- Connecting to HSM
- Connecting to Hillstone Cloud

Connecting to Hillstone Cloud

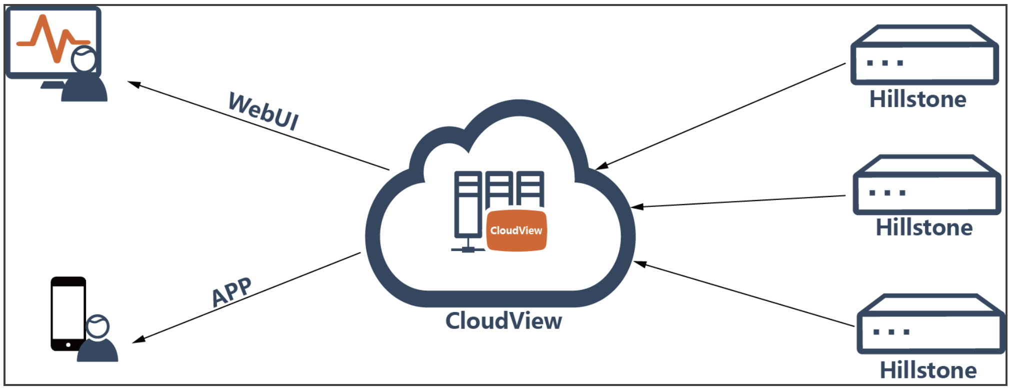
Hillstone Cloud is a cloud security services platform in the mobile Internet era, including CloudView, cloud sandbox and Cloud Vista (Threat Intelligence Center).

After the Hillstone device is properly configured to connect the Cloud , you can register the Hillstone device to the public cloud and connect the device with the Cloud, thereby remotely monitoring the device through Cloud.

- CloudView: CloudView is a SaaS products of security area. It is deployed in the public cloud to provide users with online on-demand services. Users can get convenient, high quality and low cost value-added security services through the Internet and APP, and get a better security experience.

  The main deployment scenarios of CloudView are described as follows:

  When Hillstone devices register to the public cloud, the device information, traffic data, threat event, and system logs are uploaded to the cloud, which provides a visual display. Users can monitor the device status information, reports, threat analysis, etc. through the Web or mobile phone APP.



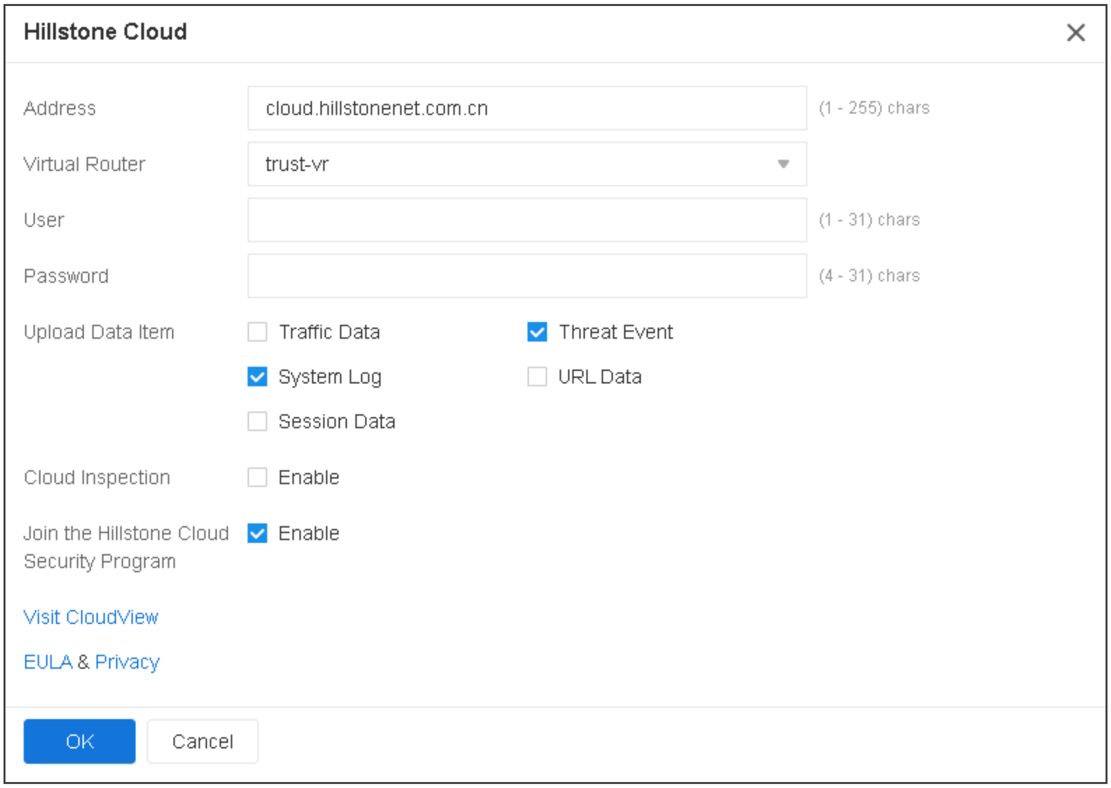
Notes: About CloudView, see CloudView FAQs page.

- Sandbox: The Sandbox function of system uses the cloud sandbox technology. After a suspicous file being uploaded to the Hillstone Cloud, the cloud sandbox will collect behaviors of the file, analyze the collected data, verify the legality of the file, send the analysis result to system and deal with the malicious file according to the actions set by system. For specific configurations of cloud sandbox, refer to **Threat Prevention** > Sandbox.

Connecting to Hillstone Cloud

When using the Cloud, the device needs to connect to the Cloud server.

1. Select **System > Extended Services>Hillstone Cloud**.Click **Edit** button.



Hillstone Cloud

Address	cloud.hillstonenet.com.cn	(1 - 255) chars
Virtual Router	trust-vr	
User		(1 - 31) chars
Password		(4 - 31) chars
Upload Data Item	□ Traffic Data ☑ Threat Event ☑ System Log □ URL Data □ Session Data	
Cloud Inspection	□ Enable	
Join the Hillstone Cloud Security Program	☑ Enable	

2. Select the **Enable** check box of Hillstone Cloud.

3. Enter the URL of the Cloud server. The default configuration is cloud.hillstonenet.com.cn.

4. Enter the username of Cloud. Register the device to this user.

5. Enter the password of the user.

6. **Server Status** displays the Cloud status.

7. Click the arrow to expand the **Upload Data Item** area and select the data option you want to upload to Cloud.

   - Select **Traffic Data** to upload the monitor data.
   - Select **Threat Event** to upload the threat events detected by the Hillstone device.
   - Select **System Log** to upload the event logs.
   - Select **URL Data** to upload the URL data.
   - Select **Session Data** to upload the session data.

8. Select the **Enable** check box in the **Cloud Inspection** section, system can receive and execute inspection command, and upload the collected data to Cloud.

9. Select the **Enable** check box in the **Hillstone Cloud Security Program**. This program will upload the threat prevention data to cloud intelligence server. The uploaded data will be used for internal research to reduce false positives and to achieve better protection of the equipment.

10. Check the box to choose whether to agree to the END USER LICENSE AGREEMENT and HILLSTONE NETWORKS' PRIVACY POLICY. Click **END USER LICENSE AGREEMENT** or **HILLSTONE NETWORKS' PRIVACY POLICY** to read confidentiality and privacy statements, user authorizations and other content.

11. Click **OK**.

Connecting to HSM

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. Using WEB2.0 and RIA (Rich Internet Application) technology, HSM supports visualized interface to centrally manage policies, monitor devices, and generates reports.

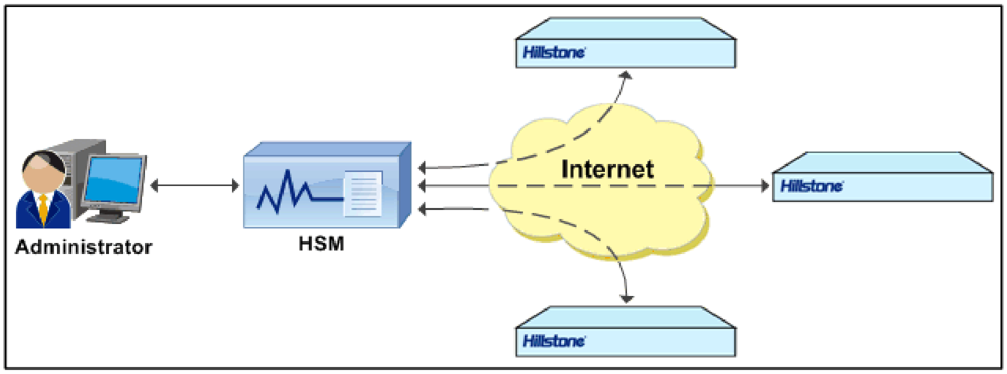
Each firewall system has an HSM module inside it. When the firewall is configured with correct HSM parameters, it can connect to HSM and be managed by HSM.

Notes: For more information about HSM, please refer to HSM User Guide.

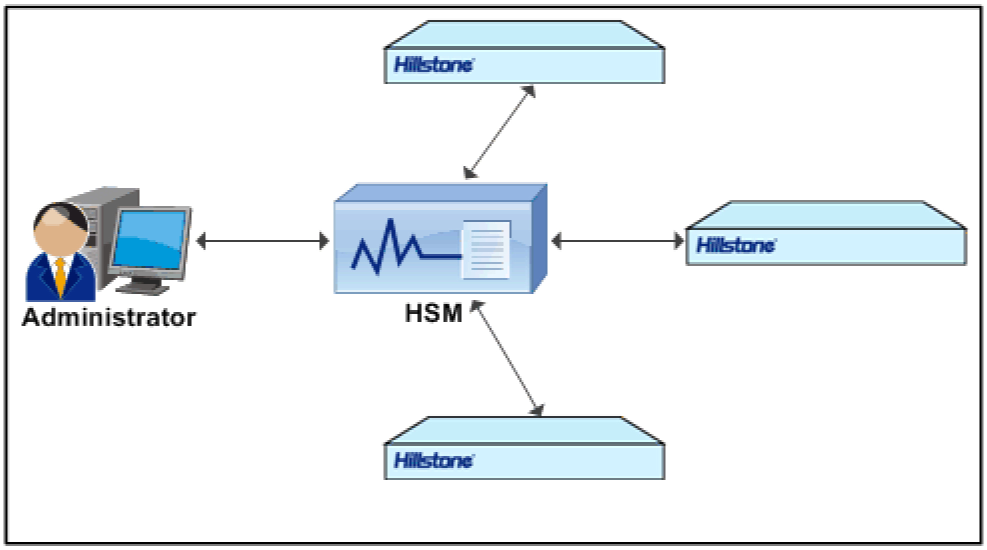
HSM Deployment Scenarios

HSM normally is deployed in one of the two scenarios: installed in public network or in private network:

- Installed in public network: HSM is remotely deployed and connected to managed devices via Internet. When the HSM and managed devices have a accessible route, the HSM can control the devices.



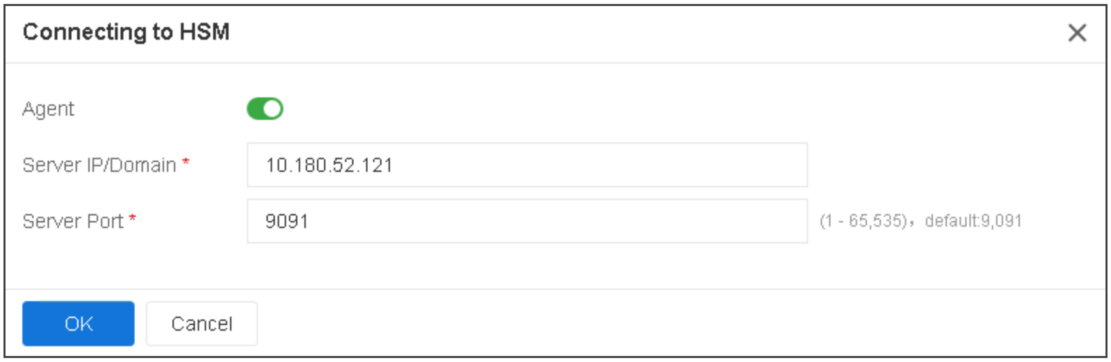
- Installed in private network: In this scenario, HSM and the managed devices are in the same subnet. HSM can manage devices in the private network.



Connecting to HSM

To configure HSM parameters in the firewall, take the following steps:

1. Select **System > Extended Services > Connecting to HSM**.Click **Edit** button.
2. Click **Enable** button of HSM Agent field to enable this feature.



Connecting to HSM

Agent ●

Server IP/Domain * 10.180.52.121

Server Port * 9091 (1 - 65,535)，default:9,091

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. Click **OK**.

> **Notes:** The Syslog Server part shows the HSM server's syslog server and its port.

SNMP

The device is designed with a SNMP Agent, which can receive the operation request from the Network Management System and give the corresponding information of the network and the device.

The device supports SNMPv1 protocol, SNMPv2 protocol and SNMPv3 protocol. SNMPv1 protocol and SNMPv2 protocol use community-based authentication to limit the Network Management System to get device information. SNMPv3 protocol introduces an user-based security module for information security and a view-based access control module for access control.

The device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213 and the Interfaces Group MIB (IF-MIB) using SMIv2 defined in RFC-2233. Besides, the system offers a private MIB, which contains the system information, IPSec VPN information and statistics information of the device. You can use the private MIB by loading it into an SNMP MIB browser on the management host.

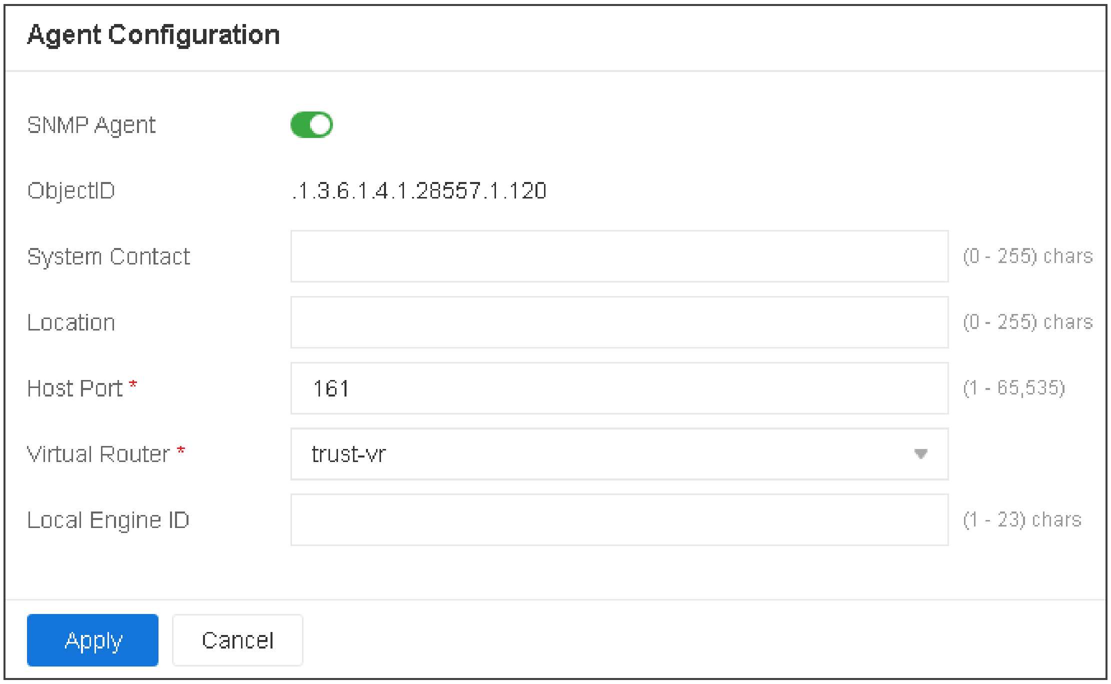
SNMP Agent

The device is designed with a SNMP Agent, which provides network management and monitors the running status of the network and devices by viewing statistics and receiving notification of important system events.

To configure an SNMP Agent, take the following steps:

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

2. Click **Enable** button. In the SNMP Agent page, configure these values.



Agent Configuration

SNMP Agent	●	
ObjectID	.1.3.6.1.4.1.28557.1.120	
System Contact		(0 - 255) chars
Location		(0 - 255) chars
Host Port *	161	(1 - 65,535)
Virtual Router *	trust-vr	
Local Engine ID		(1 - 23) chars

Option	Description
SNMP Agent	Select the **Enable** check box for Service to enable the SNMP Agent function.
ObjectID	The Object ID displays the SNMP object ID of the system. The object ID is specific to an individual system and cannot be modified.
System Contact	Type the SNMP system contact information of the device into the **System Contact** box. System contact is a management variable of the group system in MIB II and it contains the ID and contact of relevant administrator of the managed device. By configuring this parameter, you can save the important information to the device for the possible use in case of emergency.

Option	Description
Location	Type the location of the device into the **Location** box.
Host Port	Type the port number of the managed device into the **Host Port** box.
Virtual Router	Select the VRouter from the **Virtual Router** drop-down list.
Local EngineIID	Type the SNMP engine ID into the **Local EngineID** box.

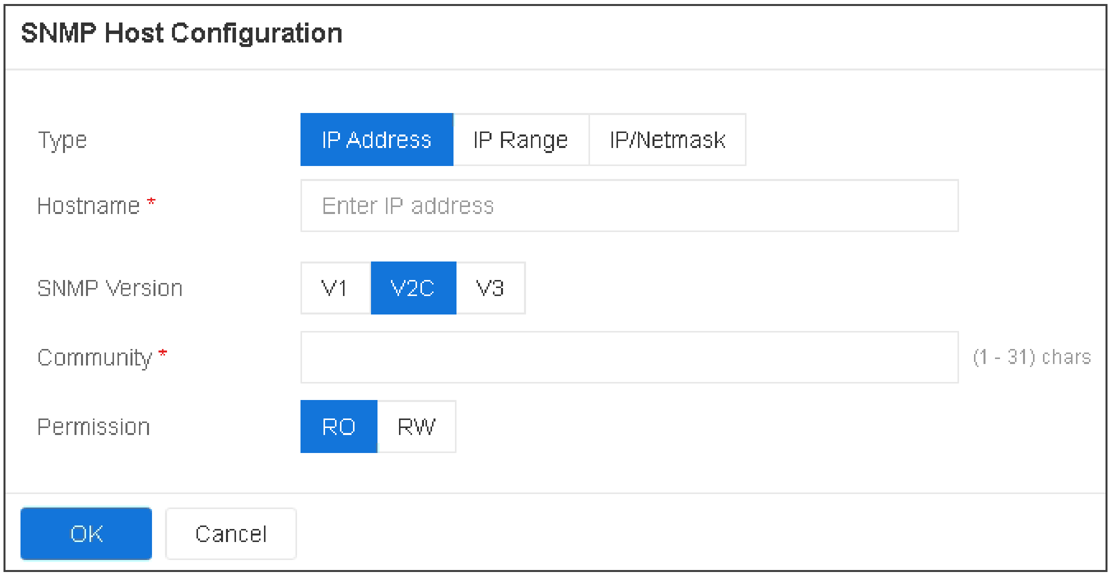
3. Click **Apply**.

Notes: SNMP Engine ID identifies an engine uniquely. SNMP Engine is an important component of the SNMP entity (Network Management System or managed network device) which implements the functions like the reception/sending and verification of SNMP messages, PDU abstraction, encapsulation, and communications with SNMP applications.

SNMP Host

To create an SNMP host, take the following steps:

1. Select **System** > **SNMP** > **SNMP Host**.
2. Click **New**.
3. In the SNMP Agent dialog box, configure these values.



SNMP Host Configuration

Type	[✓ IP Address] IP Range IP/Netmask
Hostname *	Enter IP address
SNMP Version	V1 [✓ V2C] V3
Community *	(1 - 31) chars
Permission	[✓ RO] RW

Option	Description
Type	Select the SNMP host type from the **Type** drop-down list. You can select **IP Address**, **IP Range** or **IP/Netmask**. • IP Address: Type the IP address for SNMP host into **Hostname** box. • IP Range: Type the start IP and end IP into the **Hostname** box respectively. • IP/Netmask: Type the start IP address and Netmask for SNMP host into the **Hostname** box respectively.
SNMP Version	Select the SNMP version from the **SNMP Version** drop-down list.
Community	Type the community for the SNMP host into the **Com-**

Option	Description
	munity box. Community is a password sent in clear text between the manager and the agent. This option is only effective if the SNMP version is V1 or V2C.
Permission	Select the read and write permission for the community from the Permission drop-down list. This option is only effective if the SNMP version is V1 or V2C. • RO: Stand for read-only, the read-only community is only allowed to read the MIB information. • RW: Stand for read-write, the read-write community is allowed to read and modify the MIB information.

4. Click **OK**.

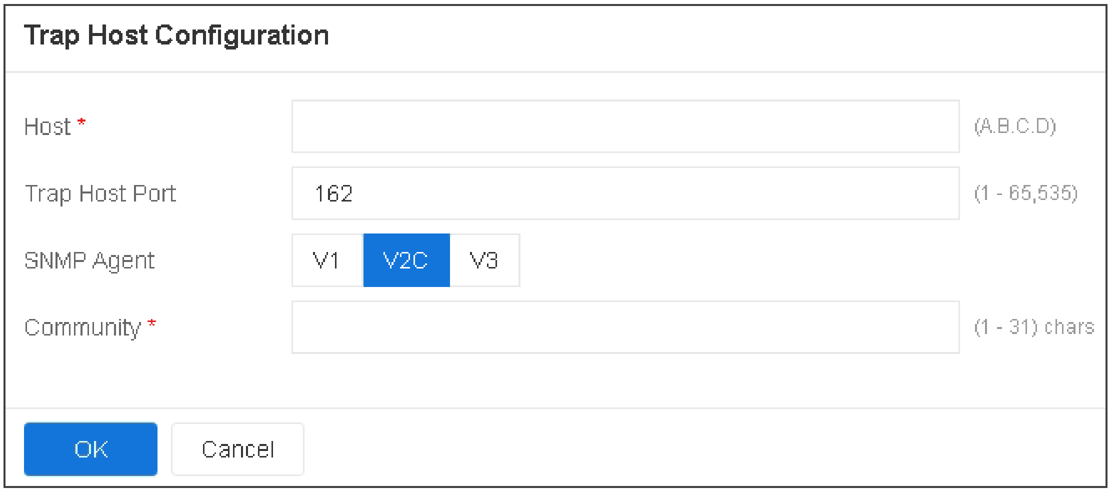
Trap Host

To create a Trap host, take the following steps:

1. Select **System** > **SNMP** > **Trap Host**.

2. Click **New**.

3. In the Trap Host Configuration dialog box, configure these values.



Trap Host Configuration

Host *		(A.B.C.D)
Trap Host Port	162	(1 - 65,535)
SNMP Agent	V1 [✓ V2C] V3	
Community *		(1 - 31) chars

Option	Description
Host	Type the domain name or IP address of the Trap host into the **Host** box.
Trap Host Port	Type the port number for the Trap host into the **Trap Host Port** box.
SNMP Agent	Select the SNMP version from the **SNMP Agent** drop-down list. • V1 or V2C: Type the community for the Trap host into the **Community** box. • V3: Select the V3 user from the **V3 User** drop-down list. Type the Engine ID for the trap host into the **Engine ID** box.

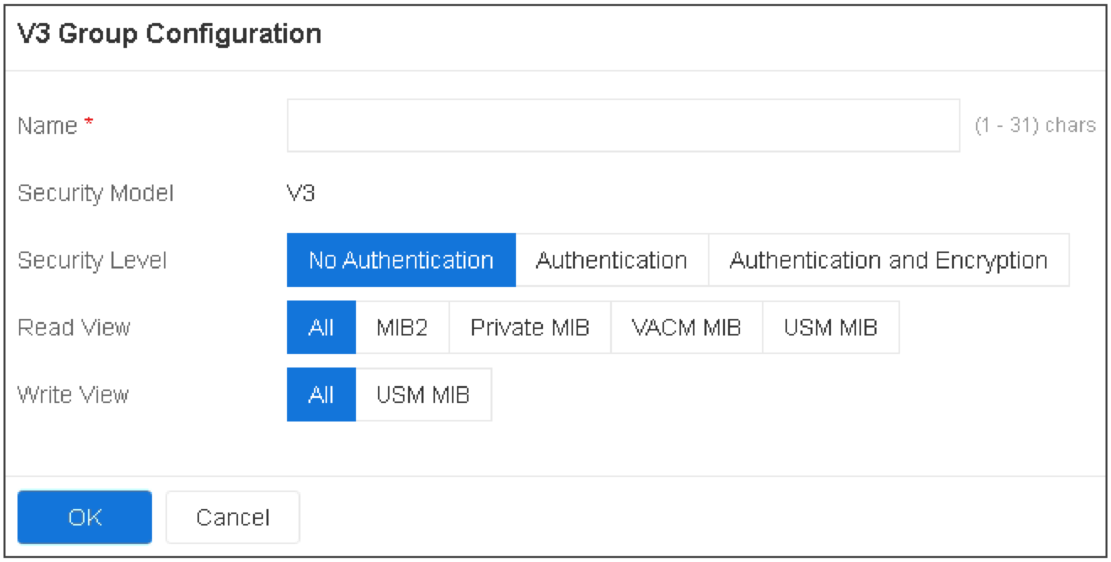
4. Click **OK**.

V3 User Group

SNMPv3 protocol introduces a user-based security module. You need to create an SNMP V3 user group for the SNMP host if the SNMP version is V3.

To create a V3 user group:

1. Select **System** > **SNMP** > **V3 User Group**.
2. Click **New**.
3. In the V3 Group Configuration dialog box, enter values.



V3 Group Configuration

Name * (1 - 31) chars

Security Model V3

Security Level [✓ No Authentication] Authentication Authentication and Encryption

Read View [✓ All] MIB2 Private MIB VACM MIB USM MIB

Write View [✓ All] USM MIB

Option	Description
Name	Type the SNMP V3 user group name into the **Name** box.
Security Model	The Security model option displays the security model for the SNMP V3 user group.
Security Level	Select the security level for the user group from the **Security Level** drop-down list. Security level determines the security mechanism used in processing an SNMP packet. Security levels for V3 user groups include **No Authentication** (no authentication and encryption), **Authentication** (authentication algorithm based on MD5 or SHA) and **Authentication and Encryption** (authentication algorithm based on MD5 or SHA and message encryption based on AES and DES).
Read View	Select the read-only MIB view name for the user group from the **Read View** drop-down list. If this parameter is

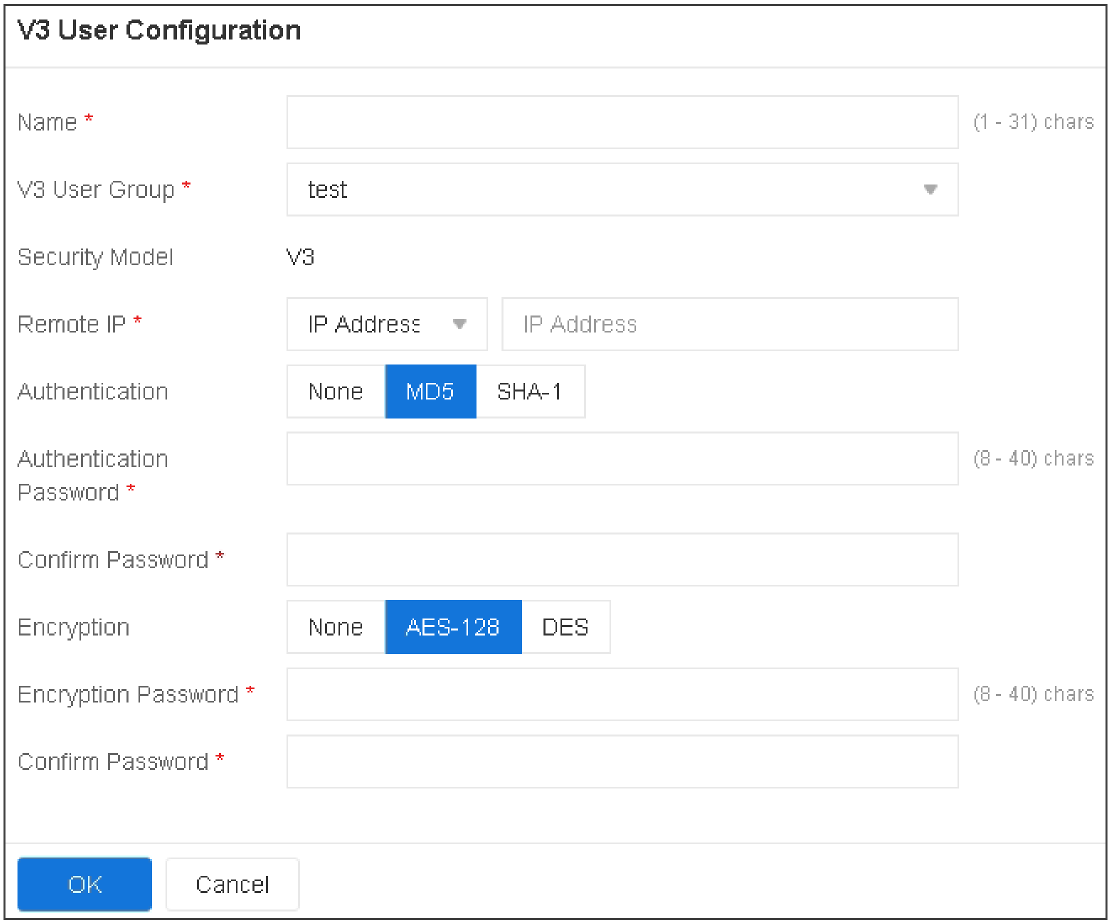
4. Click **OK**.

V3 User

If the selected SNMP version is V3, you need to create an SNMP V3 user group for the SNMP host and then add users to the user group.

To create a user for an existing V3 user group, take the following steps:

1. Select **System** > **SNMP** > **V3 User**.
2. Click **New**.
3. In the V3 User Configuration dialog box, configure these values.



V3 User Configuration

Name * (1 - 31) chars

V3 User Group * test

Security Model V3

Remote IP * IP Address IP Address

Authentication None [✓ MD5] SHA-1

Authentication Password * (8 - 40) chars

Confirm Password *

Encryption None [✓ AES-128] DES

Encryption Password * (8 - 40) chars

Confirm Password *

Option	Description
Name	Type the SNMP V3 user name into the **Name** box.
V3 User Group	Select an existing user group for the user from the Group drop-down list.
Security Model	The Security model option displays the security model for the SNMP V3 user.
Remote IP	Type the IP address of the remote management host into the **Remote IP** box.
Authentication	Select the authentication protocol from the **Authentic-**

4. Click **OK**.

SNMP Server

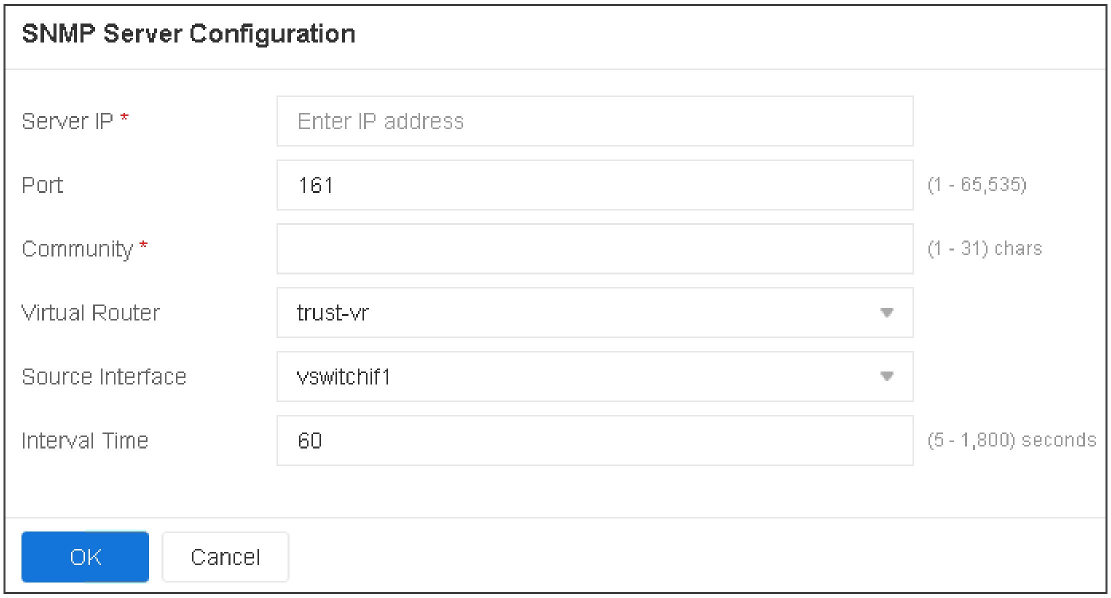
You can configure the SNMP server to get the ARP information through the SNMP protocol.

Creating an SNMP Server

To create an SNMP server, take the following steps:

1. Select **System** > **SNMP server**.

2. Click **New**.



SNMP Server Configuration

Server IP *	Enter IP address	
Port	161	(1 - 65,535)
Community *		(1 - 31) chars
Virtual Router	trust-vr	
Source Interface	vswitchif1	
Interval Time	60	(5 - 1,800) seconds

In the SNMP Server Configuration dialog box, configure these values

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.

Option	Description
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 from the drop-down list for receiving ARP information on the SNMP server.
Interval Time	Type the the interval into the **Interval Time** box for receiving ARP information on the SNMP server. The value range is 5 to 1800 seconds, the default value is 60 seconds.

3. Click **OK**.

Upgrading System

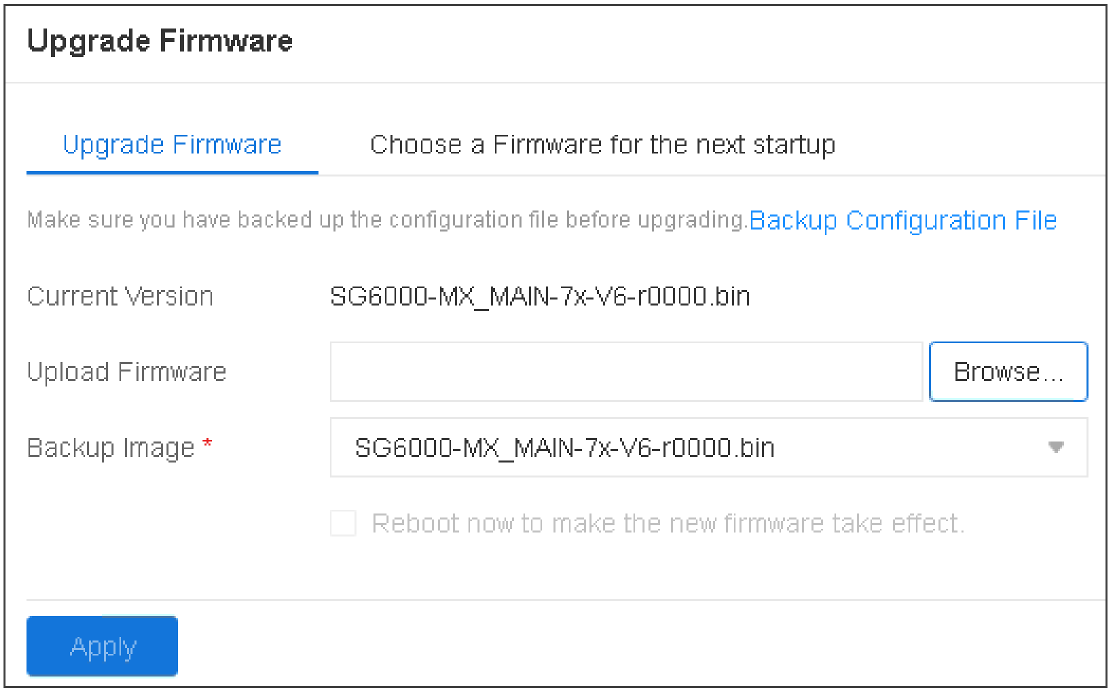
The firmware upgrade wizard helps you:

- Upgrade system to a new version or roll back system to a previous version.
- Update the Signature Database.
- Update the Trusted Root Certificate Database.

Upgrading Firmware

To upgrade firmware, take the following steps:

1. Select **System** > **Upgrade Management** > **Upgrade Firmware**.
2. In the **Upgrade Firmware** tab, configure the following.



Upgrade Firmware

Make sure you have backed up the configuration file before upgrading.Backup Configuration File

Current Version SG6000-MX_MAIN-7x-V6-r0000.bin

Upload Firmware

Backup Image * SG6000-MX_MAIN-7x-V6-r0000.bin

□ Reboot now to make the new firmware take effect.

Upgrade Firmware	
Backup Con-	Make sure you have backed up the configuration file

Upgrade Firmware	
figuration File	before upgrading. Click **Backup Configuration File** to backup the current fireware file and the system will automatically redirect the Configuration File Management page after the backup.
Current Version	The current firmware version.
Upload Firmware	Click **Browse** to select a firmware file from your local disk.
Backup Image	The backup firmware version.
Reboot	Select the **Reboot now to make the new firmware take effect** check box and click **Apply** to reboot system and make the firmware take effect. If you click **Apply** without selecting the check box, the firmware will take effect after the next startup.
Choose a Firmware for the next startup	
Select the firmware that will take effect for the next startup.	Select the firmware that will take effect for the next startup.
Reboot	Select the **Reboot now to make the new firmware take effect** check box and click **Apply** to reboot system and

Upgrade Firmware	
	make the firmware take effect. If you click **Apply** without selecting the check box, the firmware will take effect after the next startup.

Updating Signature Database

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.
Remote Update	Application signature database, URL signature database, Sandbox Whitelist Database, Antivirus signature database, IPS signature database , Share Access signature database, IP reputation database , Botnet Prevention signature database. • Update Server: By default the system updates the signature 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 according to your need. In **Update Server**, specify the server IP or domain name and Virtual

Option	Description
	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. Mitigation rule database, Abnormal behavior mode database or Malware behavior mode database. - Update Server: By default the system updates the signature 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 according to your need. In **Update Server**,

Option	Description
	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	Click **Browse** and select the signature file in your local PC, and then click **Upload**.

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 virtual router. • 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.

Option	Description
	- 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.

License

Licenses are used to authorize the users' features, authorize the users' services, or extend the performance. If you do not buy and install the corresponding license, the features, services, and performance which is based on the license will not be used or cannot be achieved.

License classes and rules.

Platform License	Description	Valid Time
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are not effective. The device have been pre-installed platform trial license for 15 days in the factory.	You cannot modify the existing configuration when License expires. The system will restore to factory defaults when the device reboot.
Platform	You can install the platform license after the device formal sale. The license provide basic firewall and VPN function.	System cannot upgrade the OS version when the license expires, but the system could still work normally.
Function License	**Description**	**Valid Time**
VSYS	Authorizing the available number of VSYS.	Permanent
SCVPN	Authorizing the maximum number of SSL VPN access. Through installing multiple SCVPN	Permanent

	licenses, you can add the maximum number of SSL VPN access.	
QoS	Enable QoS function.	System cannot upgrade the QoS function and cannot provide the maintenance service when License expired.
Cloud sandbox License	Providing Cloud sandbox function and white list update, authorizing the number of suspicious files uploaded per day. Including 4 licenses: Cloud sandbox-200, Cloud sandbox-300, Cloud sandbox-500 and Cloud sandbox-1000. The number of files allowed to upload per day is different for different licenses.	The valid time including 1 year, 2 years and 3 years. System cannot analyze the collected data and cannot update the white list when the license expires. The Cloud sandbox protection function can only be used according to the local database cache results. If you restart the device, the function cannot be used.
Twin-mode License	Providing the twin-mode function. The related parameters of the twin-mode function can be displayed and configured.	System cannot upgrade the twin-mode function and cannot provide the

		maintenance service when License expired.
Service License	**Description**	**Valid Time**
AntiVirus	Providing antivirus function and antivirus signature database update.	System cannot update the antiviru signature database when the license expires, but the antivirus function could still be used normally
URL DB	Providing URL database and URL signature database update.	System cannot provide the search URL database online function when the license expires, but the user-defined URL and URL filtering function can be used normally.
IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when the license expires, but the IPS function could still be used normally.

APP signature	APP signature license is issued with platform license, you do not need to apply alone. The valid time of license is same as platform license.	System cannot update the APP signature database when the license expires, but the included functions and rules could still be used normally.
Threat Prevention	A package of features, including AntiVirus, IPS, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.
Botnet Prevention	Providing Botnet Prevention function and Botnet Prevention database update.	System cannot update all signature databases when license expires. But the functions included and rules could be used normally.
IoT monitor&control	Providing the IoT policy function.	Permanent.
IoT monitor&control trail	After the installation of IoT monitor&control trail license, you will get the same IoT policy function as system with IoT mon-	The IoT policy function cannot be used when the license expires. If

	itor&control license. But the duration will be shorter.	you restart the device, the existing IoT policy configurations will not be lost, but won't take effect.
Expansion and Enhancement License	**Description**	**Valid Time**
AEL	Advance the maximum value of concurrent sessions and performance.	Permanent

From the version 5.5R5, the CloudEdge license has been upgraded to the latest version, with a different licensing mechanism. After the installation of the new platform license, the SN number of the device will be changed to a virtual SN (vSN for short). If you want to continue to obtain function or sub licenses, they can be applied through the vSN number. For the new license does not depend on the SN number of the original system after the re-installation of system, the new license that was originally applied for can still be effective. At the same time, Hillstone provides LMS (license management system) to verify and manage licenses, which can ensure the security of licenses.

CloudEdge is pre-installed with a free default license without application. You can apply for the platform license (the old version of the platform license) through the SN number or directly apply for the new version of the license. Old version platform license is divided into base license and trial license. The new platform license is divided into base license and sub license.

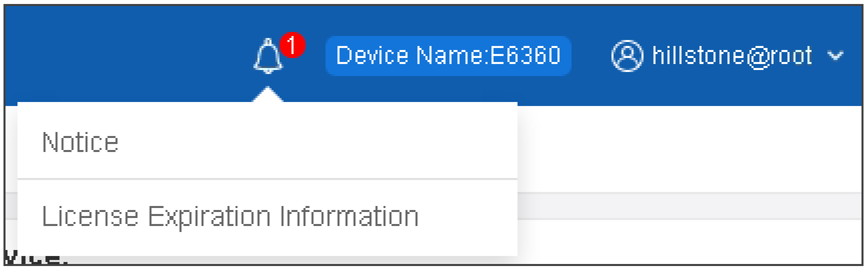
Viewing License List

Select **System** > **License** to enter the License List page. All licenses the system supports will be displayed in this page, including the authorized licenses and unauthorized licenses.

If there is license that is about to expire (the remaining valid period is within 30 days) or has expired:

- When you log into the device, the **License Expiration Information** dialog box will pop up, which prompts for licenses that are about to expire or have expired. Check the **Don't remind me again** checkbox so that the dialog box will never prompt again when you login. Click the **Update Now** button to jump to the License List page.

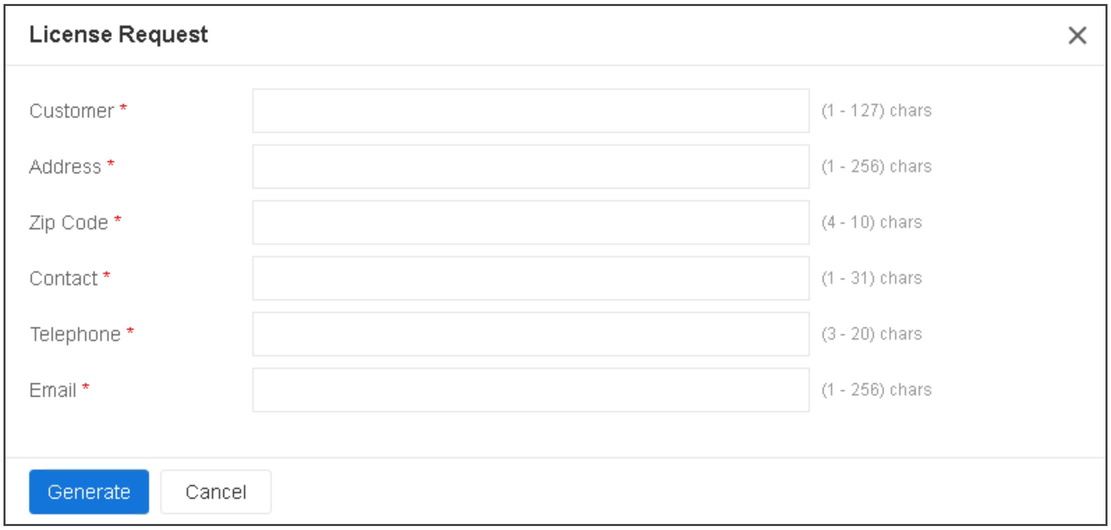
- The notification icon with the number of notifications is displayed in the upper-right corner. Hover your mouse over the icon, and click **Details** after the License Expiration Information, the **License Expiration Information** dialog will pop up.



Applying for a License

Before you apply for a license, you have to generate a license request first.

1. Click **Apply For**. Under License Request, input user information. All fields are required.



License Request

Customer *	(1 - 127) chars
Address *	(1 - 256) chars
Zip Code *	(4 - 10) chars
Contact *	(1 - 31) chars
Telephone *	(3 - 20) chars
Email *	(1 - 256) chars

2. Click **Generate**, and then appears a bunch of code.

3. Send the code to your sales contact. The sales person will issue the license and send the code back to you.

Installing a License

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. Under **Import License** page, configure options below.

Option	Description
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**, and click the **Option** tab.
5. Click **Reboot**, and select **Yes** in the prompt.
6. System will reboot. When it starts again, installed license(s) will take effect.

Notes: When you verify your license through public LMS, make sure that the interface connected to the public server is in the trust-vr zone and that you can access the Internet through the trust-vr zone.

Mail Server

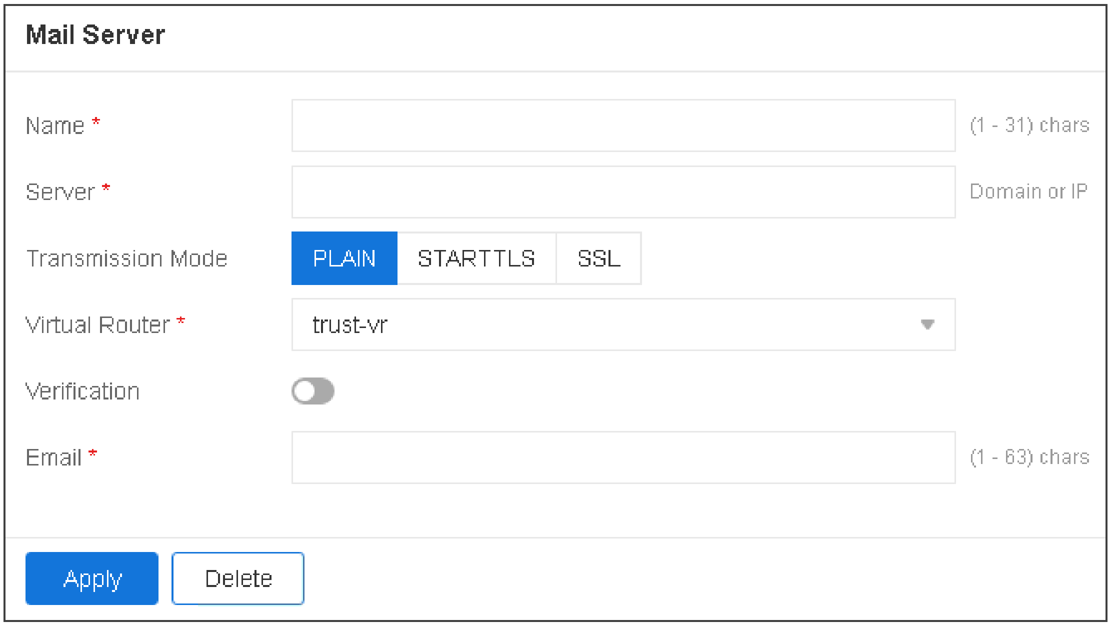
By configuring the mail server in the Mail Server page, the system can send the log messages, report or alarm information to the specified email address.

Creating a Mail Server

To create a mail server, take the following steps:

1. Select **System** > **Mail Server**.

2. In the Mail Server Configuration page, configure these values.



Mail Server

Name *		(1 - 31) chars
Server *		Domain or IP
Transmission Mode	[✓ PLAIN] STARTTLS SSL	
Virtual Router *	trust-vr	
Verification	○	
Email *		(1 - 63) chars

Option	Description
Name	Type a name for the mail server into the box.
Server	Type Domain name or IP address for the mail server into the box.
Transmission Mode	Select the transmission mode for the email. • PLAIN: Specifies that the mail is sent in plain text and is not encrypted. This mode is the default transmission mode. • STARTTLS: STARTTLS is an extension to the plain text communication protocol that upgrades plain text connections to encrypted connections. Specified in this mode, the mail will be transmitted using encrypted mode.

3. Click **Apply**.

Chapter 15

System Management

SMS Parameters

This Section contains the following contents:

SMS Modem

An external GSM modem device is required for sending SMS messages. First, you need to prepare a mobile phone SIM card and a GSM SMS Modem . Insert the SIM card into your modem and then, connect the modem and the firewall using a USB cable.

The following one models of SMS modem is recommended:

Model	Type	Chip	Interface
GSM MODEM M1206B	GSM	WAVECOM	USB interface

System will show the modem connection status: correctly connected, not exist or no signal.

Configuring SMS Parameters

You can define the maximum SMS message number in one hour or in one day. If the messages exceed the maximum number, system will not make the modem to send messages, but it will keep a log for this behavior.

Option	Description
Maximum messages per hour	Defines the maximum message number the modem can send in one hour.
Maximum messages per day	Defines the maximum messages number the modem can send in one day.

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**.
2. Enter a mobile phone number in the text box.
3. 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.

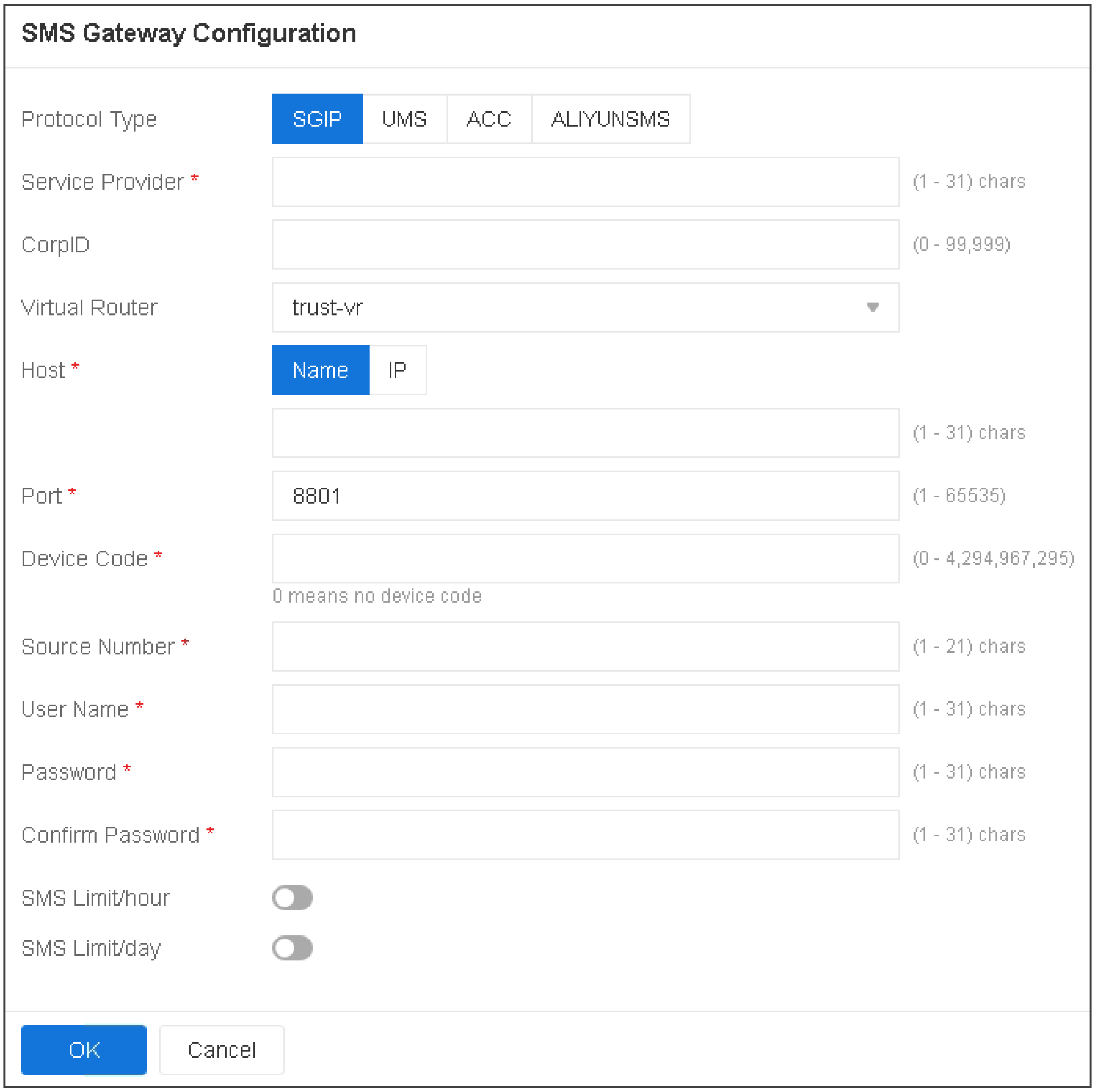
SMS Gateway

Configuring SMS Gateway

To configure the SMS gateway, take the following steps:

1. Select **System** > **SMS Parameters** >**SMS Gateway**.

2. Click **New**.



SMS Gateway Configuration

Protocol Type: [✓ SGIP] UMS ACC ALIYUNSMS

Service Provider *: (1 - 31) chars

CorpID: (0 - 99,999)

Virtual Router: trust-vr

Host *: [✓ Name] IP

(1 - 31) chars

Port *: 8801 (1 - 65535)

Device Code *: (0 - 4,294,967,295)

0 means no device code

Source Number *: (1 - 21) chars

User Name *: (1 - 31) chars

Password *: (1 - 31) chars

Confirm Password *: (1 - 31) chars

SMS Limit/hour: ○

SMS Limit/day: ○

OK Cancel

In the SMS Gateway Configuration dialog box, configure the following options.

Option	Description
Protocol Type	Specifies the protocol of SMS gateway. SGIP indicates the SGIP protocol of Chinaunicom. UMS indic-

Option	Description
	ates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud.
Service Provider	Specifies the service provider name. The value range is 1 to 31.
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" or "ALIYUNSMS", users can specify the protocol type. The default protocol type is HTTP.
Virtual Router	Specifies the VRouter which gateway belongs to. The system supports multi-VR, and the default VR is trust-vr.
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 "UMS", the default port number is 9600.
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

Option	Description
	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. The range is 1 to 31.
Password	Specifies the password for the user. The range is 1 to 31.
Confirm Password	Re-type the password into the **Confirm Password** box to confirm.
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

Option	Description
	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.

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 **SMS Test** dialog box, enter a mobile phone number in the text box.
4. 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.

VSYS (Virtual System)

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

VSYS (Virtual System) is logically divides the physical firewall into several virtual firewalls. Each virtual firewall can work independently as a physical device with its own system resources, and it provides most firewall features. A VSYS is separated from other VSYS, and by default, they cannot directly communicate with each other.

VSYS has the following characteristics:

- Each VSYS has its own administrator;
- Each VSYS has an its own virtual router, zone, address book and service book;
- Each VSYS can have its own physical or logical interfaces;
- Each VSYS has its own security policies.

Notes: The maximum VSYS number is determined by the platform capacity and license. You can expand VSYS maximum number by purchasing addition licenses.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

System contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device. When creating or deleting non-root VSYSs, you must follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you must be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see "Device Management" on Page 1169.
- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
    - A non-root VSYS administrator named admin. The password is vsys_name-admin.
    - A VRouter named vsys_name-vr.
    - A L3 zone named vsys_name-trust.

  For example, when creating the non-root VSYS named vsys1, the following objects will be created:

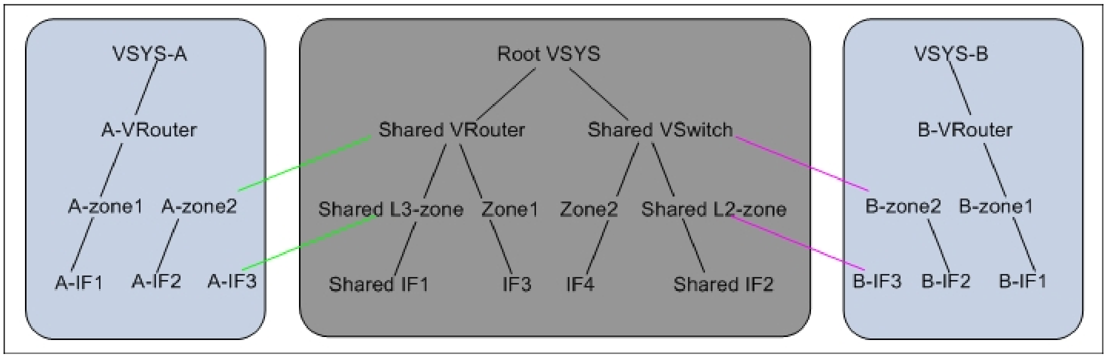
    - The RXW administrator named admin with the password vsys1-admin.
    - The default VRouter named vsys1-vr.
    - The L3 zone named vsys1-trust and it is bound to vsys1-vr automatically.
- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating l2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the l2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

VRouter, VSwitch, Zone and Interface

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

- **Dedicated object**: A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object**: A shared object can be shared by multiple VSYSs. A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

The figure below shows the reference relationship among dedicated and shared VRouter, VSwitch, zone, and interface.



As shown in the figure above, there are three VSYSs in StoneOS: Root VSYS, VSYS-A, and VSYS B.

Root VSYS contains shared objects (including Shared VRouter, Shared VSwitch, Shared L3-zone, Shared L2-zone, Shared IF1, and Shared IF2) and dedicated objects.

VSYS-A and VSYS-B only contain dedicated objects. The dedicated objects VSYS-A and VSYS-B can reference the shared objects in Root VSYS. For example, A-zone2 in VSYS-A is bound to the shared object Shared VRouter in Root VSYS, and B-IF3 in VSYS-B is bound to the shared object Shared L2-zone in Root VSYS.

Shared VRouter

A shared VRouter contains the shared and dedicated L3 zones of the root VSYS. Bind a L3 zone to a shared VRouter and configure this L3 zone to have the shared property. Then this zone becomes a shared zone.

Shared VSwitch

A shared VSwitch contains the shared and dedicated L2 zones of the root VSYS. Bind a L2 zone to a shared VSwitch and configure this L2 zone to have the shared property. Then this zone becomes a shared zone.

Shared Zone

The shared zones consist of L2 shared zones and L3 shared zones. After binding the L2 zone with the shared property to a shared VSwitch, it becomes a shared L2 zone; after binding the L3 zone with shared property to a shared VRouter, it becomes a shared L3 zone. A shared zone can contain interfaces in both root VSYS and non-root VSYS. All function zones cannot be shared.

Shared Interface

After binding an interface in the root VSYS to a shared zone, it becomes a shared interface automatically.

Interface Configuration

Only RXW administrator in the root VSYS can create or delete interfaces. Configurations to an interface and its sub-interfaces must be performed in the same VSYS.

Notes: Only adminitrator has the authority ot delete or create interfaces. If you are about to delete an interface and its-subinterfaces, you have to do it under the same VSYS.

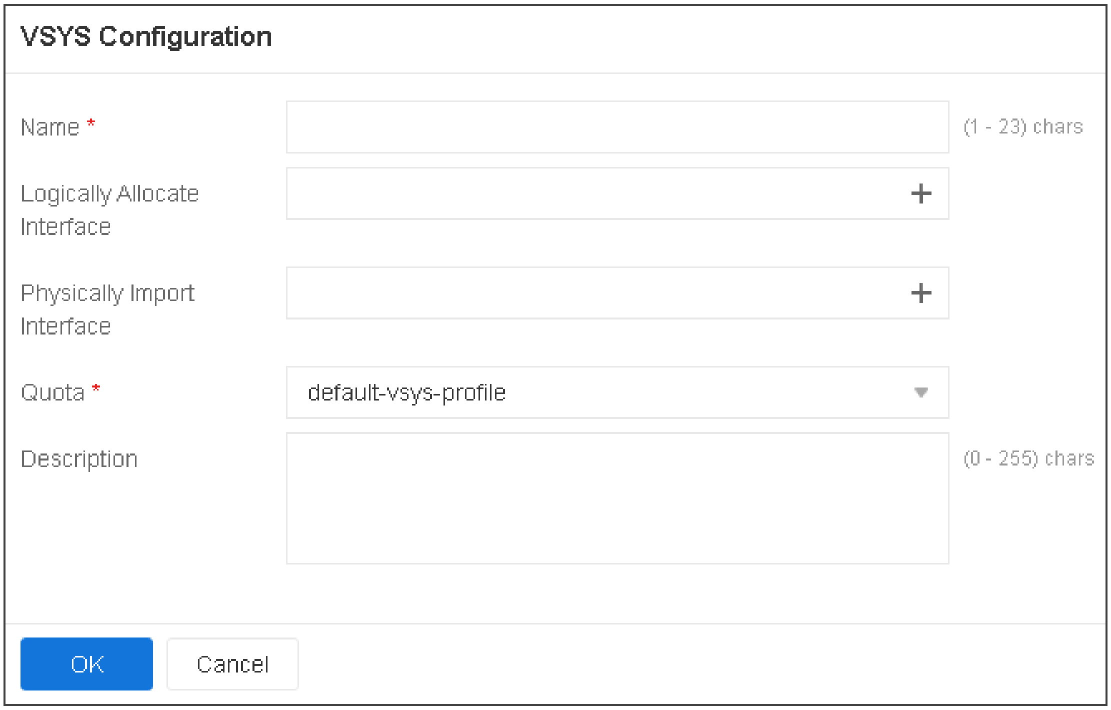
Creating Non-root VSYS

To create a new non-root VSYS, take the following steps:

1. Select **System** > **VSYS** > **VSYS**.

2. Click **New** to add a non-root VSYS.

3. In the prompt, configure these values.



VSYS Configuration

Name * (1 - 23) chars

Logically Allocate Interface +

Physically Import Interface +

Quota * default-vsys-profile

Description (0 - 255) chars

OK Cancel

Option	Description
Name	Enter a name for the non-root VSYS.
Description	Enter the description information for the non-root VSYS.
Interface Binding	Select a physical or a logical interface. In VSYS, a physical interface can have its sub-interfaces, but logical interfaces cannot.

Option	Description
	- Physically Import: Select the interface you want, and click **Physically Import** to add it to the right pane. - Logically Allocate: Select the interface you want, and click **Logically Allocate** to add it to the right pane. - Release: Select the added interface(s), and click **Release** to delete it.
Quota	Select an existing quota.

4. Click **OK** to save configuration. The new VSYS will be seen in the VSYS list.

Configuring Dedicated and Shared Objects for Non-root VSYS

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object. The dedicated object and shared object have the following characters:

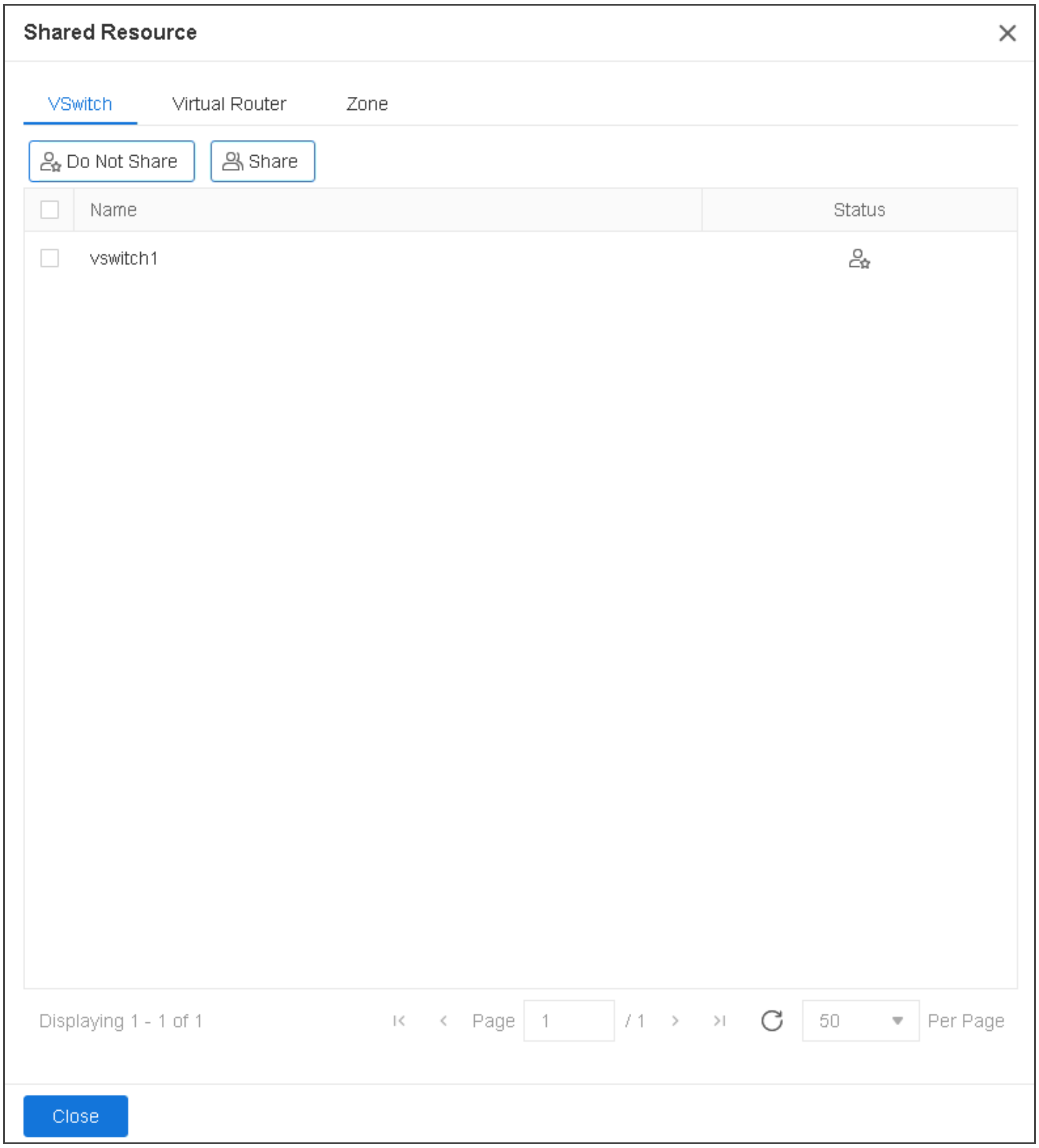
- **Dedicated object**: A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object**: A shared object can be shared by multiple VSYSs. A shared object can only belong to the root VSYS and can only be configured in the root VSYS. A non-root VSYS can reference the shared object, but cannot configure them. The name of the shared object must be unique in the whole system.

To configure VSYS shared object, take the following steps:

1. Select **System > VSYS > VSYS**.

2. Click **Share Resource**.

3. In the prompt, configure these values for VSwitch, VRouter and Zone.



Option	Description
VSwitch	In the VSwtich tab, select a Vswitch and click **Share** to

Option	Description
	set it as a shared object; to make a VSwitch as a dedicated object, click **Do Not Share**.
Virtual Router	In the Virtual Router tab, select a Vswitch and click **Share** to set it as a shared object; to make a Virtual Router as a dedicated object, click **Do Not Share**.
Zone	In the Zone tab, select a Zone and click **Share** to set it as a shared object; to make a Zone as a dedicated object, click **Do Not Share**.

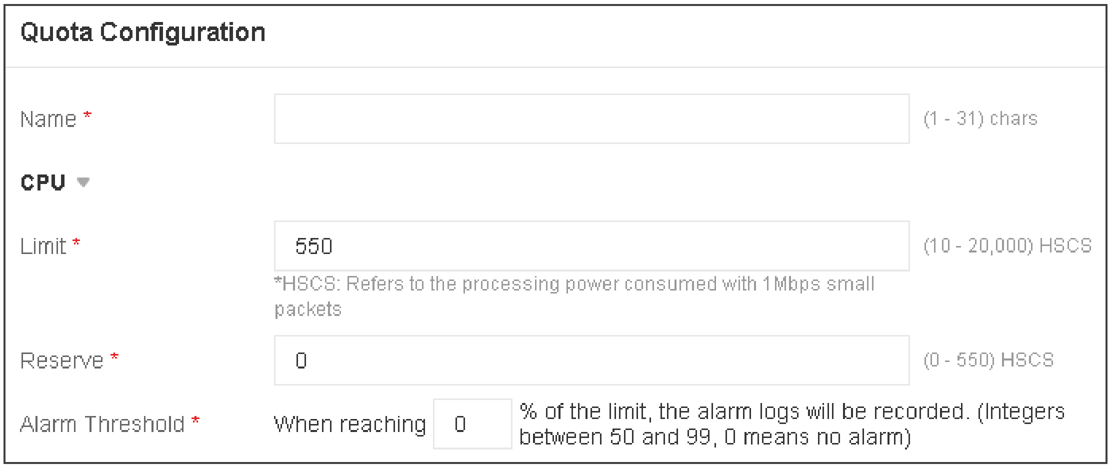
4. Click **Close** to exit.

Configuring VSYS Quota

VSYSs work independently in functions but share system resources including concurrent sessions, zone number, policy rule number, SNAT rule number, DNAT rule number, session limit rules number, memory buffer, URL resources, IPS resources, AV resources and PTF resources. You can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile. Reserved quota refers to the resource number reserved for the VSYS; maximum quota refers to the maximum resource number available to the VSYS. The root administrator have the permission to create VSYS quota. The total for each resource of all VSYSs cannot exceed the system capacity.

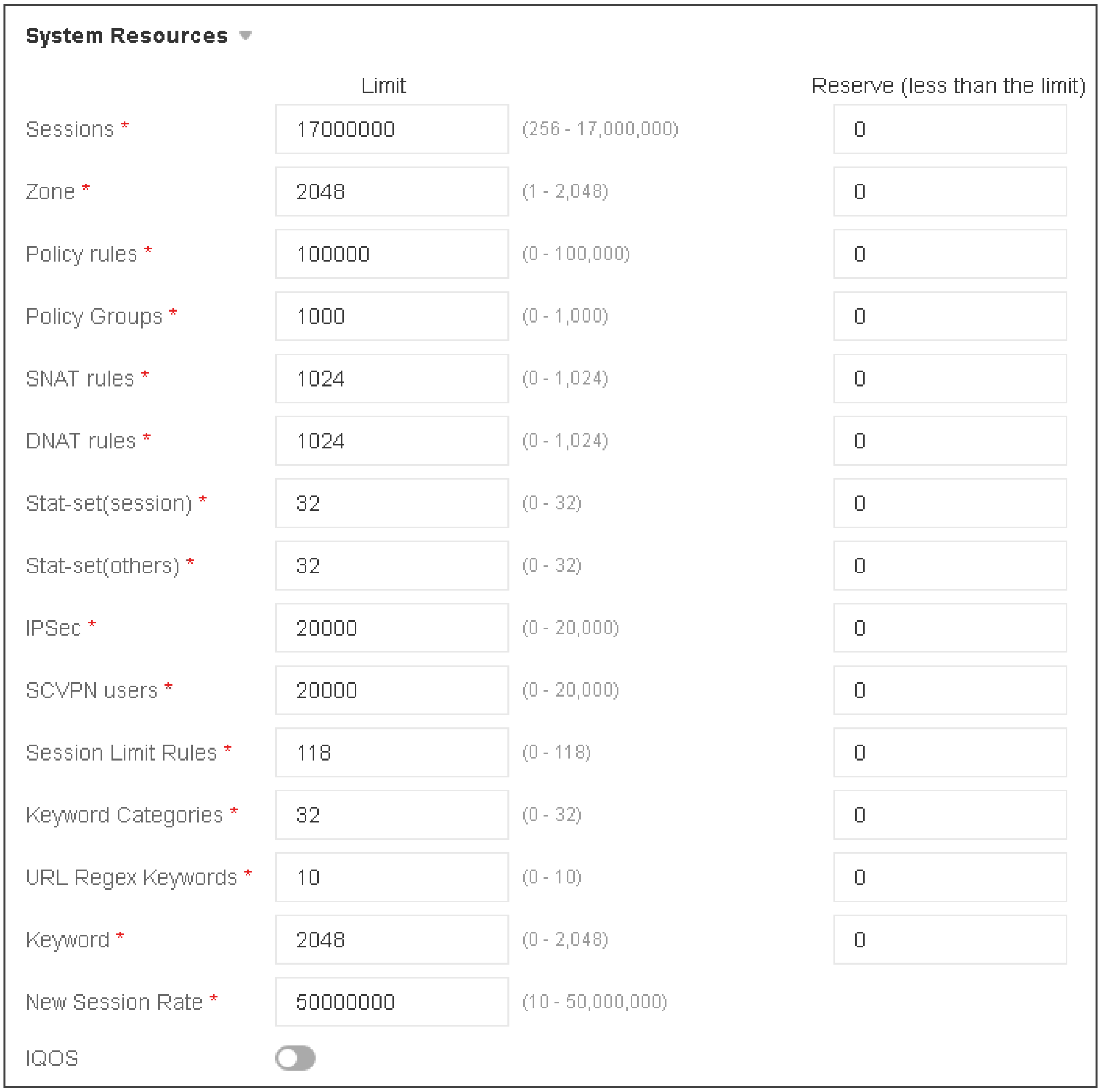
To define a quota for VSYS, take the following steps:

1. Select **System > VSYS > Quota**.
2. Click **New** .
3. **In the prompt, configure these values.**



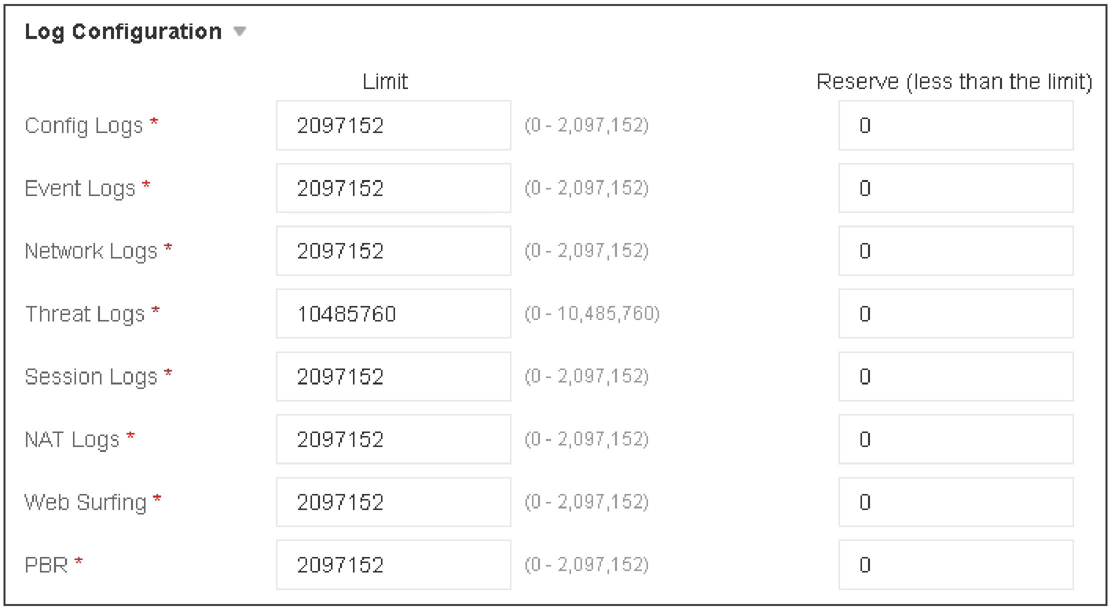
Quota Configuration

Name *		(1 - 31) chars
CPU ▾		
Limit *	550 *HSCS: Refers to the processing power consumed with 1Mbps small packets	(10 - 20,000) HSCS
Reserve *	0	(0 - 550) HSCS
Alarm Threshold *	When reaching 0 % of the limit, the alarm logs will be recorded. (Integers between 50 and 99, 0 means no alarm)	



System Resources ▾

	Limit		Reserve (less than the limit)
Sessions *	17000000	(256 - 17,000,000)	0
Zone *	2048	(1 - 2,048)	0
Policy rules *	100000	(0 - 100,000)	0
Policy Groups *	1000	(0 - 1,000)	0
SNAT rules *	1024	(0 - 1,024)	0
DNAT rules *	1024	(0 - 1,024)	0
Stat-set(session) *	32	(0 - 32)	0
Stat-set(others) *	32	(0 - 32)	0
IPSec *	20000	(0 - 20,000)	0
SCVPN users *	20000	(0 - 20,000)	0
Session Limit Rules *	118	(0 - 118)	0
Keyword Categories *	32	(0 - 32)	0
URL Regex Keywords *	10	(0 - 10)	0
Keyword *	2048	(0 - 2,048)	0
New Session Rate *	50000000	(10 - 50,000,000)	
IQOS	○		



Log Configuration

	Limit		Reserve (less than the limit)
Config Logs *	2097152	(0 - 2,097,152)	0
Event Logs *	2097152	(0 - 2,097,152)	0
Network Logs *	2097152	(0 - 2,097,152)	0
Threat Logs *	10485760	(0 - 10,485,760)	0
Session Logs *	2097152	(0 - 2,097,152)	0
NAT Logs *	2097152	(0 - 2,097,152)	0
Web Surfing *	2097152	(0 - 2,097,152)	0
PBR *	2097152	(0 - 2,097,152)	0

Option	Description
Basic Configuration	
Name	Enter a name for the new quota.
CPU	Specify values for parameters of CPU. • Limit: Specifies the maximum performance limit for processing 1 Mbps packets. • Reserve: A dedicated reservered value for CPU in this VSYS. The value range is 0 to 20000. • Alarm Threshold: Specifies a percentage value for alarms. When the CPU usage reaches this value, the system will generate alarm logs.
System Resources	
System	Specify the maximum quota and reserved quota of system

Option	Description
Basic Configuration	
Resources	resources. • Sessions: Specifies the maximum and reserved number for sessions in the VSYS. • Zone: Specifies the maximum and reserved number for zones in the VSYS. • Policy rules: Specifies the maximum and reserved number for policy rules in the VSYS. • Policy Groups: Specifies the maximum and reserved number for policy groups in the VSYS. • SNAT rules: Specifies the maximum and reserved number for SNAT rules in the VSYS. • DNAT rules: Specifies the maximum and reserved number for SNAT rules in the VSYS. • Stat-set (session): Specifies the maximum and reserved number for sessions of a staticstic set in the VSYS. • Stat-set (others): Specifies the maximum and reserved number for other items than sessions of a staticstic set in the VSYS. • IPSec: Specifies the maximum and reserved num-

Option	Description
Basic Configuration	
	ber for IPSec tunnels in the VSYS. • SCVPN users: Specifies the maximum and reserved number for SCVPN users. • Session Limit Rules: Specifies the maximum and reserved number for session limit rules in the VSYS. • Keyword Categories: Specifies the maximum and reserved number for keyword categories in the VSYS. • URL Regex Keywords: Specifies the maximum and reserved number for regular expression keywords in a URL category in the VSYS. • Keyword: Specifies the maximum and reserved number for simple keywords in a URL category in the VSYS. • New Session Rate: Specifies the maximum number for the new session rate in the VSYS. • IQoS: Select the **Enable** check box to enable the QoS function and specifies the maximum and reserved number for root-pipe in the VSYS.
Protection	

Option	Description
Basic Configuration	
AV Resources	Specify the maximum quota and reserved quota of AV resources. • AV: Select the **Enable** check box to enable the Anti-Virus function. • AV Profile: Specifies the maximum and reserved number for AV profiles in a VSYS. The range of maximum quota varies from 0 to 32. The reserved quota should not exceed the maximum quota. The default value of maximum quota is 32 and the default value of reserved quota is 0.
URL Resources	Specify the maximum quota and reserved quota of URL resources. • URL: Select the **Enable** check box to enable the URL filter function. • URL Profiles: Specifies the maximum and reserved number for URL filter profiles in a VSYS. • URL Categories: Specifies the maximum and reserved number for user-defined URL categories in a VSYS. • URL: Specifies the maximum and reserved number for URLs in a VSYS.

Option	Description
Basic Configuration	
IPS Resources	Specify the maximum quota and reserved quota of IPS resources. • IPS: Select the **Enable** check box to enable the IPS function. • IPS Profiles: Specifies the maximum and reserved number for IPS profiles in a VSYS. You can create one IPS Profile at most in non-root VSYS, i.e., the range of maximum quota varies from 0 to 1. The default value of maximum quota and reserved quota is 0, which means only predefined IPS Profiles can be used in non-root VSYS.
Perimeter Traffic Filtering Resources	Enable or disable perimeter traffic filtering and configure user-defined black/white list resources in a VSYS Profile. • Perimeter Traffic Filtering: Select the **Enable** check box to enable the perimeter traffic filtering function. • User-Defined Black/White List: Specifies the maximum quota and reserved quota of user-defined black list and white list. The range of maximum quota varies from 0 to 1000. The reserved quota should not exceed the maximum quota. The

Option	Description
Basic Configuration	
	default value of maximum quota is 1000 and the default value of reserved quota is 0.
Log Configuration	
Log Configuration	Specify the maximum quota and reserved quota of memory buffer for each type of log in a VSYS. The reserved quota should not exceed the maximum quota. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer. • Config Logs: Specify the maximum and reserved value of buffer for configuration logs in a VSYS. • Event Logs: Specify the maximum and reserved value of buffer for event logs in a VSYS. • Network Logs: Specify the maximum and reserved value of buffer for network logs in a VSYS. • Threat Logs: Specify the maximum and reserved value of buffer for threat logs in a VSYS. • Session Logs: Specify the maximum and reserved value of buffer for session logs in a VSYS. • NAT Logs: Specify the maximum and reserved value of buffer for NAT logs in a VSYS.

Option	Description
Basic Configuration	
	- Web Surfing: Specify the maximum and reserved value of buffer for websurf logs in a VSYS. - PBR: Surfing: Specify the maximum and reserved value of buffer for PBR logs in a VSYS.

4. Click **OK** to save settings. The new VSYS quota will be shown in the list.

Notes:

- Up to 128 VSYS quotas are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you must delete all the VSYSs referencing the VSYS profile.
- The maximum quota varies from one platform to another. The reserved quota cannot exceed maximum quota.

Entering the Non-root VSYS

To enter non-root VSYS, you can use the management IP of the non-root VSYS directly or enter from the root VSYS (only root VSYS admin has the privilege).

Using Management IP

After typing the management IP of the non-root VSYS in a browser, you should type the username and password in the login page. For example, the management IP of root VSYS is 10.90.89.1, after typing the username (hillstone) and password (hillstone), you can enter the root VSYS. After creating the non-root VSYS (vsys1), you should type the name management IP 10.90.89.1, type the non-root administrator username (vsys1\admin) and password (vsys1-admin), and then you can enter the non-root VSYS directly. For the detailed information of administrator configuration, see "Device Management" on Page 1169.

> **Notes:** If using the above method to enter the non-root VSYS, you cannot return the root VSYS. You need exit from the non-root VSYS, and then type the management IP in the browser for the root VSYS.

Entering from the Root VSYS

The root VSYS administrator can enter the non-root VSYS from root VSYS. The administrator in the root VSYS can configure the functions of the non-root VSYS after entering it. To enter a non-root VSYS, take the following steps:

1. Select **System > VSYS > VSYS** to enter the VSYS page.

2. In the VSYS list, click the name of non-root VSYS, and enter the non-root VSYS.

3. Return to the root VSYS, click ⌄ in the right top corner of the page, and click **Return Root VSYS** in the pop-up dialog box.